



Pekka Iivari

BUSINESS SECURITY AND RUSSIA

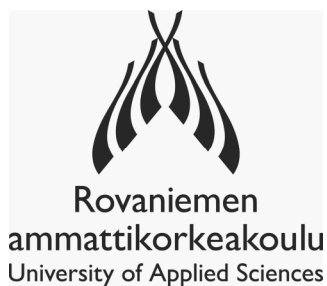
Security considerations in the development
of business operation in Russia



Rovaniemen
ammattikorkeakoulu
University of Applied Sciences

Rovaniemen ammattikorkeakoulu

julkaisusarja c 17



ROVANIEMI UNIVERSITY OF APPLIED SCIENCES

BUSINESS SECURITY AND RUSSIA

**Security considerations in the development
of business operation in Russia**

Pekka Iivari

2008

C series no. 17
ISSN 1239-7741
ISBN 978-952-5153-67-5 (vol.)
ISBN 978-952-5153-68-2 (pdf)

Translated from the Finnish publication by BSF / Keith Kosola
Rovaniemi 2008
Tornion Kirjapaino

CONTENTS

FOREWORD	5
1 BACKGROUND	7
1.1 Increasing economic co-operation	7
1.2 Russian markets and business opportunities	9
2 CONCEPT OF BUSINESS SECURITY	12
2.1 Business security in general	12
2.2 Concepts of security and business security in Russia	14
3 TRAVEL SAFETY	24
3.1 Preparing for a trip	24
3.2 Health	25
3.3 Communication and travel equipment	26
3.4 Crossing the border	27
3.5. Travel safety instructions in the Barents region	29
3.6 Services of foreign embassies	30
3.7 Travel restrictions	32
3.8 Preparing for a traffic accident	36
4 SAFE LIVING.....	42
4.1 Registering	42
4.2 Living and residing	44
4.3 Home and family security	45
4.4 A few judicial issues	52
5 SECURITY OF BUSINESS OPERATION.....	54
5.1 Security culture starts from the management	54
5.2 Partner selection and background checks	57
5.3 Observations that illuminate backgrounds.....	62
5.4 Establishing a company	65
6 RISK MANAGEMENT AND RISK ANALYSIS.....	69
6.1 Recognising risks and the probability of them materialising	69
6.2 Framework of analysis.....	70
6.3 Security environment analysis	74
7 AGREEMENT SECURITY.....	76
7.1 An important part of a company's economic security	76
7.2 Safeguarding business interests	78
8 LICENCES AND CERTIFICATES IN RUSSIA	80
8.1 License	80
8.2 Certification	84
8.3 Work permit and occupational safety	85
9 HIRING A SECURITY COMPANY	91
9.1 Background checks are important.....	91
9.2 Agreement with a security company	94
10 INFORMATION SECURITY	98

10.1 Security awareness must be increased	98
10.2 Information security mind-set is built under state control	99
10.3 Practical view on information security	104
11 FIRE SAFETY AND RESCUE OPERATION	111
11.1 Fires are a common problem.....	111
11.2 Rescue planning in co-operation with the authorities	112
12 CRIME SAFETY	117
12.1 Internal and external challenges.....	117
12.2 Initial phase security investments	119
12.3 Acquiring basic information is important	120
12.4 Organised crime	122
12.5 Crime prevention.....	125
12.6 Economic crime	127
13 FIGHTING CORRUPTION	131
13.1 World-wide situation	131
13.2 Corruption in Russia	133
13.3 Fighting corruption in the Murmansk region.....	136
14 ECONOMIC SECURITY	141
14.1 Corporate espionage.....	142
14.2 Competitive intelligence	143
14.3 Takeovers	147
15 ENVIRONMENTAL SAFETY	154
15.1 Ecological mind-set as a competitive factor	154
15.2 Norms.....	154
16 BUSINESS CULTURE.....	157
16.1 Familiarity with Russian culture as the key to co-operation..	157
16.2 Features of Russian culture	158
17 WORKING WITH THE AUTHORITIES.....	162
18. SUMMARY	165
REFERENCES.....	166

FOREWORD

Information dealing with business security is needed year after year. Economic life and authorities as well as ordinary people and educational institutions interested in security issues want to know exactly what business security means and how business security should be taken into consideration in daily business operation. There is a sufficiency of material and also textbooks produced for Finnish readers. Business security has been diversely covered in publications that have already been produced. The literature on business security has been able to credibly systematise the concept of business security into sub-areas where everyone can find the most important issues requiring development in their own organisations from the standpoint of their own operation.

After the concepts and content of business security became established, a need has arisen for more practical information to support daily business operation and teaching. For example, detailed instructions and diversified publications on office security, staff safety and fire safety are gradually becoming available. They serve security planning in these sub-areas of security.

By browsing literature databases anyone can notice that there is very little business security literature related to operation in Russia. Russia is among Finland's three most important trade partners, so the gaps in information need to be filled quickly. This Business Security and Russia booklet set out to meet the needs of the partner companies in the Doing Business Safely in Russia project realised within the framework of the Finnbarents Development Unit of Rovaniemi University of Applied Sciences. This booklet strives to respond to the demand related to business security considerations in the Russian markets. A comprehensive presentation of the Russian business security mind-set has not been produced in Finland before this. It is necessary for Finns to know exactly what kinds of issues are being discussed in Russia when the topic is business security. Business security is approached from a slightly different viewpoint in Russia than it is in Finland or the Western countries in general.

The purpose of this booklet is not to repeat the business security classification already thoroughly covered in Finland. This booklet brings out the special features that colour the Russian business security mind-set. Corporate takeovers, security company operation, emphasising background checks and a technically oriented information security mind-set are all special features of Russian business security that this booklet strives to reveal.

Legislation changes rapidly and security procedures are also modified. That's why it is worth remembering that the issues explained in this booklet depict

the situation as it is viewed in the summer of 2007. After a few years many parts may have become outdated and the focal points of business security may have changed. Naturally, this booklet is only a general presentation, since it deals with many sub-areas of security, each of which would merit even a separate publication. During the various phases of compiling this handbook the author has received bits of information from different experts and companies. The author wishes to especially thank Project Coordinator Vesa Koivumaa for his proficient comments during the compilation of the manuscript. Nevertheless, the undersigned is alone responsible for the content. Finnbarents and the Doing Business Safely in Russia project are thankful for any feedback, both critical and supportive, that the readers find in themselves to give.

If the reader's selection of tools for ensuring business security is supplemented by this booklet, the author's wish will have been fulfilled. The most important objective of the Doing Business Safely in Russia project and this booklet is to promote trade between Finland and Russia.

Pekka Iivari
Project Coordinator
Finnbarents

1 BACKGROUND

1.1 Increasing economic co-operation

After the Cold War in the 1990s business opportunities and the Finns' interest in Russia's markets grew strongly. Immediately after the fall of the Soviet Union a broad discussion began about Russia's security problems and their possible effects on Russia's internal security and for other countries. The question about Russia's mafia began to resemble an avalanche. By the end of the decade the worries about the strong hold of the mafia, whatever it meant at various times, proved to be over-emphasised. Common ignorance about Russia caused fear and uncertainty, which was either fomented or covered, depending on who presented these so-called facts.

The worst factor of uncertainty in foreign trade in the 1990s was linked not to crime, but to political and economic instability. The collapse of the rouble in August 1998 realised the threatening economic visions. Political instability was also reaching a peak at the same time. The attempted coup in 1991 and the armed uprising of the Russian Duma in the autumn of 1993 remained in peoples minds for a long time. Russia was depicted as a chaotic state that could disintegrate at any time. The economic uncertainty and the collapse of the economy during the previous decade chased foreign entrepreneurs away from Russia more than any individual traditional security risks. Of course, in individual cases lawlessness, such as company takeovers, led to a withdrawal of Western business operation.

Soon after the devaluation of the rouble the key economic figures began to move in a better direction. Economic growth began already in 1999, and it is still continuing. Improvement in the general operating prerequisites of the economy during Vladimir Putin's presidency, such as a rise in the price of oil and gas, also brought political stability. During the new millennium the administrative machine has been brought to order and the risk of Russia disintegrating has diminished.

At times security issues have entered the discussion when talking about business operation in Russia or Russian business entering the Finnish markets. Russia's societal and economic situation is still under change, but the predictability of the economic operating environment appears to be improving. Trade practices are approaching those of Western countries, although there is still room for development. Neither do the actions of the authorities in every way meet the requirements of a developed administrative culture. Although the country's central administration has attempted to create the same operating prerequisites in different parts of the country, circumstances may differ considerably by region. The fact that Russia was accepted as a full-fledged member of the G8 industrial countries in 2002 should signify something

about the stability of the business environment. Russia was also removed from the black list of the OECD's committee looking into money laundering, which indicates that the reliability of the financial sector has improved.

The need for information about post-Soviet circumstances in Russia has continuously been at a high level. The Doing Business Safely in Russia project has strived to produce up-to-date security-related information that serves business operation in the Barents region. The first phase of the project was started in 2004 after a preliminary study conducted during the two previous years. Experiences with business security-related issues of 36 Finnish companies in different fields currently or previously operating on the Russian side in the Barents region were determined with a questionnaire survey. The study, which can be found at <http://www.finnbarents.fi/safelyinrussia>, was completed from a practical viewpoint. It provided valuable information about companies' experiences in Russia.

Projects concentrating on business security have not been started earlier in the Barents region, but the topic has been discussed during the entire post-Soviet period in all the Scandinavian countries and also in Russia. The Doing Business Safely in Russia project and its continuation project have strived to respond to the need and demand for security information. As an outcome of the questionnaires it can be said that security is not an obstacle to the development of Russia's business operation. It was noted in the Doing Business Safely in Russia project that over half of the interviewed companies had been spared from crime. Yet, crime is encountered. Burglaries of homes, vehicles and offices are most common. Neither is corruption a completely unfamiliar phenomenon in the Russian business environment. A clear conclusion drawn by the Doing Business Safely in Russia project is that the significance of security in starting and developing business operation cannot be underestimated. Companies operating in Russia, not to speak of those intending to operate there, have a need for up-to-date information on business security (Koivumaa & Koivumaa 2004).

In this conjunction security is understood broadly. Business security in general or security issues in Russia are not comprised of only actual crime or the tasks of the police/militia. The surveys of the companies completed during the Doing Business Safely in Russia project clearly indicated that practical business security also includes information security, travel safety, personal matters, fire safety and rescue operation. Development of a network of co-operation comprised of security companies, authorities and educational units in the Barents region also provides tools for resolving questions of business security on a practical level. Development of a network of co-operation in the security sector has progressed during the Doing Business Safely in Russia project.

As an important observance may it be mentioned that surprisingly little business security information related to operation in Russia has been produced in

the form of handbooks. The definition of Russian business security is not familiar. An Internet search provides a good picture of the situation. Various parties do mention the issue in their lectures, but there is a scarcity of guides or other printed matter. Much information on the topic can be found, but it is scattered. The field of business security combined with Russia know-how appears to be possessed by consulting companies or experienced Russia operators, who disseminate their knowledge only on a commercial basis. Furthermore, each consultancy focuses on a special field, paying less attention to other security concepts. Public sector operators like educational institutions have not had access to an overall view related to Russia that could be placed in the form of a guide, for example. In addition, neither consultants nor public sector actors in Finland have been able to provide answers to certain special questions, such as doing background checks or company takeovers in Russia.

Concrete risks of business operation can be listed by the hundreds, and it is probably impossible to make an exhaustive presentation. For this reason the focus is usually on focal areas where management of emerging risks brings the greatest added value to operation. The Doing Business Safely in Russia project has found focal areas that arise from regional needs and the special features of the Barents region. The goal of this booklet is to provide help also when operating outside the Barents region. Many of the issues presented in the booklet also hold everywhere in Russia.

Of course, security is not the primary factor in considering development of business operation in Russia. Numerous other issues, such as language skill, taxation and customs have bypassed security when speaking of obstacles and hindrances to business operation in the direction of Russia. Nevertheless, security must not form a threshold question even on the conceptual level. Regrettably, mental images steer behaviour and conceptions. Creating a real picture of a situation, for example a crime scene and actions of authorities, brings issues to their correct scale. That is also the purpose of this booklet.

The booklet at hand was created as an outcome of the Doing Business Safely in Russia project, which strives to respond to the need for information on business security in Russia. The booklet gathers concrete information in one volume. This need for information has come up in the field where the staff has worked together with pilot companies and other business partners.

1.2 Russian markets and business opportunities

The Russian markets require a relatively large capacity to take risks, well-established relationships – preferably also on a personal level – and persistency to remain in the markets regardless of changes in circumstances. In 2007 Russia became Finland's largest trade partner. Russia is number one in imports (2007). The value of Russian imports was €7.7 billion in 2006 and exports rose to €6.2 billion. In 2006 Russia was number three in exports after

Germany and Sweden (Spiridovitch 2007). Finnish entrepreneurs are more and more interested in the Russian markets. And it is not only a question of the Russian markets. Already now, Russia produces products, goods and services with increasing demand also in the West. If the development of the past few years continues, Russia will increasingly finance large co-operation projects. Furthermore, the growing need for labour in Russia will most likely open job opportunities for specialists in various fields in the near future. In some fields Russia's competitiveness in terms of the wage level is approaching that of the Western countries.

In addition to traditional importing and exporting, starting production in Russia is an increasingly attractive possibility. Finnish subcontracting is common today in places like Kostamukša. Successful Finnish business operation can also be found in the Murmansk region. Russia has proved to be a significant opportunity for these companies. Along with Russia's possible WTO membership the country's business procedures and legislation will approach the practices of Western countries. At the time Russia will commit to certain stabilising factors like a balanced financial policy and preserving the value of currency. Stability should increase in policy and in the legislative and economic sectors. Russian administrative bodies have an increasingly positive attitude towards foreign, and namely Western, business operation in Russia. Russia's regions want to construct development programmes to attract foreign investments, and foreign trade in the regions is constantly expanding. According to statistics, foreign trade is also growing in the Murmansk and Archangel regions (Kosonen 2007).

There are differences in the economic status of companies in different localities. Some regional and local administrations collect taxes and fees even though their possibilities to levy taxes and fees and grant exemptions have been reduced and different parts of Russia have been harmonised. Official Russia emphasises the importance of foreign investors, but in practice the attitude varies by field and by region. Most regions in Russia expect foreigners to invest in infrastructure, for example as a prerequisite for establishing a production plant. Foreign investors are also expected to invest in social questions, which has remained in the administrative mind-set as a Soviet heritage.

Despite the increased stability, security is still a current topic. According to the Research Institute of the Finnish Economy, ETLA, Russia is one of the world's unsafest regions, even though some positive development has happened in Russia's overall security in the 2000s (Möttönen 2004). According to ETLA, the reliability of the legal system is weak and there is much organised crime in the country. The greatest cause of worry is the dysfunctionality of public institutions. Ownership rights are poorly protected and the independence of the legal system is minimal. Large-scale organised crime, which is linked to money laundering and economic crime, also causes security risks. Business security is affected by not only organised crime, but also the efficiency of the militia's operation, the reliability and fairness of the legal sys-

tem and the appearance of corruption. According to the World Economic Forum's 2006-2007 report on international competitiveness, published in November 2006, Russia's private business operation faces problems particularly in the operation of the legal system, and deficiencies are also found in the independence of the courts of law, for example.

According to independent international research institutes (e.g. Transparency International), the degree of corruption in Russia is of the same magnitude as it is in African countries, and in recent years the trend has even gotten worse. The above-mentioned ETLA report also expresses concern about the widespread corruption in Russia. In addition it must be remembered that corruption is directly connected to the country's competitiveness placement and thereby its business opportunities. Thus, security is a prerequisite for good competitiveness.

Due to the ongoing political, social and economic changes in Russia, Finnish regional development organisations, authorities, research institutes and educational institutions need to continuously update their information related to circumstances in Russia. This is a challenging task. Within the framework of the EU Finland is expected to have special Russia know-how, especially now when Russia's economy is rapidly growing but the country's political map is still in the making. Finland needs to bring up also difficult topics related to Russia, which undoubtedly include security issues. The Russians themselves strongly discuss about, for example, business security, corruption, company takeovers and organised crime. We need to be aware of the content of that discussion also here in Finland.

2 CONCEPT OF BUSINESS SECURITY

2.1 Business security in general

Attending to security issues is part of the daily work of the staff of companies and production plants. Maintaining security in companies is controlled by several legislative obligations. Laws governing occupational safety, rescue operation, product safety, consumer protection and chemicals are examples of legislation that controls the level of security and development of security in companies. In Finland the Rescue Act and the government statute on rescue operation obligate companies and building owners to prevent dangerous situations and to be prepared to protect people, property and the environment in dangerous situations and to be prepared to carry out rescue operations that they are capable of implementing. The basic tasks that are required in Finland to maintain security are to a great degree also applicable when arranging business and production operation in Russia.

A few books on business security have been published in Finland during this decade. In 2002 Juha E. Miettinen wrote the first basic book that described the sub-areas of business security in a systematic form. According to Miettinen, business security is comprised of many sub-areas that are integrated into a company's day-to-day management. In his book Miettinen also covered business security and travel safety in foreign operations. Business security in foreign operations is an entity comprised of functions with which a company strives to ensure the security of its operation when conducting business operation abroad (Miettinen 2002, 16).

Business security can be classified into sub-areas in many slightly different ways. According to the Business Security Advisory Board (2003) formed by the Association of Service Industries, the Confederation of Finnish Industry and their approximately 12,000 member companies, the sub-areas of business security are:

- Office security
- Crime safety
- Rescue operation
- Readiness planning
- Occupational safety
- Environmental safety
- Production and operational safety
- Personal safety
- Information security and
- Security of foreign operations.

Classifications of business security into sub-areas that are presented in Finnish literature are most often based on the Business Security Advisory Board's (YTNK's) classification. For one, Kerkko's (2001) classification is in line with the classification presented by YTNK. Also Miettinen's (2002) classification into sub-areas for the most part follows YTNK's classification presented above. One difference from YTNK's classification is that in Miettinen's classification business security management, insurance and travel safety form their own sub-areas. Additionally, Miettinen's classification includes fire safety in the sub-area of rescue operation. Miettinen calls the sub-area of readiness planning preparation for emergency conditions. However, from the standpoint of a company, it is a question of the same issue. Crime safety means preventing threats against a company's staff, property and information.

Numerous presentations of the aforementioned blocks and their contents have been compiled in recent years, which can be found on the Internet, for one. Literature on this issue can be considered extensive as far as Finland is concerned sufficient. In Finland the concept of business security and its sub-blocks are clear-cut and well established. This booklet does not rehash these sub-areas, instead it concentrates on a question that is quite rarely mentioned in Finnish literature, namely business security in Russia and its special features.

The Finnish business security concept is a good starting point also when operating abroad. The above-mentioned YTNK classification into sub-areas of security is a valid proposal for building security in any target country. The list only needs to be weighted according to each country's different concepts of culture, legislation, trade procedures, official functions, infrastructure and security, and possibly also the entity formed by religious customs.

According to the modern definition business security is part of a company's integrated management system. Business security is not viewed as a separate entity, it is understood to be included in the company's other operation. This mind-set again is closely linked to security culture, which must underlie the development of business security. Culture consists of attitudes and values as a type of higher concept (Verhelä 1997, 30). An organisation's security culture begins from the company's management, which is responsible for ensuring that security is implemented according to the laws of the country. Essential issues in the implementation of security are the staff's attitude; the people, tools, equipment and devices participating in production; security planning and the operating environment (Security guide 2005, 28 – 29).

There is no one and only recipe for security management. The way security issues are organised depends on the company's size, field of operation and location. It is the management's task to create a security strategy and security goals for the company and to decide on the measures needed to achieve the goals specified in the security strategy. To realise these goals the company

needs immaterial and material resources. The company's management assesses and specifies necessary resources and distributes them according to the focal points of the goals. Another task of the management is to foster a security culture (e.g. attitudes towards security) in the company and assume responsibility for development of security. In a small company with scanty immaterial and material resources, the manager alone is responsible for expertise in security issues. In a larger company, people responsible for security and their alternatives are appointed. The company's security manager develops and directs measures related to the company's security issues. In addition to a person with overall responsibility for security, a person responsible for security in each sector of operation is appointed, who compiles and updates security instructions for the operation in question and trains the sector's staff within the framework of their special field. Security education is also arranged for the entire staff and the people responsible for security (Kelo, Ahola & Leino 2007, 205). Never is too much emphasis placed on the fact that in a company or any other organisation the security person, or security employee, is not a man with a weapon, but a manager, analyst and educator in the same package.

International trade is imperative for more and more Finnish companies. Foreign operations are faced when selling and marketing products and services abroad, but also when planning to start production abroad. Examining business security in a strange environment will be a current issue for numerous Finnish entrepreneurs in the near future. Business security of foreign operations as such does not differ decisively from the basic issues we are accustomed to considering in ensuring security in Finland.

The special risks of a foreign country are taken into consideration in developing business security. For example, country risks (political risks) are one partial factor of security that is always kept in the headlines when talking about Russia. A country risk is a risk to a company's operation in the target country that affects the profitability of business. A political risk refers to the possibility that the target country's political decisions, circumstances or events may affect the operating environment negatively and unexpectedly. In Russia political risks may be associated with changes in laws and regulations, changes in government, environmental and human rights questions, ethnic conflicts, currency crises and terrorism. All of these have been experienced in Russia, i.e. all of these risks have materialised to a certain degree during the last decade. In addition to the challenge of business operation, Russia also offers a diversified field for assessing business security. Companies' experiences have been wide-ranging, and we can learn from them.

2.2 Concepts of security and business security in Russia

Business security and Russia form a challenging topic in which many kinds of viewpoints can be applied. On one hand we could strictly adhere to headings that are in line with the Finnish business security mind-set and present

the corresponding entities using the same template, but from the Russian viewpoint. On the other hand it would be possible to isolate namely Russian special features and weightings from the topic and use them to fill in the established concepts of business security. However, neither approach would serve the interests of practical entrepreneurs, much less readers interested in the Russian business security mind-set. The author of this booklet has deemed in most suitable to describe a company's security issues in a way that is sensible expressly in the Russian operating environment. The handbook leans on Russian business security discourse, the field's literature and available experts' experiences with Russia's reality.

Business security concepts are continuously being created and modified in Russia. While the content of business security in Finland was created within the past decade, in Russia the concepts of business security are still being shaped. Despite the fact that a uniform concept has not been created, discussion about the theme is brisk in Russia. In Russia, business security, for which there are at least three expressions (безопасность предпринимательской деятельности, деловая безопасность, безопасность бизнеса), has not found its way into the concept of security defined by the state, which is described in the federation's law on security (О Bezopasnost).

Due to the relative newness of private business, Russia business security includes varying terms that change as new threats arise or laws are passed. In recent years the following security factors have received particular attention in various seminars held in Russia:

- Business partners
- Establishment of a company and selection of employees
- Staff safety
- Property risks
- Risks related to taxation, accounting and operative functions
- Competitors
- Patent and copyright violations

Loginov (2006, 8), a Russian author who has studied Russian business security, defines business security (безопасность бизнеса) as follows: "Business security is understood as protecting the interests of the state, owners of commercial and official secrets, management, staff, material and financial reserves, buildings and equipment, raw materials and products and information resources from internal and external threats. In addition, securing business operation is understood as a company's stable business operation at the present and in the future. The state of security is the company's capacity and possibility to prevent in a desirable way the efforts of all criminal structures and dishonest competitors to cause damage to the company's legal interests." Loginov's definition depicts well the broad concept of Russian business secu-

urity operators. State security is also strongly bundled into the concept, without forgetting criminal elements and competitors.

Kuznetsov (2007) divides the concept of business security into blocks of economic security, information security, personal safety and security of foreign operations. According to Kuznetsov, economic security is the most extensive block of business security, in which he includes measures from access control and guarding to a competitor's intelligence activity and a threat to economic operation caused by organised crime. Writing to Russian readers, Kuznetsov (2007, 111 – 185) emphasises the technical solutions of computers in information security because according to (Russian) experts Russians do not take ADP security into account enough in their own information security solutions. This is considered to be caused by Russia's lagging behind in information-related security solutions compared with Western information security culture. Jushtsuk (2006), in discussing intelligence activity performed by a competitor (competitive intelligence), devotes a large part of his book to information security solutions and utilisation of information networks. Most of the technical concepts and mind-sets of business security have been directly influenced by Western, particularly American, business security literature, which is clearly visible in Jushtshuk's manner of presentation.

Petrov's (2007, 48) description of security management indicates that the Russian mind-set of security management and business security being part of an integrated management system is comparable with the Western concept of security. Russian business security management emphasises the significance and responsibilities of both the manager and the assistant manager responsible for security. Their work is supplemented by security consultants from different fields and the department managers of the organisation. A security commission or team functions as an operative tool for the organisation's management. The commission-centred operative security system, typical of the Russian organisation mind-set, includes management of various security blocks, such as electrical safety, fire safety, terrorism and production safety (Petrov 2007, 48). This type of security structure ensures the special expertise of each security block, but it may also appear to be heavy to manage in the private sector from the Western (Finnish) viewpoint.

In addition to the Russian professional literature mentioned above, many popularisations of business security have dominated the reader markets. Some of this type of literature belongs in the plagiarised espionage novels department (see e.g., Melton et. al. 2005).

Thus, the way of looking at the sub-areas business security in Russia differs significantly from the established Finnish understanding. The major change in Russian society during the last decade and a half and the violent growth in crime brought about by the change have put their mark on the business security mind-set (Loginov 2006, 10). Both small companies and Russia's gov-

ernment are worried about the criminalisation of the economy, especially, and thereby of business life (see Russia's small enterprise fund 2007). At the government level, preventing crime from penetrating the private sector and public administration involves preventing corruption and other economic crime. At the business level, acquiring information about one's partner, his background and operating principles emerges as the most important preventive security issue in preventing criminalisation. In Russia, the information that a partner wishes to give is not enough for initiating a partnership. For this reason the significance of checking backgrounds rises to an important, even decisive position. Backgrounds should be checked during the employee recruitment phase and the backgrounds of partners should be checked before entering any agreements.

From the viewpoint of small companies, especially the following sub-blocks come up in developing business security in Russia (source: Biznes Tezaurus 2001):

1. development of the legislative base, which includes, for example, increasing the transparency of political-administrative operation;
2. protection of intellectual property;
3. government measures to protect from crime;
4. decreasing threats caused by corruption of government officials;
5. supporting foreign operations of significant Russian companies;
6. government support of nationally significant fields of operation.

Compared with Finland, the business environment in Russia is significantly more dependent on the government regulation system. Practical official actions create day-to-day prerequisites for business operation. Indeed, the quality of official actions may vary by region. Some regions in Russia have been able to create an image of business friendliness. Such regions include, for example, Kaluga and Nizhnyi Novgorod. Furthermore, most Russian regions compiled foreign investment laws and prepared crime prevention programmes, for instance.

The Russian business security concept derives its content especially from the following entities, which according to Russia's small enterprise fund are targets of development efforts in Russia:

- Protection of technological processes
- Prevention of industrial, scientific and technological, and economic spying
- Immediately notifying management of illegal actions within a company and by parties outside the company
- Protection of persons with confidential business information
- Many-sided examination of partners
- Prompt reaction to disinformation related to a company
- Protection of commercial information

- Reaction to unhealthy competition
- Protection of intellectual property
- Rescue and readiness operation
- Co-operation with law enforcement authorities
- Measures to be carried out in case of threats

The small enterprise fund's (Fond Malogo i Srednogo Predprinimatelstvo) focal areas in business security were not in any way highlighted in Finland. A significantly different viewpoint concerns prevention of disinformation and corporate espionage, for example.

What is a small enterprise in Russia? The Federation's law supporting small enterprise operation (law 14.6.1995, No. 88-F3), passed in 1995, defines a small enterprise as a commercial organisation, in which the ownership share of the Federation, regions, religious and societal associations or charitable funds does not exceed 25 % and in which the ownership share of one or several juristic persons does not exceed 25 %. In addition, the number of employees must be:

- less than 100 in industry, construction and transportation;
- less than 60 in agriculture and scientific and technological operation;
- less than 50 in wholesale trade;
- less than 30 in retail trade;
- less than 50 in other fields.

The law also mentions that small enterprise operation includes physical persons who conduct business operation without establishing a juristic person, but who are nevertheless registered as individual entrepreneurs. The definition of a small enterprise is clearly based on a different scale compared with the Finnish concept of a small or medium-sized enterprise.

Crime prevention is viewed in Russia as the best way to improve security. Attention is paid to crime prevention activity by the authorities in Finland, also, for example in the Police Act (1995). In business security and home security the technical and human measures used to prevent crime are generally more robust in Russian than in Finland. Metal doors and special locks are used to shield the outer shell of residences. Visible and armed security personnel are used in access control and to maintain discipline in public places.

Although crime, its visible forms, are the first to come to mind when speaking of business security, security must be treated as a much broader and far-reaching concept also in operations in Russia. Crime prevention is only one part of the sub-areas of business security, as already mentioned. Most often the following issues are covered at business security seminars arranged in Russia (see e.g. <http://www.ya-plus.ru/other.php?prog=266>):

- Economic security
- Corruption
- Personal safety
- Government control
- Legal issues
- Information security

Russian business security programmes also deal with other themes that differ from Finnish focal areas, such as company takeovers and problems caused by piratism and bogus bankruptcies. These problems are widely known in Russia and the range of methods used to fight against these disadvantageous factors is being diversified. As an example, the Russian Central Chamber of Commerce's business security committee's programme for 2007 includes the following measures for promoting business security (source: Russian Central Chamber of Commerce 2006):

- National forum on information security in January 2007
- Development of corporate legislation to prevent company takeovers
- Co-operation between the private sector and the state in preventing terrorism
- Development of innovation and investment in Russia's defence industry
- Prevention of production and sales of bad-quality and counterfeit pharmaceuticals
- Promotion of an anti-corruption programme
- Protection of intellectual property
- Food safety
- Prevention of parallel imports and counterfeiting in textile and light industry
- Counterfeit aviation and transportation technology
- Bogus bankruptcies

The goals of the Russian Central Chamber of Commerce's business security committee are in line with the interests of the state. Take prevention of terrorism, for example, which is a relatively distant issue for Finns. It has become a priority in the government's security mind-set, but it also appears in the private sector's development programmes. Prevention of corruption and protection of the defence industry serve both business operation and the security objectives of the state.

Based on the above it can be concluded that business security is manifested as a different type of issue in Russia than it does in Western countries, e.g. Finland. Business security includes the government's strong, controlling grip. Threats and risks experienced by the state are directly included in the risks of business security (corruption, terrorism, defence industry interests). Yet, business security is not a mysterious issue in Russia, either. There is no need

to learn a new, totally different approach; the sub-area classification of Finnish business security can still be used as a basis. On top of that it is possible to tailor a business security structure weighted according to Russian principles. Probably most important is that issues related to Russian business security are discussed freely in Russia, and the Internet, for one, contains a variety of instructions for dealing with different threats.

An example is a consulting company that provides business security courses. It divides business security into the following parts (<http://www.vla.ru/>):

- Physical safety
- Personal safety
- Financial and economic security
- Information security
- Technological security
- Fire safety

Most often business security is not isolated from ensuring a company's economic security. The objective is continuity of the company's operation, which would not be possible without economic tenability. The complexity of the security concept is depicted with yet another viewpoint, according to which the following list of factors affecting a company's tenable existence was compiled (Ljannoi 2006):

1. Protection of business secrets, commercial secrets and confidential information
2. Computer security
3. Internal security
4. Building and equipment security
5. Physical/personal safety
6. Technological security
7. Security of technological connections
8. Agreement security
9. Passenger and freight transportation safety
10. Security of advertising, group events (exhibitions), business meetings and negotiations
11. Fire safety
12. Ecological safety
13. Radiation and chemical safety
14. Competitor's spying
15. Information – analysis work
16. Staff's sosio-psychological preventive actions and education in economic security issues
17. Expert assessments of security systems

Typical of Russian printed sources is that they openly tell about risks caused by organised crime and actions of the authorities. Finns are not accustomed to considering the impact of crime rings on business life – nor has it probably

been necessary. Certainly serious organised crime can be found in Finland, but its impact on the risks of business life have been studied very little. A joint strategy for preventing crime and malpractice directed at companies, published by economic life and authorities in 2006, is a good start in this direction. The strategy also deals with the threat that organised crime poses to business operation (Ministry of Internal Affairs 2006).

A Finn that becomes familiar with Russian internal discourse can easily note that people on this side of the border write about the security of the Russian business environment with much more restraint than do the Russians themselves. Perhaps insufficient information about Russia's security circumstances is the reason for this relative quiet in Finland. However, the fact that there is a certain amount of wariness in Finnish publication culture and economic life about bringing up issues thought to be unpleasant and even able to strain relations between the countries seems to be a more believable explanation. In Russia, however, it is customary to boldly publish the names of criminal leaders and participants in crime rings and to write very detailed accounts of crime cases that even reach abroad (see e.g., Leonov 2007; Rumjantseva 2007).

The number of operators affecting business security is no greater in Russia than the amount we are used to in Finland, but their influence varies by both region and competitive situation. In Russia both domestic and foreign business operations are objects of interest and are monitored by the state, competitors, criminal organisations and the companies' own staff.

The state monitors whether a company is registered, its operation is licensed and the company and its employees pay statutory taxes. Law enforcement authorities again are interested in all types of possible violations of the law from accounting offences to piracy and money laundering. For this reason in Russia one quite often comes across various tax and accounting audits, fire inspections or inspections conducted by hygiene officials and work permit officials. In addition to the objective of promoting security, inspections conducted by the authorities also serve to prevent crime. For example, an accounting audit could lead to the trail of a wide tangle of economic crime.

Criminal organisations closely follow the operation of foreign companies in Russia. Organised crime is a reality in Russia. According to the Russians themselves, at some stage it is necessary to enter into discourse with criminals; it cannot be avoided. Security companies know much about these issues and know how to fit their own operation according to the challenge posed by criminal groups operating in the region. If one's own actions breach the ethics or laws of business operation, the danger of having to deal with criminals grows. Pressure on a company does not necessarily come directly from criminals, but also through unhealthy competition. Of course, a company's financial reserves are the most important target for criminal elements.

The most important sub-areas in economic crime are fraud, counterfeiting and betrayal of trust. The most important methods of fraud are use of counterfeit documents (forged stamps) and actual or fictitious firms. Even more sophisticated forms of fraud are known. Establishment of firms for the purpose of doing a specific task, such as receiving orders, is a much used method of swindling. A prepayment is taken and then the firm disappears without leaving a trace. Nevertheless, the most skilful frauds are carried out by legal firms that have operated for some time in a manner that awakens trust. Such firms have created a credible facade as a cover for their true intents. Neither can anything obscure be found in the backgrounds of the people employed by such firms. Complex background checks and analyses of their financial operations are needed in order to identify such cover companies. Such background work can only be done by someone specialised in such work.

Competitors are naturally interested in the operations of foreign companies and also of companies with partnerships with foreign companies. New technology, work methods, expansion plans, information about current and future partners and customers are desired information. The objective of a competing company may be, for example, "seizing" advantageous contacts, investment projects and goods suppliers for itself.

According to the Finnish-Russian Chamber of Commerce Association SVKK (2005), Finns' experiences with the risks of operating in Russia indicate that the picture given of Russia with its criminals and mafia is not correct. SVKK's survey came to the same conclusion as the survey of companies conducted a year earlier by the Doing Business Safely in Russia project: Most had not experienced problems because of crime or an underground economy. According to SVKK, the greatest risks came from the direction of competitors and Russian administration.

Competitors may use the following forms of unhealthy competition.

- Economic spying
- Erroneous advertisement
- Compromising a firm, i.e. damaging its reputation
- Product forgery
- Physical and mental pressure, material damage
- Cartels
- Underground economy
- Customs tariffs
- Illegal business operation
- Bogus bankruptcies

All Finnish companies do not deem it necessary to set up all-encompassing internal and external security systems when operating in Russia. According to questionnaire studies, companies that fix attention on these issues in order to develop their internal security system not only check the background of

recruits, they also add confidentiality obligation and business secret clauses to job contracts. Rationalisation of the company's internal document management and improvement of information security have been important security development procedures. Reinforcement of their external security system includes external risk analysis, assessment of partners' reliability, arrangement of physical guarding and security technology, and acquiring information about competition and business operation (SVKK ry 2005, 69).

3 TRAVEL SAFETY

3.1 Preparing for a trip

Starting business operation in a foreign country requires careful advance preparation. The same serious attitude is necessary when embarking on a business trip. The staff going to a foreign country needs to become familiar with their tasks, the country's culture, the functioning of the society and the laws and customs of the country beforehand. Daily security routines must be reviewed with the travelling staff and their families.

Travel safety is the most common and perhaps most important form of security that needs to be considered in both business operation and private travel in Russia. Travel safety is part of a company's daily operation. Its goal and purpose is to provide people with the knowledge, skills and tools they and their fellow travellers need to make a (business or other) trip without mishap. Travel safety is emphasised here because the most likely risks of foreign operation are associated with travel.

Numerous good sources of information about travel safety are available. Travel instructions compiled by the Travel Safety Committee (see www.formin.fi) offer a usable tool that helps both entrepreneurs and ordinary travellers take the risks associated with travel into consideration. Particular information about each destination can be obtained from the foreign ministry, the embassies of the countries and travel agencies. The foreign ministry's web pages also offer good advice about travel bulletins, mobile phone services and making a travel notice. Travel safety touches both business travellers and tourists. For example, the Tourism Act passed by the regional Duma in the Murmansk region obligates the region's authorities who have obtained information about a danger that threatens the safety of travellers to inform travel organisers, travel agencies and tourists about the danger (Oikarinen 2005, 14).

How does one travel to Russia? In order to be able to travel to Russia, every foreigner except for the citizens of certain CIS countries needs a visa, which is appended to the traveller's passport. The visa grants permission to travel to and from Russia. The duration of stay in Russia is specified in the visa.

There are seven different kinds of Russian visas: 1) tourist visa, 2) business visa, 3) student visa, 4) private visa, 5) transit visa, 6) short 72-hour visa and 7) group visa. Usually the best alternatives in terms of cost are a tourist visa and a business visa. A tourist visa is a good choice for a short-term stay (no longer than one month) and only one or two visits. A tourist visa is not recommended for official visits, in such a case the visa should be a *delovoje* or business visa. Security company representatives have told the author of this

booklet, among others, that they wondered why officials travelling to official meetings have travelled with a tourist visa. A business visa should be obtained if several trips need to be made. If necessary, travel agencies can arrange an invitation.

3.2 Health

Since the beginning of June 2007 it has no longer been necessary to submit an HIV certificate for a one-year visa. However, HIV test results no more than one month old are needed for a more than three-month continuous stay in Russia (work or study). HIV is spreading rapidly in northwest Russia, and tourists should be careful because of this phenomenon.

Country-specific vaccination recommendations can be found at www.rokote.fi. For a long-term stay in Russia, the following recommendations are recommended (situation in 2007):

- diphtheria (recommended for everyone)
- typhoid fever (based on a risk assessment)
- tick-borne encephalitis (based on a risk assessment)
- Japanese encephalitis (based on a risk assessment) for those travelling to the eastern parts of Russia
- measles (recommended for everyone)
- mumps (recommended for everyone)
- German measles (recommended for everyone)
- tetanus (recommended for everyone)
- A and B hepatitis (based on a risk assessment)

Tuberculosis is spreading in Russia, mainly in prisons and among people seriously displaced from society. This fact needs to be kept in mind when selecting travel destinations and visiting sites. The danger of salmonella also needs to be taken into consideration just as it does when travelling elsewhere in the world. There are vaccination requirements or recommendations for these diseases. A salmonella vaccination is recommended for someone travelling to southern Russia, e.g. the Caucasus region. Cholera has been reported here and there in Russia, but the risk is not significant.

Western travellers have noticed that meals and cold salads can be enjoyed in Russia without health effects. Of course, the place where one eats should be chosen carefully. The availability of fresh water is not a given, for which reason it has become common for travellers in Russia to carry their own water container with them. Bottled mineral water is the safest alternative. Drinking tap water is not recommended, although the tap water of Hotel Poljarnye Zory in Murmansk did not cause any heartburn for the author of this booklet.

3.3 Communication and travel equipment

A person planning to travel should arrange to contact a family member or other person, e.g. his/her employer regularly during the trip. This way it is possible to make sure the person's trip progresses as scheduled and the person is not stuck along the way for some reason. Sending a text message is the easiest and cheapest way to notify of the progress of the trip. In arranging the contacts the person can agree on a method for keeping in touch. For example, at the customs station the person can send a message saying that the next message will be sent from Alakurtti (if going to Kandalakša) or from Ylätuloma (if going to Murmansk). Travel safety should be taken into consideration in the contents of one's suitcase and other travel equipment. Depending on needs and assessed risk, travel equipment could include:

- Lockable suitcase
- Warm clothing
- Ordinary pain relievers and prescription medication
- First aid kit; in a vehicle, a well-equipped kit
- Filled out health card (see the separate paragraph on this)
- Portable crime reporting system and kidnapping alarms
- Smoke, carbon monoxide and gas alarms
- Phone and spare battery
- Spare phone and alternative SIM card
- Secret pockets in clothing for hiding cash
- Camera
- GPS device
- Extra travel insurance, e.g. electronic equipment carried along

It is necessary to keep an eye on one's own suitcase during the trip. It is possible for someone who wants something smuggled across the border to insert illegal objects or goods (drugs) into a suitcase without the owner knowing it. A well-equipped vehicle also includes a fire extinguisher, a fire-extinguishing blanket, a shovel, a checked spare tire, a spare fan belt and possibly also a satellite phone.

- Copies of travel documents should be kept along.
- Sufficient clothing in case it is necessary to sleep in the cold
- Special precautions if children are along → home and family security
- Notify someone at the destination and in Finland upon leaving
- Travel insurance, vehicle insurance

From the standpoint of a company's information security, particular attention should be paid to important property. Laptop computers and memory sticks are not only desired items for resale, they may contain valuable business material that, if lost, may cause losses in business operation either immediately or sometime later. Keeping a laptop computer elsewhere than in its original carry bag lowers the risk of theft. Protective software and passwords make it

difficult to access information and provide security in case ADP equipment is lost. Keys and other items not needed on the trip should be left home. In busy places like airports a laptop can easily end up in the wrong hands. At airport security checks one should make sure the computer is not picked up from the conveyor belt by the person ahead in line. Cases have been reported where a thief has waited for a computer to pass through an X-ray machine on a conveyor belt and has then disappeared with the computer.

3.4 Crossing the border

Before crossing the border it is necessary to check that the vehicle has enough fuel and there are no items in the vehicle that could cause problems at the customs station, like, for example:

- a hunting rifle, cartridges
- a radar detector (illegal in Finland)
- medication that is not intended for one's own immediate use.

Pain relievers and stomach tablets should be taken along from Finland. If anything other than over-the-counter medication is taken along, the prescription should also be taken along to prove that the medication is for personal. Prescription medication must be listed on the customs declaration. Medication should be transported in its original packages and sales receipts should be taken along. This way customs officials can ascertain the content of the product(s) and time is not lost in determining the active ingredients of the medication. The officials also compare the amount of medication brought along with the length of stay. Large amounts, especially of sedatives (containing ingredients that are classified as drugs), in proportion to a short stay may lead to administrative legal consequences.

When travelling from Finland to Russia, the border formalities include:

- an entry card (see appendix); part B must be kept along during the entire trip
- possibly a customs declaration form, on which is entered the, amount of currency and other valuable property
- the entry card and customs declaration form are returned to the customs officials upon leaving the country
- a vehicle pledge that obligates the driver to bring the vehicle out of Russia within a specified period
- in winter, a studded tire ID (if the vehicle has studded tires)
- a nationality ID; FIN
- mandatory traffic insurance can usually be purchased at the Russian border crossing, but this should be verified before embarking on the trip. Finnish agents also sell insurance
- it is good to take copies of all documents

When returning to Finland, check if you have with you the following:

- so-called rarity items, like old objects from Russian cultural history; samovars, icons, old paintings, require an exporting permit
- over 10,000 USD requires a permit from the Central Bank of Russia
- alcohol (Finland's customs regulations) and tobacco
- medication that requires a prescription in Finland but is over-the-counter in Russia

TABLE 1 International passport inspection points and their open hours (Finnish time unless mentioned otherwise).

Vaalimaa	
Mon-Sun:	24 hr
Tel.	+358 20 410 2170
Nuijamaa	
Mon-Sun:	24 hr
Tel.	+358 20 410 2370
Vainikkala	
Mon-Sun:	According to the train schedule
Tel.	+358 20 410 2330
Imatra	
Mon-Sun:	07:00 – 23:00
Tel.	+358 20 410 2450
Niirala	
Mon-Sun:	24 hr
Tel.	+358 20 410 3270
Vartius	
Mon-Sun:	07:00 – 21:00
Tel.	+358 20 410 4273
Kortesalmi (Lämsänkyläntie 465, Kuusamo)	
Mon-Sun:	08:00 – 20:00
Tel.	020 492 8540
Fax	+358 20 492 8545
Salla	
Mon-Sun:	07:00 – 21:00
Tel.	+358 20 492 8560
Raja-Jooseppi / Lotta	
Mon-Sun:	07:00 – 21:00
Tel.	+358 20 492 8600
Storskog / Borisoglebsk	
Mon-Sun:	06:00 – 23:00 (Norwegian time)
Tel.	+47 78 994 830

When you return from Russia the Russian customs official will ask if you have any of the above items along. On returning make sure to return the vehicle return pledge to customs. Make sure the duration of the trip does not exceed the deadline mentioned on the vehicle return pledge.

There are surface stations in population centres, but population centres are scarce. For example, in Raja-Jooseppi and Salla in the north, diesel fuel and gasoline can be purchased at the border crossing from East Oil's pumps on the Russian side.

3.5. Travel safety instructions in the Barents region

Compiling and updating the staff's travel instructions is one of the security processes of companies and other organisations. The instructions should cover the most important issues in preparing for a trip (travel documents, insurance, health matters), security issues that need to be considered during the trip (transportation, travel, lodging, money) and instructions in case of a mishap (traffic accident, illness, other accident, injury, missing a ride, loss of documents, liability for damage or injury). The travel instructions should cover the above items in the case of each company and tailored to each trip/destination. More information on compiling travel instructions can be found on the foreign ministry's web pages at www.formin.fi.

Areas outside the cover of communication devices cause a security risk on the road. Mobile phones primarily work along main roads and in population centres. Finland's network extends some distance across the border, for example to the old parish village of Salla. Russia's main operators are Megafon, MTS and Beeline. Even along main roads there are long stretches without cover. Between Raja-Jooseppi and Murmansk mobile phones do not work along the section of road 10 km-165 km from the border, with the exception of Ylätuloma.

From Salla to Kandalaksa phones do not work from 10 km-155 km from the border, with the exception of Alakurtti.

In addition, there are extensive areas between Kandalaksa and Murmansk without mobile phone cover. The situation is even worse further on the Kola Peninsula, where for example the interior regions are totally outside the cover of the mobile phone network. However, mobile phones do work between Storskog/Borisoglebsk and Murmansk.

The most reliable mode of communication in the regions outside of cover would be a satellite phone, but it requires a permit from Russia's communications agency (Glavgossvjazznadzor) in Moscow and a declaration in customs.

Beginning from the border station at Raja-Jooseppi, the road on the Russian side is difficult to traverse for a distance of twenty kilometres. The beginning

stretch is soft sand (situation in 2007) in which a passenger car can get stuck or even be damaged. It has even been reported that the Russian traffic militia may also give a fine for driving too slowly.

Highway crime can be avoided by driving in the daytime, especially if travelling alone. Sleeping in the vehicle along the way is not recommended. Of course, hitch-hikers should not be picked up, although in the border zone it has been customary to give a border guard or customs official a ride to the nearest population centre if they ask for one. In transporting unknown people there is a danger of getting caught for being an accomplice in a drug violation, for example, if the person happens to possess drugs.

3.6 Services of foreign embassies

According to § 13 of the Council of State's regulations, the foreign ministry is responsible for looking after the interests and rights of Finns and arranging consular services and other similar official services abroad. Finland's foreign ministry is a good source of information about travel safety. The ministry's web pages contain practical instructions for travelling in Russia. Information is also categorised by region in Russia. The contact information of the nearest Finnish embassy should be kept in a notebook and saved in a mobile phone.

Finland's foreign embassies are there to help Finnish citizens who are in trouble for the following reasons:

- lost passport or other document
- lost money
- illness or accident
- travel insurance issues
- arrest or imprisonment
- death
- evacuation assistance in case of a major accident or crisis
- acquiring and disseminating information about major accidents.

In escaping from a crisis (e.g. a major accident, a large fire), often it is not possible to take along a passport, money or travel tickets. The local embassy will assist in transferring money from Finland for the purchase of a passport and tickets. The money is either transferred from the person's own account or deposited by someone named by the person via the ministry and the embassy or a commercial currency transferral agency. If this is not possible the person may be given funds to cover travel expenses to get home on the basis of a repayment note. Thus, unless he/she has valid travel insurance that covers such expenses, as a rule the person him/herself has to pay the expense of getting home. If necessary, the local Finnish embassy and the ministry will assist in arranging the trip back home. The need to evacuate a crisis area is decided by the authorities.

The foreign ministry has a text message service that sends brief situation bulletins about the security situations in different countries. Text messages can also be used to acquire Finnish foreign embassies' contact information. It is recommendable to send travel notices by text message service to make it easier for the foreign ministry or foreign embassy to contact the person and travel companion in case a crisis suddenly occurs. Also Finns living abroad permanently can send a travel notice.

The number of the text message service is 16 358, and it works with DNA, Elisa and TeliaSonera connections. With other connections – also foreign – the number is +358 400 358 300 (source: www.formin.fi).

Murmansk has both Norwegian and Finnish foreign embassies. It is recommendable to save their number in a mobile phone and write them in a separate notebook:

Finland's St. Petersburg consulate general, Murmansk office
Ulitsa Karla Marksa 25A, Murmansk
Tel. +7 8152 44 53 82
E-mail: sanomat.msk@formin.fi

Consul on call for emergency situations concerning Finns (24 hr)
Tel. +358 9 160 555 51, mobile +7 (8) 921 272 50 95, +7 (8) 921 272 50 96

Finland's St. Petersburg consulate general on-call number (24 hr)
Tel. +7 (812) 967 37 82
The St. Petersburg consulate general's other numbers are
279 0482, 272 8747, 272 2082, 279 1102.

For more information about Finland's diplomatic embassies in Russia, in Finnish and Russian, see www.finland.org.ru.

Norway's royal consulate general's office and Sweden's honorary consul
Ulitsa Sofii Perovskoi 5, 183038 Murmansk
Tel. +7 (8152) 40 06 00 (24 hr)

If an accident, terrorist strike or other crime, natural catastrophe or other similar event takes place abroad in which Finns are involved or targeted, the foreign ministry begins to take measures to solve the situation and assist the Finns. According to international law, the authorities of the country in question are responsible for the safety of both their own citizens and foreigners visiting their territory. Based on co-operation between Scandinavian and European consulates, Finns have the right to receive consular assistance from an embassy of another Scandinavian or EU country if Finland does not have an embassy in said country.

It's good to remember that, according to the Package Tour Act (1070/1994), the trip organiser is primarily responsible for arranging travellers' medical care or premature return, solving a crime or accident and other necessary measures. The Package Tour Act primarily applies to ordinary mass tourism.

3.7 Travel restrictions

Russia has begun to take a stricter attitude towards people travelling in regions governed by the new Border Zone Act passed at the end of 2006. The name of the border zone locality where a person is staying must appear on the visa. On the Kola Peninsula the new Border Zone Act has resulted in measures in monitoring foreigners. As an example, the Russian Federation's security service FSB invoke the new Border Zone Act in deporting a Norwegian person from the city of Nikkeli on 13.3.2007. According to public information, the person's visa did not mention the city of Nikkeli. Practical interpretation of the border zone statute is still unclear in mid-2007. The current situation should be checked on the Russian embassy's pages (www.rusembassy.fi).

The border zone statute awakens discussion especially among tourism companies. According to the Murmansk region's tourism committee, negotiations with the defence administration may promote more freedom to travel in certain regulated localities. Tourism has potential in the Murmansk region. In 2006 the number of customers of Murmansk's tourism companies was 26,500, of which 13,000 were foreigners. There were 25 % more customers than in 2005. Tax income amounted to 30.5 million roubles, or twice the amount of the previous year.

Foreigners' travel restrictions in closed military city areas should be taken seriously. Closed military cities include Severomorsk, Zaozersk, Poljarnyi, Snezhnogorsk and Skalistyi on the northern coast of the Kola Peninsula. Foreigners must have a permit to travel in these areas.

Even though one doesn't travel in a closed military city, gathering location data and information about natural resources with a GPS or other device is considered questionable even though gathering is only linked to scientific or commercial activity. It is permissible to bring a GPS device to Russia, but using it in a way that appears to endanger Russia's state security may result in confiscation of the device or possibly also an arrest.

According to the Russian government's decree effective in 2002 (11.10.2002, no. 754), a permit is needed to travel in the following areas and sites:

1. Russian Federation's closed regional areas (abbreviated ZATO)
2. Areas where foreigners' travel is otherwise restricted
3. Areas in a state of emergency or a state of war
4. Areas with special conditions due to risk of infection and poisoning
5. Closed military lodging areas
6. Areas with anti-terrorist operations
7. Environmental disaster areas
8. Border zones
9. Russian Federation's defence administration sites and organisations
10. Sites where public authorities work with secret information
11. Other areas, organisations and sites where Russian citizens need a permit to travel.

According to the situation in 2007, foreigners have limited access to the following areas in the Russian Federation:

1. Kamtshatka area: part of Kamtshatka is off-limits along the line formed by Ivashka - Voyampolka – Klychevskaja Sopka Volcano – Sivutshi Peninsula (except for the southern slopes of the volcano, the mentioned population centres and a 20 km-wide zone along the east coast of the peninsula);
2. Kalygir Peninsula – Koryaki and the motorway Koryaki - Jelizhovo - Termalniy - Mutnovskaja Sopka Volcano – Vhodnoi Peninsula (except for the cities of Petropavlovsk-Kamtshatsky, Jelizovo and the population centres of Paratunka and Termalniy the motorway connecting them);
3. Habarovsk area: Komsomolsk on the Amur;
4. Primor area: Russky Island; 20 km-wide coastal zone is the sector Cheyrek Skala - Cape Yuzhny;
5. Part of the coastal zone bounded in the east by the Livadia-Anisimovka line and in the north by the Anisimovka - Shokotovo railway (except for the railway and the mentioned population centres);
6. Krasnojarsk area: Taimyr (Dolgano-Nenets) autonomous area – the area bounded by Polovinnoye - Kazantsevo - Messoyakha – Maduika Lake – Dyupkun (except for the harbours of Dudinka, Igarka and the Jenisei ship route);
7. Orenburg area: the area south of the Orenburg - Ilek motorway, bounded in the southwest and east by the Ilek River and the Chingirtau - Sol-Iletsk - Orenburg railway (except for the mentioned population centres, the motorway and the railway);

8. Nizhnyi Novgorod area: the area bounded by Pervomaisky - Purekh - Chistoye - Krasnaya Gorka - Volodarsk - Dzerzhinsk - Pervomaisky (except for the mentioned population centres). Transit is permitted along the railway and along the Gorokhovets - Nizhny Novgorod motorway;

9. The area bounded in the south by the boundary of the area and the river Moksha, Sumorieve - Bakhtyzine - Sarminsky Maidan - Naryshkino - Alamasovo-Satis - Yakovlevka - Bereshchino- Zhegalovo motorway in the Mordva Republic (exc. population centres, Moksha River and the motorway);

10. Mordva Republic: the area bounded in the north by the border of the republic and the Moksha River and the Stary Gorod - Russkoe Karaevo - Zhegalovo - Bereshchino line (except for the mentioned population centres and the motorway);

11. Murmansk region and the Karelian Republic: a 10 km-wide zone along the shore of the Kola Peninsula from Krestovy Peninsula to river Voronya and west from Voronja, bounded in the south and west by the Tumanny - Kola motorway, the Kola – Petsamo railway and Petsamo - Shchel (except for the mentioned population centres, the motorway, the railway, the city of Murmansk, and transit by railway and motor vehicle from Kola and transit along the Zapoljarny - Kola - Murmansk motorway). A kilometre-wide coastal zone in the Kandalaksa Bay area bounded by Kochinny Peninsula – Titov Peninsula in the west and Nosok Peninsula – Sharapov Peninsula in the east;

12. Archangel region and the Komi Republic: a 25 km-wide coastal zone from Primorye District west from the North Dvina River to Letny Navolok; a 50 km-wide zone along the railway in the Archangelsk - Shalakusha sector (except for Archangel and Novodvinsk and transit by railway and motorway), and the area east of the Emtsa-Shalakusha line towards Verkholeodka - Seltso – Pogost. Also the area bounded by Khalmer - Yu - Yary - Ust-Kara - Karataika (except for the mentioned population centres); from Svyatoi Nos Peninsula – Indiga River - Sula River - Kotkino - Nelmin Nos (except for the population centres and rivers); part of the Kanin Nos Peninsula and the area within a 10 km radius;

13. Novaya Zemlya Islands from the Russkaya Gavan Bay - Cape Midden-dorf line south;

14. Sverdlovsk area: part of the area west of the Nizhny Tagil - Ivdel railway bounded by the Ivdel River in the north and the Kushva - Serebryanka line in the south (except for the mentioned railway and population centres);

15. Part of the Nevyansk and Kirovgrad Districts bounded by the Verkh-Neivinsk - Kalinov - Murzinka - Belorechka - Meovo-Rudyanka - Verkh-Neivinsk line;

16. Tsheljabinsk area: the area bounded by the Kyshtym - Kasli - Tyubuk - Mauk -Filippovka line and Kosmakovo, Sysert District, Sverdlovsk region - Tyubuk - Karagaikul - Argayash - Kyshtym (except for the mentioned population centres);

17. Part of the Katav-Ivanov District bounded by the Vasilovka - Pervukha – Meseda - Yekaterinovka - Polovinka – Sovkhozny line;

18. Leningrad area: the islands in the Gulf of Finland, a 20 km-wide coastal zone from the Narva River to the population centre of Malaya Izhora;

19. Moscow area: Part of the Odintsovo District bounded by the Uspenskoye - Zhavoronki - Odintsovo – Barvikha line; part of the Balashikha District bounded by the Nikolskoye - Trubetskoye - Balashikha - Kuchino - Tomilino line to the west (except for the Gorky motorway); part of the Mytishchi District bounded by the Moscow ring road and the Nagornoye state farm - Borodino - Volkovo - Perlovka line to the south (except for the mentioned population centres and the motorway); part of the Solnechnogorsk District bounded by the Pyatnitskoye motorway and the Korostovo – Podolino - Brekhovo line to the southwest (except for the mentioned population centres and the Pyatnitskoye motorway); part of the Podolsk District bounded by the Simferopol motorway and the Altukhovo - Romantsevo - Meshcherskoye - Stolbovaya line to the west (except for the mentioned population centres and the Simferopol motorway); and part of the Shchelkovo District bounded by the Shchelkovo motorway and the Dolgoye-Ledovo - Oboldino - Shchitnikovo line to the southeast (except for the mentioned population centres and the Shchelkovo motorway);

20. Kaliningrad area: the city of Baltiisk (except for its eastern part) bounded in the north, east and south by the shore of Primor Bay and the Kaliningrad sea canal; in the west by the line that passes along the canal (east from Sevastopolsky), intersecting Nahimov Street, continuing to the northeast to the 2.2 marker, and from there along the road to the southeast via the 2.4 marker, intersecting the dirt road and from there to the southwest along the road to the coast and the Baltic sea base area no. 3, Baltiisk Spit and the Zelenogradsk District (except for the part of the area from the Muromskoye - Kovrovo - Romanovo - Grachevka – Otradnoye line north), part of the Guriev District to the west along the Khrabrovo - Sosnovka – Orlovka - Kaliningrad motorway (except for the mentioned population centres and the motorway), part of the Krasnoznamensk and Nesterovo Districts bounded by the Kibartai – Nesterovo - Vysokoye - Dobrovolsk - Pravdino - Pobedino motorway and the Pobedino - Shilgalyai line (except for the mentioned population centres and the motorway);

21. Entrance to accessible population centres and districts in the Kaliningrad area passes along the Kaliningrad - Ryabinovka - Zelenogradsk - Svetlogorsk railway or the Kaliningrad - Pereslavl'koye - Dubovka - Svetlogorsk motorway and the Kaliningrad - Orlovka - Muromskoye - Zelenogradsk motorway. Entrance to the Baltic sea base area no.3 happens along the Kaliningrad - Baltiysk railway or the Kaliningrad Baltiysk motorway, continuing along the Lenina, Serebryanskaya roads and the lower Baltiysk motorway;

22. Volgograd area: part of the Pallasovka District bounded in the north and east by the 45 km point from the Mayak Oktyabrya population centre north and the 67 km point from the Otkonny population centre north and the 20 km point from the Otkonny population centre south and the northern end of Botul Lake;

23. Astrakhan area: east along the Volzhsky - Akhtubinsk - Kharabali – Akkol railway (except the railway);

24. Tshukotka autonomous area;

25. Jamalo-Nenetsia autonomous area: the area bounded by the Ust-Kara - Aksarka - Kholm - Vyngapurovsky - Khalyasaway – Tibeisale line, the bank of the Taz River, along the Tax Gulf and Ob Gulf waterline, the Malygin Inlet, the Kara Sea and Baidaratsky Bay (except for the population centre of Ust-Kara and the ship channel along the Ob River). (Source: VISTA Foreign Business Support)

Today the areas that contain travel restrictions are marked quite clearly in Russia, so there should be no possibility of erring. In planning trips to the above-mentioned places the areas with travel restrictions should be determined on maps beforehand.

3.8 Preparing for a traffic accident

The question of travel safety steps into the picture fully upon crossing the border to the Russian side. Travelling on a business trip or as a tourist in itself is an action that is not without risk in the Barents region. Even traffic regulations are not fully compatible with customary practice in Finland. One classic reminder is that a driver in a traffic circle must yield the right of way. Regarding alcohol, the principle of zero tolerance does not apply. Changes in the Russian Federation's legislation on administrative offences, which are taking effect in phases starting from the end of July 2007, specify the minimum limit in Russia as 0.3 grams of pure ethyl alcohol per litre of blood or 0.15 milligrams per litre of exhaled air (paragraph 27.12). The revision of the law allows the traffic militia to take breath tests of drivers on the road. The driver has the right to demand a test at a health care centre if he/she does not trust the test conducted on the road. According to the same paragraph, allow-

ing someone under the influence of alcohol to drive is also punishable. The changes in legislation regarding administrative offences also bring with them changes in the penalties for speeding, prohibition of the use of a mobile phone while driving (without a hands free system) and mandatory wearing of seatbelts.

Preparing for a traffic accident is a necessary part of traffic safety planning. Different possible situations should be gone over in one's mind already before the trip. The risks of road traffic must not be underestimated. Traffic causes perhaps the most significant serious risks for travel in Russia. Traffic signs and information signs are not used in abundance in Russia, at least along longer stretches of road. Seatbelts are not used as much as they are in Finland, either. Traffic on roads near the Finnish border is not very busy or fast-moving, but the risk of an accident increases, for example when meeting large lorries on the winding roads among the fells in the Kola Peninsula. The winter driving conditions between Borisoglebsk and Murmansk are difficult, which causes an additional risk for travel. Military vehicles on the roads may also cause dangerous situations.

In case of a traffic accident on the Russian side:

- Help the victims as well as you can and if necessary, call for help (emergency numbers: ambulance: 03, near the Finnish border try calling 112).
- Place a warning triangle on the road if the accident vehicles can endanger others on the road.
- In all situations, call the traffic militia GIBDD (emergency number 02).
- The Murmansk region's rescue centre is on call 24 hr, tel. +7 8152 250 166. They also have a helicopter and an ambulance unit.
- Report the accident to the Finnish embassy and ask for instructions.
- Also report the accident to your own contact person in Finland and the Russian party waiting for you at your destination.
- Do not disturb the tracks of the accidents.
- The militia will examine the accident site: just in case, also take photographs of the site from different angles and of the licence plates of all involved parties yourself.
- Record the names and insurance companies of the involved parties on an insurance form (a Russian version of which must always be along).
- Possible interrogations are done by the traffic militia.
- If you do not understand the Russian report written by the militia, it is absolutely necessary to write in Finnish that you do not understand the content of the report before signing it.
- If your vehicle cannot be driven, ask the traffic militia or consulate which repair shop they recommend.
- Obtain a copy of the militia's report as soon as it is completed; the insurance company needs it.

About 700 people a year are killed in traffic accidents in the Barents region, of which 90 % in the Russian parts of the region. The area's challenges include long distances, varying road conditions, freezing temperatures and poor mobile phone cover in some areas on the Russian side. Luckily, serious traffic accidents involving Western travellers have been avoided. The Russian traffic militia does not know of any fatalities among Finns or other Scandinavians in the Murmansk region in recent years (situation in June 2007).

In rural areas it is possible to see cattle walking in the middle of the road or crossing the road at all hours of the day. Road repair jobs sites may be poorly marked and abandoned vehicles may lie in even very dangerous places. Warning signs, road work signs or blinking lights have not necessarily been installed, so dangerous situations may become serious at night. Bicycles rarely have lamps, but neither is it a given that both headlamps of motor vehicles are functional. It is worth being prepared to stop suddenly at any time. Road signs are inadequate and written with Cyrillic letters. Thus the route should be memorised from a map before the trip. If you do not understand Russian, it would also be good to become familiar with the Cyrillic alphabet before the trip. Learning the alphabet is also a security issue, since it is easier to explain one's location to outsiders. The doors of the vehicle should be kept locked while driving through large population centres (market squares, market events, city centres).

Photo: Pekka Iivari



Russian drivers use lights sparingly. The brakes and winter tires of old Russian vehicles may also be in poor condition. On the other hand, Russians driving in Finland have noticed the Finns' tendency to drive over the speed limit on Finnish roads. The author of this booklet has heard about this from, among others, the chauffeurs of groups of Russian officials visiting Lapland. In Russia fines are always paid in a bank. The militia do not have the right to demand payment in cash.

Russia does not yet have a common emergency number, but plans for one do exist. In Finland the police, ambulance and fire department are summoned by calling 112. In addition, a person can get along in Finland by using English. It is difficult to get along with English in Russian emergency numbers. An English militia phone number can be found in St. Petersburg.

The traffic militia's investigation points are located in Alakurtti, Ylätuloma and Petsamo. If a traffic accident happens between a customs station and one of these population centres, the investigation is conducted at the population centre. The traffic militia and local business services can provide information about towing services.

The traffic militia (abbreviated GIBDD) can also be contacted at the following places:

- City of Murmansk GIBDD, ulitsa Gerojev Severomortsev building 63, apartment 24, Murmansk, tel. +7 (8152) 421833

Hospitals in the Murmansk region have been instructed to immediately inform the Murmansk office of the Finnish St. Petersburg consulate general about Finnish emergency cases brought to the hospital. The Murmansk office of the Finnish St. Petersburg consulate general will assist in finding an interpreter. Most population centres have doctor's services and their blood products are safe and their needles are sterile. Payment for doctor's services is usually paid in cash. Receipts should be saved for possible compensation by an insurance company. The receipts also indicate the reason for a possible stay beyond the period of validity of a visa. In 2005 the provincial government of Lapland published a traveller's pocket guide containing practical hints for travellers in the Murmansk region and a road map of the Murmansk region (Lapland provincial government 2005). Below is the contact information of some health care services:

Murmansk City Hospital
Ulitsa Volodarskogo 18
Tel. +7 (8152) 45 10 71, 45 19 39

Kandalaksa District Hospital
Ulitsa Tshkalova 54
Tel. +7 (81533) 7 12 33

Ambulance service in Alakurtti: address 184060, Alakurtti, Danilova street 7,
Tel. +7 (81533) 52395

Alakurtti Military Hospital: 184060 Alakurtti, Tel. +7 (81533) 52861

Alakurtti Apothecary: address 184060 Alakurtti, Danilova street 14,
Tel. +7 (81533) 52233

Murmansk Region Rescue Centre (24 hr); helicopter and ambulance unit
Tel. +7 (8152) 25 01 66, 25 03 12

In acute cases help can be summoned by directly calling the international emergency service, SOS International in Denmark, which also provides daily service in Finnish. If necessary, it will arrange help on site and transportation home and also help in contacts with a Russian hospital if the insurance company has made an agreement with SOS.

SOS International (24 hr), Tel. +45 70 10 50 54
MedFlight Finland (24 hr), Tel. +358 (0)400 463 875

It is recommendable for travellers to keep a health card in their passport or pocket. The health card should show possible illnesses, medication and blood type (see the appendix at the end of this booklet). The hospital staff do not necessarily know where to report a patient, and the health card helps in that case, also.

Rarely does it come to mind that a snake may bite on a hunting safari or a visit to a residential area. Snakebites have happened near Kandalaksa in the summer of 2006, for example (source: euroarctic.com, 20.7.2006). In such a case, also, it is necessary to be prepared to use helicopter services.

The extent and price of insurance coverage can be found on Rosgosstrak's pages at www.rgs.ru, or Ingonord's pages at www.ingonord.com

Enter the following information in a mobile phone and in case it gets lost, also in a separate notebook:

- Family member or other contact person who you will notify of the progress of your trip;
- Contact info of the receiving person, hotel or company;
- ICE code; contact information of the nearest contact person;
- The numbers of the above-mentioned foreign ministry and consulate;
- Contact information of the border crossing;
- Russian emergency numbers;
- Direct numbers of the traffic militia;

- Loss of a credit card should be reported in Finland; tel. +358 20 333

4 SAFE LIVING

4.1 Registering

In the section on travel safety we also mentioned issues that are important from the standpoint of living, such as the contact information of hospitals. Living starts with arrival at a hotel or other lodging. The paperwork associated with registering in a locality is part of ensuring safe living.

People residing, living and visiting in Russia are regulated by different registration procedures that depend on the length of stay. If a person is on a short visit of less than three days, the hotel stamps the person's entry card as proof of registration (see appendix). A stay of more than three days elsewhere than at a hotel requires registration on one's own initiative. Independent residence and living require registration with the passport and visa department of the internal affairs administration. According to a law that became effective in January 2007, a foreigner must submit his/her registration notice to the passport and visa department through his/her employer, hotel, landlord (landlord's registration form enclosed) or other inviter each time he/she leaves the country. He/she must re-register upon returning to Russia. Re-registration is not necessary if the absence is less than three days (Russian Federation law 25.7.2002).

Upon arriving in Russia a person must register within three workdays, and upon leaving notification must be made within two workdays. A foreigner living in Russia who moves to another locality must re-register there. If an employer neglects to observe the notification obligation - even in such a case where an employee just leaves the city - a stiff fine may follow. You should make sure the hotel receives foreigners, since the additional bureaucracy brought about by the new law results in more work for hotels. You should keep your passport and entry card with you when you leave the hotel to travel in the city. The militia are authorised to check documents on the street. You should be very careful with your documents if you have with you your original passport instead of a copy.

It's better not to lose your passport. But if that should happen, do as follows: Call the Finnish consulate and report what happened. Go to the nearest militia station and show a copy of the passport and other identification you may have with you. The militia will make a "*spravka*", which is a temporary certificate verifying the loss of the passport. If you encounter problems at this stage, ask them to call the consulate. Verify that you have a plane ticket (if you are flying). Obtain three passport photos of yourself. Go to the consulate to get a new passport. Bring the papers to a travel agency, preferably the one where you possibly registered your visa or through which you obtained your visa. You may be fined by the immigration authorities, but you'll get your visa within a few days.

Long-term (over three-day) residence in a rented apartment in a locality requires registration with the passport and visa department. Below is a landlord's form, which must be submitted to the passport and visa department if you reside in private lodging in Murmansk:

В ПВУ ГУВД г. Мурманск (Murmansk militia department)

От

Паспорт серии (Passport, series) _____ № _____

Выдан (granted) _____ « _____ »

_____ г. проживающего (ей) по адресу: г.

Мурманск

(who lives in Murmansk at the following address)

Я (I), _____, являясь

ответственным квартиросъемщиком / собственником

(apartment possessor/owner)(ненужное зачеркнуть), согласен(на)

зарегистрировать по месту пребывания до (have agreed to register at my residence by « _____ »

_____ 200__ года на моей жилплощади по вышеуказанному адресу гражданина (person)

_____,
_____ г.р., паспорт (passport) № _____, виза (visa)

№ _____

гражданство (nationality), Ф.И.О. (name), число, месяц, год рождения

(date of birth), № паспорта, № визы

подпись (signature)

Все совершеннолетние граждане, зарегистрированные по месту жительства в данной квартире, с регистрацией по месту пребывания иностранного гражданина согласны (everyone marked at said address have agreed):

подпись (signature)

подпись (signature)

подпись (signature)

Подписи граждан, указанных в заявлении (registree's signature)

Удостоверяю (witness)

Должность, фамилия и подпись должностного лица ДЭЗ (РЭУ)

« _____ » _____ 200__ г.

1 Печать ДЭЗ (РЭУ)

The security preparations regarding lodging depend on the place chosen for lodging. A hotel is the easiest alternative from the standpoint of lodging security. Of course, there are many kinds of hotels. Hotel security is usually han-

dled by the hotel's own security department, whose service may have been purchased from an external security company. The level of security of a hotel in Russia with an international status is equivalent to that of a Western hotel. To make it easier to assess the security and quality level of hotels, an international star classification system will be implemented in 2007.

When lodging at a hotel, it is recommendable to store valuables in a safe arranged by the hotel, which can only be opened against a separate receipt. Hotels and other public places pose a challenge regarding information security (e.g. computer and fax use), which is explained in more detail in the section on information security. Leaving a bag unattended in a hotel lobby may trigger a bomb alarm. The lost and found service works well at some hotels. For example, lost clothing can be found at Hotel Poljarnye Zori (Murmansk) by asking at the reception desk. The reputation of hotels is well known by companies and travellers who have been in the area long.

4.2 Living and residing

In general, it is safe to live in Russia. For example, the staff of Finnish embassies live in the locality of their post and no security threats out of the ordinary have appeared. Entrepreneurs and private individuals also live in the northwestern part of Russia. People living in a locality take the same security issues into consideration as they do in Finland. Essential issues from the standpoint of security are rental or ownership apartment arrangements, neighbours, apartment location, technical security solutions and the resident's own behaviour. The last-mentioned issue can never be overemphasised. Sad to say, but both Finnish and Russian law enforcement authorities well know that a significant portion of Finns who are victims of crime are in some degree of intoxication.

In renting an apartment and making a rental agreement, the same rules apply as in Finland. The agreement should contain the renter's and rentee's data, a description of the property belonging to the apartment, the monthly rent, and electricity, water and gas payments. The agreement should also specify questions of responsibility if water leaks to the lower floors or from the upper floors into the apartment. Sometimes rent agreements require the signatures of everyone living in the apartment. Renting is a relatively risk-free form of living. Also when renting, you must remember to insure the apartment and your own property. The safety of living and residing is increased if the traveller in Russia and the person going abroad from there regularly informs a family member or some other person about the starting and ending dates of his/her travels. A text message is the least expensive and often most efficient way to inform.

Living in Russia takes place on the basis of a temporary or permanent residence permit. A temporary residence permit is granted for three years. The authorities should make a decision on a residence permit within six months of

the application date. In considering whether to grant a temporary permit, a quota specified by the government of the Federation is taken into account. Regardless of the quota, a temporary residence permit may be granted to:

1. a person who was born in the Soviet Union and has been a Soviet citizen, or a person who was born in Russia;
2. a person who is declared to be under guardianship and whose child is a citizen of Russia;
3. a person who has at least one parent under guardianship and said parent is a Russian citizen;
4. a person who is married to a Russian citizen living in Russia;
5. a person who invests in Russia.

A temporary residence permit is requested for a period of six months either in the receiving state or from a Russian foreign embassy. An application for a temporary residence permit is filled out in the receiving state during the visa's period of validity. When the permit is granted, the visa's period of validity is extended. In considering whether to grant a temporary residence permit the local UVD office is required to request statements concerning the residence permit from the security service, the execution authority (*pristava*), the tax office, the social service and health care officials, the immigrant service and other possible authorities, who must respond to the request within two months. A residence permit may be denied if the person has been convicted of a serious crime or is suspected of planning one. The application may also be rejected if the person has been guilty of breaking the residence regulations, presenting false information in the application, suffers from a serious infectious disease or cannot prove the ability to arrange his/her own or family members' maintenance.

A person with a temporary residence permit is allowed to work in Russia. If a foreigner wants to leave the country, he/she must apply for a departure visa. A person with a temporary residence permit cannot change his/her locality of residence or work outside the locality or area of residence. When a foreigner has lived in Russia with a temporary residence permit at least one year, he/she can apply for a permanent residence permit for five years. A permanent residence permit can be extended another five years. A person with a permanent residence permit can travel to and from Russia without a visa.

4.3 Home and family security

If a company and its staff intends to be in Russia for a longer period, a person in the company should be appointed as an interim security contact person already before the move to Russia is made. This person could be the employee who will be appointed the head of security of the company that will operate at the site, for example. This person will then observe the security situation in the locality and provide Finns living in the area up-to-date secu-

rity information. In addition he/she could act as a contact person in the direction of that area's authorities and security companies.

Living in the locality lessens the risks related to travel safety, but requires initiative in ensuring personal safety and the security of one's family and protection of property. It is recommendable to provide the nearest Finnish embassy with the up-to-date contact information and addresses of Finns living in the area. To ensure their safety in case of a crisis, the embassies can maintain a register of Finns living in the country (Consular service law, § 36). Registration with the embassy is entirely voluntary, but highly recommended in crisis-prone countries and regions. The main crisis-prone areas in Russia are the Caucasus region and the region near Central Asia. In crisis areas it is also possible to register with other embassies of the EU area. All the Finnish embassies in world have readiness and evacuation plans in case of a crisis, and the plans are updated as necessary. The readiness plans map the crisis situations in the country in question and list necessary operating instructions.

A person who is commissioned to work abroad probably first lives in a hotel or tourist lodging, but as he/she becomes established, a rental or ownership apartment may also come into question. Among the basic issues of home security and safe living are the building's location (peacefulness of the section of city, nearby and offices and buildings) and structural security (exterior doors, windows, lighting, locks, fire safety). The apartment's functional security includes healthfulness of living (traffic, pollution, moisture, heat), the type of immediate neighbours (obscure travellers, quiet elderly residents) and the impact of possible natural catastrophes.

Traffic is the greatest risk, both when travelling and when living in a locality. Fire safety is also a factor that requires special attention in day-to-day living. The apartment must have its own fire detectors. Exit routes and gathering places must be familiar so that actions are automatic if such a situation arises. Fire safety is one of the most important aspects of safe living in Russia. For example, the number of fire deaths (and traffic fatalities) per year in the Murmansk region, with a little less than one million inhabitants, is of the same magnitude as it is in all of Finland.

Important emergency phone numbers necessary in day-to-day living are 01 (fire department), 02 (militia) and 03 (ambulance). Gas-related accidents should be reported to the number 04 (works at least in St. Petersburg). In Murmansk, questions related to public utility services can be asked from the number 051. Business is taken care of in Russian. The militia in St. Petersburg has special phone numbers for foreigners, +7 812 164 9787 and +7 812 326 9696, where business can be taken care of in English.

In St. Petersburg, the Euromed Clinic is recommended in cases of illness and emergencies. The address is Suvorovsky prospekt 60, tel. +7 812 327 0301.

The clinic has agreements with EMA Group and Euroflight, and the clinic accepts Scandinavian and European insurances. The phone numbers of Vyborg Central Hospital are +7 278 24 552 and +7 278 23 915.

When selecting an apartment, in addition to determining its ownership basis, the following security issues should be taken into consideration:

- Neighbours (nationality, behaviour, attitude towards security);
- Lighting in hallways and outdoor areas;
- Possibility to park a car in a closed courtyard;
- If a separate garage is located far away, how is transportation to the apartment arranged;
- Emergency exits and cellars and their condition;
- Fences and other outdoor protection (also lockable exits);
- Fire safety equipment also in the hallways;
- Security of attics and cellars and possible undesired occupants;
- Condition and sturdiness of doors and locks;
- Condition and locks of windows and balconies;
- An apartment off the ground floor is always better (2nd-4th floor), but not too high (fire safety);
- Location of the apartment with respect to the workplace, to avoid having to travel through questionable neighbourhoods;
- Evacuation plans and instructions, their currentness and visibility.

Studies have indicated (e.g. Aromaa & Lehti 2001, 64) that Finns have relied mainly on investing in the security of doors and locks to raise the level of security in living in Russia. Rental apartments generally do not have particular problems related to safe living. Security electronics are still quite rarely installed, although fire safety-related devices are becoming more common. Questions of the street and leisure time security of company employees in Russia cause more headaches than do those related to safe living (Aromaa & Lehti 2001, 65).

Alertness based on common sense, avoiding sections of the city with a bad reputation and obscure friendships, and sensible use of alcohol are the most important ways to avoid ordinary street crime. Normally, living in Russia does not require significant investments in security. For example, use of gas weapons or bodyguards is rare among Finns (Aromaa & Lehti 2001, 66 – 67). In this conjunction it is good to remember that, according to Russia's crime codex, carrying so-called cold weapons (*holodnoje oruzhije*, sheath knives, ordinary knives and sabres) is forbidden if a person does not have a permit to carry a hunting weapon or the cold weapon is not part of the person's national costume. According to the Crime Act, illegal purchase and possession of gas weapons is not a penal act, but according to the Weapons Act, a licence is required to purchase a gas sprayer. Nevertheless, certain licence-free gas weapons for self-defence are sold in Russia.



The militia administration of the Murmansk region (UVD) has published instructions with which residents can prevent on unwanted entry into a residence or burglary, and thereby improve the safety of day-to-day living. Although the following list contains things that are obvious to many, there is reason to consider the recommendations of the local militia administration.

The militia's guidelines for protecting a residence are:

1. Burglar alarms with motion detectors (crime detection system in Finland);
2. Do not open the door for strangers;
3. Install a peephole;
4. Do say you are home alone;
5. Do not talk about your travel plans;
6. Leave a light on when you leave;
7. Lock the windows;
8. Replace the locks if you've just moved in or if someone has lived there before you;
9. Arrange to have a neighbour or friend check the mail in the box;
10. Door chains are enough; install a gas sprayer just inside the door that you can use if someone attempts to break in. Obtain a permit for the sprayer from the militia. Some models do not require a permit;
11. In an emergency, call for help, attract attention to yourself;

In planning a burglary, burglars may fish for important information through the (fixed) home, door or office phone.

12. Do not answer questions posed by people you don't know;
13. Do not tell an answering machine your name, phone number or current location. The necessity of having an answering machine at all should be considered;
14. Obtain a phone line meter. With it you can determine if there is a stranger on the line;
15. Enter quick-select numbers for the militia, ambulance and fire department in your phone;

Safety in a vehicle is just as important as it is at home or the office. The militia's guidelines for improving vehicle security include the following measures:

16. Obtain a gas sprayer for your car and a permit from the militia;
17. Be careful if there are strange objects inside or outside the car. Do not get in the car, instead report it to the militia;
18. Do not leave valuable items (mobile phone, sunglasses, computer, etc.) visible;
19. Keep the car key separate from other keys, otherwise you may lose all your valuable keys at once;
20. Do not park the car in an obscure place or near a doubtful-looking group of people;
21. Keep your mobile phone at hand;
22. In case of an accident do not begin arguing with the other party and do not hand over any documents. If necessary, ask a bypassing driver to report the accident to the nearest militia guard post;
23. Fill the tank even though it's only half empty;
24. Do not stop to relieve yourself in random, lonely places;
25. If you think you are being followed, drive to a militia station;

The following general guidelines improve your personal safety:

26. Be careful when leaving a bank or store. A thief imagines that just then you have money or goods;
27. Keep one hand free of baggage;
28. Avoid dark sidewalks and alleys;
29. Avoid using a lift with a stranger. Press the call button (VYZOV) if the situation looks threatening;
30. Be especially careful when entering a building (stairway), without lighting. Putting lamps out is a common tactic for criminals;

A person accustomed to freely using a mobile phone in the West may be surprised by the fact that mobile phones are still desired items among pick-

pockets. Because it has monetary value and is easy to sell, a mobile phone may be snatched from your hand or bag on the street. To improve mobile phone security, the militia give the following instructions:

31. Keep your mobile shielded, for example in your vest pocket, when travelling in public places, on public transport, at squares, etc.;
32. Avoid using the phone in a crowd. See if there are any people nearby when you talk on the phone. Most phones are lost because of carelessness;
33. If the mobile phone is in a case worn around your neck, keep the case under your coat or shirt;
34. Save the serial number of your phone as follows: Press *#06#. A 15-digit code will be displayed. If you lose the phone, report this code to have the phone closed;
35. In case of theft, report it to the nearest militia or guard;

The above-mentioned also applies in part to laptop computer security. The militia's guidelines also take personal physical protection into consideration:

36. Choose a suitable mode of self-defence for yourself; it may be a burglar alarm in the car and sprayers at home;
37. Obtain training in the use of gas weapons. As a rule, gas weapons require a permit in Russia. In addition you must observe rules regarding storage of the weapons at home.

Several other security measures can be added the militia's guidelines presented above, for example:

- Verify the intentions and papers of anyone presenting themselves as a policeman or plumber or someone similar. Call the firm that sent them;
- Take note of monitoring activity: are questions asked about yourself or your family, are you followed by car or is a strange vehicle like a van parked for a long time near your residence;
- Be wary about mail deliveries, packages and letters from unexpected companies or persons or especially if they have no return address;
- Obtain phones with secret numbers for all family members so the whole family can be contacted quickly.

Any monitoring of a person, residence or vehicle should be discovered by observing the surroundings. Physical monitoring by criminals or state security organisations indicates that some sort of operation is being planned for the future. Monitoring by criminals must be taken very seriously. There are methods for identifying and revealing monitoring on the street. They should be discussed with a local security company.

Ensuring personal safety is a more demanding task for a family with children. Co-operation between the home and school is very important. Choose a school and a nursery with a good reputation that is recommended by other foreigners or a trusted friend. Co-operation between the home and school includes arranging the children's transportation and agreeing on who accompanies them. Family members should transport the children to and from school. Otherwise their escorting should be arranged in some other safe way. Who will pick up the children must be settled with the teacher.

Exchanging contact information between the parents and teacher is also a basic issue. What information may be given about the children and to whom must also be settled with the school and other institutions. Leaving the children unattended, for example with their friends or at a movie theatre, is not recommended. It should be emphasised to the children that they should avoid associating with strangers. If strangers have tried to approach them, this should be reported to the school and the parents. It is very important to teach the children and family members the basic safety issues of day-to-day living. The children also need to know what to do in case of a fire.

In Russia the fact that the phone may be tapped must be taken into consideration in security issues and safe living. The Russians feel this is not only common, but also natural. One should be careful and reserved on the phone. All calls should be recordable in case a threat is given by phone. Recording devices should be installed at work and at home. Any blackmailing attempts should be immediately reported the militia department that fights against organised crime. After discussing the event with the militia, it should also be reported to the management of the security company if security services are used.

Family members should be warned not to allow strangers in the residence. Family members should not tell anyone about another member's work or present location. It is good to emphasise to the family that receiving packages or other deliveries from unknown parties is forbidden. Good relations should be maintained with the neighbours. They can well make observations about strange travellers and can provide advance warning about dubious persons who have possibly attempted burglary, threatened the children or been especially inquisitive.

One should always be wary about people who pose as officials, municipal employees, repair and maintenance persons and who suddenly appear at the home or office. The purpose of their visit must be verified from their superiors. At the office and why not at home, also, such matters should preferably be left to the care of a guard or security manager. In the case of a home search, the persons must present their names, personal identification, the names of their superiors and a search warrant. One's own lawyer, or in an emergency some other witness, must be summoned to the site.

Planned business trips or meetings should not be discussed in the presence of strangers. Neither should work matters be discussed on the phone in the presence of an outsider or stranger. The caller can call again later.

The family should also discuss the possibility of what should be done if a member is kidnapped and what phone numbers should be called in such a situation. The militia department and authority that is to be contacted in such a situation must be determined beforehand.

4.4 A few judicial issues

In Finland a juristic person has been criminally responsible since 1.9.1995, when a new chapter was added to the Penal Code (PC chapter 5). In Russia a juristic person cannot be criminally responsible (Crime codex § 19), but according to moment 2 of § 2.1 and the provisions of § 2.10 of the administrative crimes codex, a juristic person may be administratively responsible. Finland's penal code contains over 30 crimes for which a juristic person can be given a corporate fine. These crimes include bribery, welfare fraud, concealment, occupational safety offence, environmental damage and wrongful use of inside information (Koistinen 2006: 52).

According to Russia's crime codex, a person who has received foreign trade rights may become guilty of illegal exports of raw material, materials, technology, scientific and technical information and labour used in war industry. A person who has received foreign trade rights may be the director of a juristic person registered in Russia and a physical person living permanently in Russia, who has registered as a private entrepreneur in Russia. The director of an organisation may become guilty of neglecting to repatriate currency (PC § 193). The owner of director of an organisation, some other person that takes care of administrative tasks in the organisation or a private entrepreneur may become guilty concealing such funds or property owned by the organisation that are subject to taxation or payment collection. Typical of Russian legal text is that the sphere of offenders is exhaustively delimited in the essential elements of the offence. This has happened in this case, also (Koistinen 2006, 95).

Living in Russia requires a certain degree of understanding of Russian legislation. A foreigner should also know what things are acceptable on the street level and which rights and obligations are comparable with Finnish practice, for example. The Russian penal codex frees a person from criminal responsibility in the following cases, among others:

Self-defence (PC § 37)

A person can defend himself or others against an attacker if the attacker threatens with violence. In such a case the attacker can be injured. A person can defend using commensurately suitable methods if the attacker does not threaten with violence.

Everyman's right to arrest (PC § 38)

A person who has committed a crime can be injured while being arrested, when delivering him to the authorities or to prevent him from committing further crimes if arrest is otherwise not possible. The injury may not be intentionally disproportionate to the circumstances and the damage caused by the offender. A clause in Russia's penal code that causes bafflement to foreigners is that all citizens of the Federation have the right to arrest. Nevertheless, foreigners also have the right to arrest a person caught in *flagrante delicto* (red-handed). In addition to arresting after a crime is committed, it is also possible to arrest someone attempting a crime, but of course proof of the attempt is ultimately left for the court to decide. Clear-cut cases are when a person is caught in *flagrante delicto*, persons indicated by witnesses, and persons found in an apartment or other place where there are definite indications (and goods) of a crime. Someone who has escaped from a penal institution and a wanted person can also be arrested with everyman's right.

State of emergency (PC § 39)

Damage of legally protected interests is not condemnable in an extreme state of emergency, when moving a direct threat to a person himself or another person if the threat could not be moved in any other way and the caused damage is not disproportionate and intentional.

5 SECURITY OF BUSINESS OPERATION

5.1 Security culture starts from the management

At the core of all development of security is personal safety. Staff safety, customer safety and the safety of residents in the surroundings of a company are some of the most important objectives of security. Personal safety is the starting point and priority of security analyses. Customer and staff safety are basic operational issues in a business that provides customer service. Work done for the good of customer safety in Russia can not differ much from the practices of other countries. The fire safety of the building and operating facilities (customer service rooms) and other structural aspects essentially form the framework for the prerequisites for developing security. If a company provides customer service, it must also remember that other customers, their behaviour and quantity also affect customer safety.

Photo: Pekka Iivari



Security is comprised of numerous small and even a little larger factors that need to be in tune with each other. It is not enough that an organisation uses expensive video monitoring devices if it has primitive information security practices. Strong locks are meaningless if access rights are handed out carelessly. The level of security is assessed according to the weakest link in internal and external protection.

Business security issues are the responsibility of the company's management operating at the site. The company's security manager provides assistance and expertise to the management as needed. If the company's main office operating at the site is registered abroad, the branch office/subsidiary observes the security instructions of the main office. Thus, at the same time partial responsibility for security lies abroad.

In mapping security risks and preparing for risks, the company's security manager employs the locality's network of security officials and reliable security companies. Nothing prevents the company from establishing relations with the local management and headquarters of Russia's internal affairs administration UVD, rescue administration MTshS (MЧC Emercom) and security service FSB. The internal affairs administration UVD, Emercom and FSB are the most important security officials with whom a company should have good co-operation (Petrov 2007, 53). The Finnish embassy has the contact information of the most important security officials and can assist in forming relations. The company's opening ceremony offers a good opportunity to expand contacts with the authorities, although communication with the authorities has to happen already when establishing a company. It is recommendable to keep the locality's security officials informed about the company's nature, its staff and the number of foreign employees, as well as particular risks and security needs.

Supervisory authorities in the security sector:

- State fire inspection agency in Emercom (Pozharnyi nadzor)
- Vehicle inspection agency GAI (Gosavtoinspektsija)
- Ecological, technological and atomic inspection agency (Rostehnadzor), which was formed in 2004 by combining the radiation safety inspection agency (Gosatomnadzor), the industrial inspection agency (Gosgortehnadzor) and the electrical inspection agency (Gosenergonadzor)
- Sanitary-epidemiological inspection agency (Gossanepidnadzor)
- Work inspection agency (Rostrudinspektsija)
- Standardisation system inspection agency (Gosstandart)
- Ministries and central offices in their own fields; the most important agencies being Emercom, MVD, FSB, finance ministry and tax authorities
- Security supervision formed by social organisations (professional unions, political parties, media)
- General procurator's office as the highest supervisor of the implementation of official operations and security.

The staff of a foreign company is always an object of special attention in Russia. Staff members, their living habits, living and travel are noticed and scrutinised by authorities, competitors and also criminals. The tasks of authorities in Russia (tax authorities, customs, security service) include making sure residence and work permits are in order, money used in business transactions is legally obtained and camera monitoring used by companies is implemented according to good practice. A government agency possibly located on an adjoining property or in an adjacent building will probably not look

kindly on a company if its camera monitoring is perceived to also cover the neighbour's side.

An information package intended for the authorities at the least will not hinder business operation in the future. Law enforcement authorities, who nevertheless are quite influential in Russian administration, may be suspicious even though in principle they know exactly what type of operation a foreign company practices. Here the administrative culture differs considerably from what we are accustomed to. In Finland it is not customary to visit the local police station to introduce oneself. It is important to know the structure of the militia administration, because in Russia the internal affairs administration UVD, or in practice the militia organisation, is responsible for preventing ordinary and organised crime, supervision of foreigners, permit administration and supervision of security companies. Someone living in the area should also know that the UVD's passport and visa department monitors the registration of foreigners residing in the area. In addition to the militia administration, the authorities responsible for internal security and rescue operation can give instructions and regulations that affect business operation. The security service FSB is responsible for preventing espionage and serious organised crime. Russia's emergency ministry's (MЧC, EMERCOM in English) local and city departments are specialist authorities in fire fighting and rescue operation. They provide information about preparing for emergency situations, evacuation needs and readiness planning practices. The tax administration and occupational safety authorities also hold key positions from the standpoint of business operation.

Comprehensive management of risk identification and protective measures are part of a company's practical security culture that everyone in the company and organisation should internalise to the extent required by their job. There should be awareness of the various forms and causes of dangers and risks and information about them should be actively collected. Identification of dangers that may appear wherever and whenever should be practiced. Unnecessary risk-taking and dangerous situations and places should be avoided. Other people's experience should not be underestimated, and good hints should be collected. New ideas may emerge from things others have related. The objective of a security culture is to guarantee the rights and interests of employees and customers and protect property.

It must be remembered that security authorities alone cannot protect people and property. The organisation's security system is the first phase of security, which supplements the support given by public authorities. The private and public security sector forms a security system that includes different levels of public administration from municipalities to the state, a technical protection system, societal and organisational funding and resource systems, official co-operation systems, employee-level co-operation, normative documents, a medical and psychological support system and a security infrastructure (Petrov 2007, 19 – 24).

5.2 Partner selection and background checks

Many times selection of a business partner is of crucial significance to the company's success in the Russian markets. At best a good business partner, a company or person, may act as a sort of lawyer and provider of security for the Finnish business partner. At worst a partner selection may result in loss of the business operation through a company takeover or, more commonly, in the form of an economic crime, such as fraud. Finnish and other Western companies have had to solve even difficult security challenges in Russia. A common worry of Finnish companies in St. Petersburg in the 1990s was protecting themselves against extortion and the authorities' arbitrariness. In some cases a Finnish company was forced to select a certain business partner from the Russian side if the company wanted to continue operating or even existing in Russia. The possibilities of choosing a partner were limited (Aromaa & Lehti 2001, 24 – 29). Extortion was more common in St. Petersburg in the 1990s in the retail trade and construction subcontracting sectors. Wholesaling and sales of various business services were the least risky (Aromaa & Lehti 2001, 69, 93).

Fortunately, these chaotic times have been replaced by slightly more established trade practices, but it is still necessary to be careful in selecting a business partner or, say, a security company.

Finnish companies faced the following types of unfair competition in St. Petersburg in the 1990s:

- Dodging customs duties
- Dodging manufacturing and other similar taxes
- Avoiding quality norms
- Purchasing/sales cartels
- Bribing and discrimination by the authorities
- Inappropriate marketing
- Violence and property crimes
- Corporate espionage
- Pirate products
- Incorrect use of copyrights
- Underpricing

The most common forms of unfair competition were dodging customs duties corruption of authorities (Aromaa & Lehti 2001, 113).

Finnish companies' familiarity with the local area and their experience in operating there has increased over the years. Ready networks help in finding the correct persons and companies. Problems may arise in more unfamiliar areas like central and eastern Russia. Making investments in Russia without previously assured, actual undivided authority in the company being established appears to be very risky. The actual realisation of rights of ownership

and disposal based on purchased shares of a subsidiary must be verified (Aromaa & Lehti 2001, 78). Nowadays it is not recommendable to establish joint companies. Better investment protection is achieved with 100 % ownership of a company in Russia.

Checking the background of business and trade partners is still the most important way to forestall problems. As recently as the early 1990s it was difficult to obtain information on the backgrounds of customers and business partners. At that time Russia did not yet have business register, real estate information systems or credit information registers. Entrepreneurs had to rely on their own personally created information sources (Aromaa & Lehti 2001, 111). Now in the new millennium the situation looks different. Analyses of the business security in Russia are done by consulting companies, among others, from whom it is possible to order reviews and assessments of particular threats or challenges related to the crime situation in a certain locality, for example. Licensed private security companies also conduct background checks of a business partner or potential partner. Specialist companies rely on their own and public information in addition to official information, which includes crime registers maintained by the militia and tax data. Russia's tax authority's principle of publicity is comparable with Finnish practice. The tax authority publishes in the media the names of companies on the tax authority's so-called black list that have unpaid taxes or their operation has been nullified. The same information is available in Finland in the Official Journal and the Kauppalehti newspaper. Nevertheless, the tax authority in Russia is not able to monitor all business operation as efficiently as we are accustomed to in Finland. Due to the larger share of the underground economy, information that is important from the standpoint of background checks passes by the tax authority.

It is not rare in Russia for a company to receive a purchase offer from a previously unknown party that mentions only the company's name and phone (or fax) number in the letter (or fax). The names of responsible persons or contact persons may be missing completely. In such a case a background check is more than necessary. A basic check of open registers may indicate that the company has not even been registered. A certain mentality of secrecy is ingrained in Russian business culture. There is not necessarily anything wrong in a company that presents itself without names. The company may well be new or for some reason the persons behind it wish to yet remain anonymous. An open inquiry about responsible persons from the number given in the letter may cause irritation in the Russian owner/director. One has to be prepared for this. Finns naturally ask for the owner or the company's contact person in order to be sure of to whom they are talking to. This is not yet a background check. A professional background check is done in such a way that the subject of the check is not aware of the check.

The period of validity of the licence of tourism companies or security companies can be checked from the local administration. In Russia the register,

comparable to a trade register, is maintained by Gosstandard. The justice ministry's regional offices provide information about company registrations. It is possible to get quite an extensive picture of the validity of the permits and practical operation of the subject of a background check even by using various open sources. Naturally, all this should be left to a security company, for example. It is only necessary (in giving the commission) to make sure the information in at least all open registers is used in the background check. It is worth always remembering that background checks show only a momentary cross-section of the history of a person or company. Determining reliability does not guarantee a change in a person's behaviour, for example due to extortion or a change in his/her life's situation.

Russia's authorities are active collectors of information and today also providers of information. Russia's tax authorities warn about so-called one-day companies that complete one or more business transactions and then disappear without taking care of their tax obligations. The tax inspection agency conducts routine audits of companies, requiring their registration certificates and establishment documents. Sometimes it happens that a company's bank account is closed before the audit is done. This may cause problems for business partners and the company's contract-based operation.

In a security investigation procedure that inspects backgrounds, the backgrounds of both employees and partners are checked. In some cases background checks of temporary employees may be done more lightly, but correspondingly, closer attention should be paid to monitoring their work and restricting their access rights than the rights of other employees. The process of selecting the management and accountant and checking their background should be conducted especially carefully. In conjunction with the compilation of a joint business security strategy for economic life and the authorities it was discovered that only half of the companies in Finland checked the background of key persons (Ministry of Internal Affairs 2006). From the standpoint of preventing crime this inadequate background checking is an alarming phenomenon. In addition one can ask that if background checking is inadequate in Finland, is any more attention given to the issue when beginning to operate in Russia? It can be said that background checking mechanisms and sources related to operation in Russia are even more unknown issues than they are in Finland.

According to a questionnaire compiled by SVKK ry in 2005, employees were most commonly selected in Russia through Russian staffing and recruitment offices and through the state's specialised staff leasing companies. Recommendations of Russian partners, employment ads and employees of a mother company operating in Finland are also important sources (SVKK ry 2005, 64).

An extensive background check of a partner obtains reliable information about the company's (and its staff's) financial situation, professional reputa-

tion, the management's personal situation, etc. Contrary to common belief, it is possible to very extensively obtain public information that is directly beneficial in checking backgrounds. The following sources of information, among others, are available:

1. The registration authorities provide information about:
 - a) basic capital payments;
 - b) a juristic person's shares/establishing persons, their shares and basic capital;
 - c) identity of the manager and sometimes the main accountant.
2. The tax inspection agency and pension fund in the locality where a company is located provide information about:
 - a) unpaid taxes and payments to these instances and budgets;
 - b) if the partner is a bank, a possible ban on bank operation.

The tax authority's registers are in themselves already a good source of information on whether a company actually exists, whether it has a government register number, what changes have been made to the company's structure and whether the organisation has possibly been terminated. For someone who understands Russian, the Federation's Tax Inspection Service's (Federalnaja Nalogovaja Sluzhba) register, which can be found on the Internet and is open to everyone, is a good aid in checking business information. The tax authority's open register also provides information about companies' register numbers and home offices. The tax authority also maintains a register (<http://sbk.fcod.nalog.ru/disfind.do>) of so-called disqualified juristic persons, or organisations that the tax inspector does not recommend as partners. In addition, information is available from the following open sources:

3. Licence chamber (Лицензионная палата), which provides information about operating permits in a specific field.
4. Consumer protection association (Общество по защите прав потребителей) has a "black list" of repeat breachers of consumer rights with whom co-operation is not recommended.
5. Local statistics committee (Комитет по статистике) provides chargeable accounting and statistical information about companies.
6. Non-government organisations specialised in collecting information about undesirable customers and partners.
7. Firms and agencies specialised in legal assistance provide albeit often high-priced information on application of the law in situations of conflict. The information is sought by conflict category.
8. Law enforcement authorities, e.g. the information centre of the ministry of internal affairs (MVD) and the information centres belonging to the ministry of internal affairs' regions' administration (UVD) provide information about the subjects of background checks for operators in the financial sector, such as banks and other juristic persons. The information includes sentenced crimes, the date and clause

of the sentence and warrants of apprehension. The information costs three times the minimum wage (about 3 x 100 roubles) (price information from 2007).

9. Regional entrepreneurs' associations can also help, but the efficiency of their operation is not certain. At the national level, for example the Russian Central Chamber of Commerce maintains a register of good business partners. The register can be found on the net at: <http://www.tpprf.ru/ru/main/punkt/>. Regional chambers of commerce have their own corresponding registers.
10. An operator in the food products sector can obtain information about the existence of product certificates from the sanitary-epidemic service.
11. An Internet search on a company and person can give good results from the standpoint of background checks. Information obtained from the Internet may offer a hint about the need for further inquiry, for example in conjunction with an interview.
12. The mass media have chargeable databases that may contain extensive article material about a company or person. The Russian media's Integrum database has excellently served Finnish researchers, as Russia has granted a few Finnish universities free user rights to the database. This free use is ending at the end of 2007.

In background checks the initial investigations are done in Finland. By efficiently utilising open information resources, it is possible to get far during the initial phase background checks. A Finn with a command of Russian and expertise in background checks and Russian organisations can find useful information before needing to turn to Russian specialist organisations. According to Kuznetsov (2007, 84), the price of a basic background search in Russia is about 100 – 150 USD.

An essential part of background checking is an assessment of the quality of accounting and credit arrangements and if possible, the structure and scope of the company's network of co-operation. Staff members' participation in politics and business associations is also important background information that is easily found in public sources. An expert who has followed the area's social life in the media can immediately say if an entrepreneur is known in the locality if he/she has been negatively portrayed in public.

Russia does not have a separate law concerning background checks like Finland does (Law on security investigation procedures). The activity is mainly governed by labour legislation and legislation concerning processing and archiving of personal data, which is explained in more detail in the chapter on information security. Thus, obtainment of information is not systematised in Russia as it is in the law on security, and both the information and the information obtainment channels may be disparate. Many sources of information require personal relations. Independent obtainment of information requires composure and restraint. A foreigner very actively searching for in-

formation will arouse suspicion in the authorities about what the foreign company actually intends to do. Additionally, too much questionable activeness will cause a danger factor from the direction of possible competitors and the criminal sector. The most demanding phases of background checks should be left to professional organisations.

5.3 Observations that illuminate backgrounds

In choosing a business partner, in addition to the above-mentioned document-based background checking it is possible to fill in this information by fixing attention on some supplementary matters. The company should have sufficient evidence (at least 3 years) of successful business operation, indicated by business documents like financial statements and annual reports. The company's prior names should be determined as well as the nature and success of operation under those names.

Mapping the profile of the management and the company's ownership are essential tasks in background checking. It is important to know the company's ownership base even though it may be difficult to determine the true owner. Information about the owner may have a strong effect on negotiating and decision-making processes. Currently a large share of SMEs in Russia are managed by the owners. It is also good to know about the relations between the owners. The company may be owned by a bank, for example. In that case it is necessary to become familiar with the owner when making agreements.

It is a good sign if a manufacturing company has operated in a certain place or locality under the same name for a longer time (at least 2-3 years). Other good signs are if the facilities are owned by the company and mentioned in the profit and loss accounts. Location of the facilities near other companies or in a special business building brings more credibility. Changing facilities and locations may say something about the company's development cycle.

If the company has customers in the public sector (projects delivered and on order), it is a good sign of the partner's reliability, proper tax payment and relations with the administration. Public sector procurement's trustworthy companies are often found on the client's list of most favoured companies. Some clients also publish a list of undesirable companies (www.zakupki.gov.ru). Public procurements are monitored closely in Russia and the legislation on competitive bidding is constantly developing.

An important prerequisite for co-operation is that a company already has a functional telecommunication, communication and other basic infrastructure so that their improvement does not fall on the client. The company should have maintenance and delivery agreements and spare parts service for technical equipment. Electricity, water and gas delivery and the sewer system

should work flawlessly and without interruption. Problems with public utility services reveal significant things about a real estate company's situation.

The level of education and certificates of competence of the staff and management are often an indication of professional skill. Normally the management's CVs are available, on which basis something can be decided about the people's expertise. The authenticity of education certificates and degrees should be verified with the institutions in question. Unfortunately, in Russia it is possible to buy a degree. The company's presence at international or Russian exhibitions indicates a desire to co-operate and belief in the company's product and marketing know-how. Publications and articles by the management and staff members offer an opportunity to assess their qualification in the field. The company's (staff's) publications in their own special field indicate the companies' undisputable merits in its own sector.

Careful inspection of documents is a part of the process of recruiting the management and staff. During the selection process the domestic passport and possible foreign passport, degrees and various certificates should be checked. As a hint may it be mentioned that it is possible to verify the validity of Russian citizens' passports on the Internet pages maintained by the Russian Federation's immigration agency (FMS). The same register includes information on the legality of residence and passports of foreigners working in Russia (<http://fms.gov.ru/inspection/index.php>). Chronological information (work history) obtained during an interview can be compared with facts presented in documents. Just to make sure, the candidate for a job should be asked the names and contact information of his/her superiors at earlier workplaces and possible referees. The applicant's closest workmates and the reason for leaving the previous job should be investigated. Of course the person should reveal any previous penalties or disciplinary measures. The person should be asked for written permission to check and handle the above-mentioned personal data in accordance with the labour legislation (KZOT RF, paragraph 86, moment 3). The employer is obligated to make sure the received personal data are not released to a third party. The employee has the right to review his/her personal data in the possession of the employer and ask for possible corrections to be made. According to the labour legislation the employer may not collect or receive information about the employee's religious and political convictions. As a rule it is also forbidden to collect information about his/her membership in societal associations and professional unions.

Sufficient language skills are a prerequisite for successful international co-operation. In practice, the Russian partner should be able to use either English or Finnish, unless the Finnish company has someone with sufficient fluency in Russian. In simple, specified matters it is also possible to function with the help of a reliable translator. Forming truly deep relations most often requires a command of the language of the receiving country. Skill in English is absolutely necessary in the IT sector. In making agreements the congru-

ency of translations must be verified by an experienced business translator. Agreements must be approved by a notary. The smaller the company in question, the more the significance of language skill is emphasised. Large companies do not consider language skill a threshold question.

Low labour costs are still an advantage in Russia, but this advantage is weakening as competition in the job market gets stiffer and the productivity and efficiency of companies increases. Too much should not be expected from a high-quality partner by only concentrating on labour costs. For example in St Petersburg and Moscow labour costs in the IT field have risen to the Western level or even higher.

The Finnish partner should use various methods to carefully verify the level of technology and quality of production, on-site if possible. Some Russian SMEs have certified their products according to the ISO 9000 standard or some other quality system. An international quality system tells of the company's intent to enter the international market and/or its desire to become part of a multinational distribution network in the Russia market. Proof of certification should be requested.

The knowledge, skills and know-how (economic management, marketing, technology) of managers may be lacking in Russia, which has become apparent especially after 1998 in the stiffening competitive situation in the markets. Along with the management, the professional skill of accountants is in a key position. The professional skill and level of motivation of managers and accountants reveal the true prerequisites for business operation.

Development in turnover and sales and existing customer contacts provide significant information about a company's financial situation. It is quite common practice that a Russian company's official turnover indicates only a part of the company's actual turnover. According to recent studies, 20 - 50 % of companies' turnover may be "obscure" (Kauppapolitiikka 8.1.2004). A company's good solvency is indicated by the fact that it has a bank loan or a reliable investment agency has invested in the company, for example. KMB-Pankki (Small Business Credit Bank) and Sberbank's NW department (savings bank) are good examples of this.

Russian companies with good international experience can give reference information. Most of these companies have WWW pages (often in two languages). Information obtained there is usually quite reliable (University of Joensuu 2005). A customer is given reference information if the desire to co-operate is authentic.

The region's and locality's public media and the Internet probably also contain abundant information about partner companies. At some phase something has definitely been written publicly about a company that has long operated stably (or unstably). Mapping the public image is possible during the

initial phase of co-operation also from Finland. In discussing with a potential Russian business partner an experienced operator in the field will quickly notice any contradictions or attempts at covering something up. If something attracts particular attention, it is worth investigating the background in more detail. Familiarisation and discussion with the company's other staff members may offer valuable hints of a Russian company's actual situation, internal atmosphere and visions of the future. Of course it is understandable that the management must give permission to discuss with the employees of a Russian company. Management that truly desires to co-operate will give such permission.

5.4 Establishing a company

Establishing a company in Russia is the result of extensive consideration and analysis. In a narrow sense establishing a company involves getting the company's name and operating rights in the Russian markets (registration of the company). Broadly understood establishing a company also includes acquiring a staff and operating facilities and equipment. Each phase of work requires security awareness. As already mentioned, mere selection of a partner and consideration and planning of the establishment of a company require their own security analyses. Staff recruiting involves background checks, and essential in selecting facilities is to verify the facilities' ownership and other structural safety. Physical protection of the company's facilities also requires its own planning.

Establishing a company in itself is a thoroughly covered theme in business guides and advice that deal with Russia, so there is no need to dwell on this topic in this booklet. Guides on establishing a company in Russia are available from several quarters, and detailed presentations can be obtained from educational institutions, for example (see e.g. Siikaluoma & Metso 2001). Chambers of commerce also offer up-to-date information. Russian regional development and business sources contain detailed information on the phases of establishing a company. Murmansk's regional administration's portal contains detailed instructions for establishing an individual company, for example. Below are links to company establishment instructions:

http://www.b-port.com/info/spravka/law_base/

http://www.b-port.com/info/spravka/how_to_become_businessmen

In Russia, agreement-based co-operation, a representative office or subsidiary and a company are forms of international co-operation. A representative office and a subsidiary are registered with the ministry of trade and economic development in Moscow. A representative office may operate only as a general representative, but it is not an independent company. The price of the yearly licence of a representative office is high enough that it may be too high a threshold for a small businessman. A subsidiary again has the same operating rights as the parent company. Thus, according to Russian legisla-

tion, a subsidiary and a representative office are not legally independent operators. At least in the 1990s in St. Petersburg (Aromaa & Lehti 2001, 5), it was noted that the position of representative offices was less problematic from the standpoint of criminal and security threats, because there is no significant cash flow through them and their activity is more limited than it is in actual business operation.

Joint companies (SP, *sovmestnoje predpriyatije*) as a mode of business proved to be unreliable in the 1990s because in many cases the Russian party gradually attempted to gain possession of the company's authority. According to SVKK ry (2005, 13), the use of representative offices has diminished in recent years. Finnish companies increasingly operate through Russian partners, importers, wholesalers and retailers. A good alternative is still a one hundred percent-owned subsidiary or purchasing shares in a Russian company. One hundred percent ownership prevents possible disputes over ownership and rights of possession. Full ownership protects intellectual property, reinforces supervision of interests and reduces the possibility of illegal copying of products. Additionally, feedback from the markets goes directly to the owners. The staff's motivation will most likely also remain at a higher level if the ownership is clear.

The process of registering the establishment of a company is the same for a foreign investor as it is for Russian entrepreneur. The above-mentioned web addresses explain the registration process in detail. According to the law, also non-profit organisations must be registered according to the standard registration procedure (including units with foreign shareholders).

Establishing a company begins with choosing the type of company. The types of companies used the most in Russia are ITshP (ИЧП, individual company), ООО (limited liability company), ЗАО (closed company), ОАО (open shareholder company, large share capital/large companies), АО (open shareholder company, small share capital) and ТОО (partnership company). In past years the most popular type was SP or joint company, as mentioned earlier. Of course this alternative still exists. A company's prefix indicates the type of company, i.e. whether it is an individual company formed by a single person, a limited liability company, a partnership company or a shareholder company. The choice of principle of liability is either business operation where the extent of liability is the entrepreneurs entire property or where liability is only based on invested property (АО).

A company is established at an establishing meeting. The establishers may meet personally or an establisher may send an authorised representative with a letter of proxy (a letter from a lawyer). Russia's law enforcement officials may send a representative only with a letter containing the organisation's seal or stamp. Foreign representatives must have a copy of the letter that is translated into Russian and certified. The meeting must produce the following

documents: agenda, establishment agreement (if deemed necessary) and the minutes of the meeting.

When the company is established, the company's registration application is filled out. The applicant must fill out and sign a standard application form. The application form is also found on the Internet. The applicant may be one of the company's establishers, an establisher's higher manager or legal entity, or some other person authorised by the establishers (must be mentioned in the minutes of the establishing meeting). The applicant is responsible for the correctness of the information on which basis a decision is made. A notary public must certify the authenticity of the applicant's signature.

The tax inspection office is the first authority to which the documents are submitted. The most important tax inspector is the inspector in the locality where the company's main office will be located. All the company's establishing documents must be included along with the signed application form and a receipt of payment to the state. Foreign operators must also submit a translated and certified copy of the operator's registration certificate in his/her own country. The above-mentioned documents must be brought directly to the tax inspector or sent by registered mail. Registered mail is recommended if the tax inspection office is busy and waiting in line would be unreasonable.

According to the law the registration certificate is available within five days if the application is submitted in person and within seven days if it was sent by mail. The tax inspection registration must be done within five calendar days of the date on which the company was registered.

The company also has to register with the social security fund, a voluntary health insurance fund, a pension fund and the state's statistics committee. The above-mentioned registrations must be done within 30 calendar days of the company's registration. Having a company stamp made is one of Russia's oddities. The law does not require a company to have a round stamp, but a stamp is nevertheless deemed necessary in business practice. In practice a company is obligated to use a round stamp (Federation's law on establishing a company: "possible registration of a stamp"; Kaakkois-Suomen TE Keskus 2005; Oikarinen 2005, 20; SVKK ry 2005, 42). It is possible to set up a bank account only after these procedures. When all of the above-mentioned measures have been carried out, the company may begin normal operation. If the establishers register the company alone, the registration lasts about a month and the cost is comprised of the following payments: Payment to the state – 2,000 roubles (€60), notary public's fee – 200 roubles (€6), registered mail – 60 roubles (€2), altogether €68. If the establishers want to use a lawyer's office, registration lasts 7-10 days and costs about €100 – €200.

The process of establishing a company was presented here on a very general level. As mentioned earlier, detailed on establishing a company in Russia can be found in other texts, which should be studied for more exact information.

6 RISK MANAGEMENT AND RISK ANALYSIS

6.1 Recognising risks and the probability of them materialising

Risk management and assessment and risk analysis are concepts that are closely linked to business operation. By examining risks it is possible to identify threats against which a company needs to protect itself. In risk management a company becomes aware of the nature and scope of undesired events and defines an acceptable risk level. Risk management begins with identification of types of risks. The first phase of risk assessment is identification of danger, in which a company strives to determine whether a factor under scrutiny is dangerous to people, property or the environment. In assessing risks a company assesses the consequences and impact of undesired events (Miettinen 1999, 50 — 51).

Risks can be categorised in many ways. External and internal risks, known and unknown risks, old and new risks, and indirect and direct risks are the most commonly used categorisations of risks. There are also other ways to categorise risks, such as the consequences of an event (minor, detrimental, serious) or the probability of an event occurring (improbable, possible, probable). The above-mentioned categorisations are often used to facilitate risk identification when mapping and grouping risks. Most challenging are risk identification and classification into various degrees of probability and seriousness. Prior experience helps in risk grouping and analysis.

Risk analysis is a company's and an organisation's tool for meeting future challenges. Risk analysis is a detailed technical research process, in which undesired events are determined. Risk analysis provides a picture of what known risks exist and what their effects are if they materialise. As a result of the analysis the organisation's alternatives are planned to cost-effectively match the probabilities of risks. Thus, in risk analysis the company examines what kind of, where, when, how and why a risk may materialise. The types of risks are business operation, competition, economic cycle, investment, product and staff risks. In addition to marketing and financial risks, a company's operation faces numerous disturbances during normal times, among them crime risks (Harju & Söder 2007). As a part of crime risk management, Samociuk, Iyer & Lehtosuo (2004) propose sharpening risk analysis in companies to prevent and reveal malpractice. A strategy for managing malpractice like fraud and theft is part of a company's overall risk management. Identification and prediction of psychological and social risks is a challenging task for technical risk mapping. Furthermore, their impact is hard to predict.

As a main principle, a company's risk analysis is comprised of a) defining the organisation's operating environment, b) identifying risks, c) assessing risks,

d) prioritising risks, and e) choices related to risk management. In the field of security, agreement on common concepts has been a continuous challenge. Due to the variety of security systems, the terminology is problematic. In speaking of risks one needs to first define what is a danger. A danger is a possible source of a mishap or a situation that enables a mishap. A risk again is the possibility of an event that causes or results in personal injury or causes environmental, cultural or economic loss.

- Accidents
- Catastrophes in a nearby area
- Unexpectedly or violently acting persons
- Crime
- Destructive acts and vandalism
- Technical malfunctions in production processes
- Malfunctions in building technology and public utilities
- Fires: intentional or unintentional
- Problems in medical care
- Problems in information security and information protection
- Problems in computer spare parts delivery
- Disturbances in communications systems
- Disturbances in food service
- Terrorism
- Natural damages: floods and storms

Risk is the probability of an accidental event multiplied by its impact. Risk management refers to an overall understanding of existing dangers and a systematic study of how losses caused by dangers can be minimised and how the least expensive management methods can be chosen. Risk analysis is independent of culture in that the rules governing of risk materialisation and risk prevention are applicable globally. This means risk analysis related to business operation in Russia can be done at home (in Finland), but on condition that the field of operation is thoroughly familiar.

6.2 Framework of analysis

Risk analysis begins with risk identification. Firstly one needs to know what risk is. Risk is the probability that something detrimental will happen. For example, a flood is a threat that appears rarely, so it is a small risk. The purpose of an analysis is to first find a name for a risk and the probability it will materialise. The size of a risk is based on research data. Intuitive brainstorming is used in addition to research data to assess risk. Often a familiar risk is perceived to be smaller than an unknown risk. An unidentified is nevertheless the greatest risk. Thailand's tsunami can be considered such an unidentified risk that caused immense losses when it materialised. The probabilities of materialisation and subjective methods of analysing consequences may bring

an analysis astray, but on the other hand the intuitive method is capable of uncovering risk factors that have not happened or been taken into consideration earlier. The purpose of risk analysis is to also identify unknown risks and find ways to reduce them. After risks are identified and assessed, it is necessary to search for procedures with which to manage or prevent them. In risk mapping a company analyses both the company's internal and external operating environment.

Photo: Vesa Koivumaa



Risk management again requires both internal and external security solutions, operating instructions, training and equipment. External and internal risks falling upon a company depend to a great extent on the size, location, field of operation and operating experience of the company. Most often it is not possible to notice all dangers. Special checklists and standardised lists can be used as an aid in mapping and assessing risks.

It is desirable for an organisation to have its risks under control. Risk management is based in decision-making and accordant operation by which risks revealed in risk assessment are minimised. Risk management is no longer scientific operation; it is also steered by the rules of economic, political and social life and people's understandings and attitudes. Risk management compares different kinds of alternative actions and selects the most suitable (cost-effective) methods for reducing or eliminating risks. It is impossible to control all risks. Decision-making must be able to make prioritised choices whose impact is most effective within the framework of available resources. Various risk management tools that are available to everyone have been de-

veloped (see e.g. <http://www.pk-rh.com>). Risk management methods are divided into risk-taking (acceptance), risk avoidance (elimination of materialisation), risk transfer (insurance) and risk reduction, i.e. reducing risk to a tolerable level (for example, armoured vehicles for transporting of valuables).

Analysis of a company's operating environment covers:

- the company's internal field of operation
- the company's objectives, strategies and associated tasks
- production processes, key processes
- parties closely involved with the company's operation
- management and staff

External field of operation

- general state of the external operating environment (stability, crime, disturbing factors)
- co-operation with the operating environment, manner of dealings
- most important exiting and entering signals, products, services

Risk identification

- listing of (internal and external) factors affecting the organisation's operation
- regional and local risks

Risk assessment

- probability of risks materialising
- impact of materialised risks (positive and negative)

Risk prioritising

- arranging risks in the order of materialisation and impact
- grouping and categorisation of risks (internal – external, short-term – long-term)

Choice of risk prevention and management methods

- compilation of scenarios, i.e. descriptions of alternative future events
- compilation of plans for different scenarios, taking into consideration the most probable and improbable events and mildly detrimental and overwhelming scenarios

Compilation of a risk prevention plan

- integration of individual risk management methods into an overall plan
- development of as cost-effective risk management mechanisms as possible

- follow-up of the implementation of the plan and modifications based on experiences gained

Risk analysis in business operation in Russia must particularly consider:

- company takeover
- fire
- law enforcement and other official inspections
- information leaks (to competitors)
- burglaries, especially of storage rooms
- fraud carried out by goods suppliers and customers

Risk identification, analysis and management is a process in which applicable communication inside and outside an organisation can prevent fear and uncertainty. Non-specialist parties, such as employees, must also be able to participate in the various phases of the process. Usually this participation phase needed at the start of risk mapping is an essential part of risk identification, since people's experiences can bring new ideas. The employee is the best expert at his/her work site. To be successful, communication that is a part of risk analysis must be bi-directional. Communication increases trust in the management's capability to control risks, whereupon various unexpected social and psychological risks decrease and the security attitude develops in the right direction.

Risk assessment, analysis and management are not very complex issues even though the concepts may seem theoretical. We consciously and unconsciously do risk management work every day. When we go for ride with a bike, we first (at least subconsciously) go through the possible accidents and mishaps that could happen along the way. At the same time we consider what we would do if the bike trip were interrupted, say, if the bike broke down. We also consider the impact of the weather on our trip. After this risk mapping (risk identification) we analyse how we can respond to these identified risks. We prepare for the coming challenges according to the results of the analysis. Our equipment might include a raincoat, a helmet, a pump, a tire repair kit and a snack. From here we easily go to risk management. If we go in the rain we assume responsibility for the risk. Risks that we were able to assess upon leaving continuously materialise around us. We avoid an almost inevitable risk of damage to the bike by choosing a road instead of a forest path. In case the bike is stolen we have transferred the risk to an insurance company in our home insurance. The risk of injury in case we fall is decreased with the help of a helmet.

Risk assessment and risk management in Russia require good local and regional familiarity and detailed knowledge about economic and societal functions. According to a survey conducted by SVKK ry in 2005, the risks of operating in Russia are divided into political and economic risks, changes in legislation, property risks, competition risks, financial risks, crime, a company's internal risks and trade barriers and discrimination. In its study SVKK

ry presented a detailed list of concrete risks belonging to each risk category, so the issue does not need as much attention in this booklet. Risks created by actual security factors are intertwined with crime risks, which nevertheless only about 30 % of companies have experienced (SVKK ry 2005, 73 – 75).

6.3 Security environment analysis

Security environment analysis is a concept used in Russia that is broader than risk analysis. It emphasises the significance of societal and social events on the level of risk faced by a company. In Russia security environment analysis is also linked to tasks given to a security company. Co-operation with a company that provides security services and the person responsible for security in a client company is strengthened if the client company first of all compiles a security analysis dealing with the internal and external operating environments alongside and in support of the company's risk analysis. A company planning business operation in an area is responsible for, and as much as possible also compiles, a security analysis, which can then be included in the company's risk analysis package. Some parts of the compilation of the security analysis can be given to a security company.

A security analysis specifies the tasks of the company's security management and possible external security service in the area of operation. Necessary conclusions are drawn from the external and internal security environment description (situation description) and resources are allotted to match the challenges described in the analysis and to focus actions according to each changing situation. The situation description includes first of all a review of production and market security. Competitors' power blocs and the region's crime elements, including their structures and operating methods, are taken into consideration as external challenges in the situation description. Other external threats are described as possible as a reflection of the political, economic and social situation of the state, region and city in question.

The description of resources included in the security analysis is an inventory of the company's security organisation's operating capacity and the need to purchase security from outside the company. At the same time a division of tasks is done to specify which tasks remain as the responsibility of the company's security management and which tasks are taken care of by an external security service. In emphasising the importance of a security analysis in planning a company's operation, Kuznetsov (2007, 304) also wants to link authorities like the militia administration (MVD) and other security officials as primary resources in the situation description. The situation description is used as a base for compiling a preparation plan for different scenarios and forming security management plans according to the different alternatives. The operational readiness of the internal and external security organisation and response times to various threats is ensured on the basis of the analysis.

By nature the description of the security situation is a societal analysis that presents the essential factors of the external environment without addressing technical details at this stage. Kuznetsov's (2007, 305) model analysis first describes the company's basic information and operating principle, facilities, staff and general economic key figures. Next the analysis includes the political and economic situation of the state, region and municipality (city) and the economy, politics and social circumstances in the areas on which the company depends in terms of spare parts delivery, raw material flow and customer relations. The impact of operational changes of individual authorities, such as customs, are taken into consideration in the analysis, as are possible special situations brought about by changing seasons (summer vacations, heating, electricity tariffs, difficulties in energy delivery, etc.).

The impact of society's social situation on crime and thereby the company's security is taken into consideration in a comprehensive security environment analysis. Russian security analyses take into consideration things like the effects of delays in wage payment, lay-offs and rises in living costs at the local level on the crime situation in general and property crime in particular. By this conclusions are made concerning guarding needs and property protection in the near future. At the same time the company's competitiveness and financial situation with respect to competitors and the city's/region's other companies is assessed. From this again conclusions are drawn about the company's relative attractiveness in the eyes of organised crime and as a precaution against possible corporate takeovers.

The company's relative negative position should also be taken into account. Weakening of the company's competitiveness affects the atmosphere, work ethics and productivity of the workplace, which in turn makes the company susceptible to the effects of criminal organisations and information leaks. The company's management is responsible for correct allocation of limited resources. Should the company's internal and external supervision be increased and is it at all possible to affect certain external factors of change like legislation and actions of the authorities. The company's management may use the solutions of similar companies operating in other cities as a model. The West is just awakening to the need for extensive security environment analyses. However, an extensive analysis is a significant tool in a company's risk analysis system. Its usability is measured especially in previously unfamiliar areas of operation where the impact of the region's/locality's societal and social situation on the success of the company may be crucial. There is very little of this type of risk analysis expertise in Finland.

7 AGREEMENT SECURITY

7.1 An important part of a company's economic security

Agreement security consists of creating an advantageous and economically feasible business framework for one's own operation. Agreement security is closely linked to the above-mentioned assessment of a partner's reliability. Russian law (civil codex) specifies formalities for many types of agreements that Finns are not accustomed to. For example, agreements related to financing and pledging must always be drawn up in the presence of a notary, and foreign trade agreements must always be written. If specific formalities are to be used in a main agreement, then related preliminary agreements and authorisations must comply with the same formalities. Agreements drawn up in Russia must always contain the companies' official stamps. Model agreement templates can be found at <http://pantaliainteractive.com/> and <http://law.rambler.ru/patterns/>. Unofficial Finnish translations of model agreements such as job contracts, purchasing and sales agreements, opening and account and renting an apartment can be found on the Doing Business Safely in Russia web site at www.finnbarents.fi/safelyinrussia2/.

Literal compliance with agreements is just being learned in Russia. An agreement is not necessarily followed even though to a Finn (Western trade culture) the agreement fulfils all requirements and recognises the obligations of all parties. In the Russian business culture an agreement may still be understood mainly as an intent or desire to co-operate. Nevertheless, those who have worked with Western companies for a longer time have learned a precise agreement practice. It is not uncommon to build on verbal agreements (SVKK ry 2005, 51). Cases still come up where, for example, representation agreements have remained verbal, and in a crucial situation a representative in Russia has disappeared without a trace and left his/her work half finished. In practice, if a dispute arises, only a written agreement is valid in Russia.

A company should always become familiar with model agreements in the company's own field. They can be obtained from companies operating in Finland or Russia and from many books dealing with agreement practice. Russia does not have any general mandatory standard agreement models. Each company can, following Russian laws, compile its own agreement template and use it as a type agreement. The company should use the services of professional lawyers and translators in compiling or at least in checking an agreement. If possible, to reach the best end result and to ensure that details important to oneself are entered precisely, the agreement should be compiled by one's own company or lawyer. However, in practice the seller usually proposes using his/her old agreement models as a starting point, and then both parties add or delete clauses. If the agreement is bilingual and there are differences between the two language versions, the original language version

is given priority unless the parties have agreed otherwise. Purchasing, sales, agency, distribution, etc. agreements essentially follow standard international practice.

Special features of agreement practice:

- The agreement must be written
- One copy must be in Russian
- International terms and procedures (INCOTERMS, arbitration procedures, etc.) are in standard format.

According to the recommendations of the Russian authorities, a foreign trade agreement should contain at least the following information:

- agreement number
- date and place where the agreement is signed
- official full names of the seller and buyer
- destination state
- name and full description of goods (specification)
- package and markings of goods
- volume, weight and quantity of goods
- price and total value (delivery clause, currency, price formation)
- terms of payment
- banks and contact information
- delivery time
- inspection of goods
- notice of defects and period of notice
- definition of *force majeure*
- warranty
- technical assistance, training
- arbitration
- sanctions
- signatures
- agreement language

The above-mentioned terms are not mandatory in all agreements, and the type of goods and the other content of the delivery determine which terms are actually included in the agreement. It is also well advised to include terms other than those mentioned above if they are important to the parties and clarify the content of the agreement. For example, in construction project exporting the orderer and supplier agree on the main contract issues as well as secondary issues that each party is responsible for (social premises, office premises, electricity, data connections, water, possible official fees, translations of user guides, training, etc.). As an example a model agreement of a security company is appended to this booklet to indicate what types of issues need to be taken into consideration when using guard services. The company should also have its own agreement model to offer to the Russian trade partner. An agreement model brings uniformity and logicalness to agreement negotiations and the final trade transaction.

7.2 Safeguarding business interests

A correctly implemented agreement procedure gives a strong guarantee of the continuity and economic security of business operation. There are no comprehensive instructions on the functionality of purchasing and sales agreements against fraud, but the following issues are the most important:

- Goods are paid when they are received. Account arrangements are agreed with good terms (e.g. a buffer account; opens when goods arrive). Prepare for the possibility that account opening documents are counterfeit;
- Even though a couple of prior business transactions have gone well with a partner, it does not mean a third, somewhat larger project will succeed as well. The risk grows especially if the partner is able to arrange funding in conjunction with a big business transaction;
- In entering an agreement one should be sure the company can participate in all essential phases of co-operation, use of money, costs and profit distribution. The company's economic interests must be specified in detail in the agreement. If they are not met it is possible to require compensation;
- Unusually low-priced bids and agreements should not be entered. At least the possibility of realising them must be closely examined;
- Sanctions for delayed delivery of goods should be specified in the agreement;
- It is absolutely imperative to become familiar with the partner company's establishment agreement/articles of association;
- One must make sure the partner company has the right to practice the operation associated with the agreement. One must also make sure the director/representative has the right to sign/enter an agreement without approval from upper management. If the partner refers to known, stable establishers/owners, this must be verified from the establishment document. It is also beneficial to become familiar with the company's financial statements and profit and loss account;
- The passport (identification) and right to sign of the agreement's signer must be checked as well as the congruence between the company's name and stamp and the names on the agreement and other papers;
- The agreement text must not refer to any companies other than those signing the agreement. One must be especially careful if the agreement is entered under a known company name but payment is to the address of some other company (even if the latter is called a subsidiary or representative);
- Verification of necessary pledges;
- If security is offered, the background and owners of the security must be checked;

- Verify the quantities and qualities mentioned in account documents and receipt and relinquishment papers;
- Minimise the need to transfer own employees to another company's employment;

Photo: Pekka Iivari



Use the company's own lawyers and consultants specialised in agreement practice to verify the correctness of the agreement. One must not relax even when dealing with a company that looks good. Russia has companies that are outwardly impeccable, but whose goal is to gain a partner's undivided trust and finally commit a fraud. The officials of a reliable-looking company may have forged passports as identification.

As a rule, agreement disputes are handled as civil cases in a court of arbitration. An agreeing party that is legally well prepared is the strong party in such cases. It's no news that the parties' business skills, familiarity with business culture and expertise in relations are tested during the agreement negotiation phase. Language skill is an asset during the negotiation and agreement phases. A rough rule is that the smaller the company, the more important it is to know the agreeing partner's language. Large companies can afford to and have a sufficient name to influence agreement negotiations with their own weight. Actual language skill does not have significant meaning in the negotiations of large companies.

8 LICENCES AND CERTIFICATES IN RUSSIA

8.1 License

A licence is a permit or right to practice licensed operation. With the help of licences the state supervises operations that are strategic or contain specific (security) requirements from the standpoint of the state. Licensed fields include operations that, when practiced, may hurt the rights, legal benefits or health of citizens, the defence and security of the state and the cultural heritage of the people of the Russian Federation. A certificate again is a quality standard that must be met before applying for a permit to operate. Operation must be practiced in the manner stipulated by the licence. Sometimes a certificate functions as a marketing aid in enhancing the success of a product on the market. A company needs a separate licence for each licensed operation that it intends to practice. A licence granted by the Federation gives permission to operate everywhere in Russia. If a subject's licence organisation has granted the permit, the operation may only be practiced in the region of the subject in question.

The company's operation must meet certain terms and requirements that the grantor of the licence sets for juristic persons of individual entrepreneurs. Licences are granted by the Federation's state officials, regional administrations and local autonomous organisations. According to the law a licence should be granted within 45 days after the application has been submitted. If the licence has been granted by a regional administration, it is valid only in the region of the Russian subject in question. The minimum period of a licence is 3 years, but it is possible to apply for a shorter period for special reasons. If the terms of the licence are not breached during licensed operation, the licence may also be extended according to the wish of the licence holder. Licensed operation in Russian includes:

- Aircraft technology (production and repair);
- Distribution of cryptographic devices and other related services;
- Operation related to exposure of technical listening and monitoring devices, unless it is for one's own purposes;
- Operation related to concealment of information using codes: development and production of coding technology and protection of information and telecommunication systems with the help of codes;
- Operation related to electronic signatures, registration of their owners, renting of electronic signature services and production of services related to verification of the authenticity of electronic signatures;
- Production or development of accessories intended for protection of confidential information and protection of confidential information;
- Publication;

- Manufacture, purchase and distribution of equipment needed to acquire secret information;
- Manufacture of securities and equivalent documents that need to be protected against forgery;
- Manufacture, repair, use and sales of military technology and weapons;
- Manufacture and sales of major components and shells for firearms;
- Display and collection of weapons and shells;
- Manufacture and use of explosives and their components;
- Storage, transport and disposal of chemical weapons;
- Use of explosion, fire or chemically hazardous production sites;
- Specialist work in industrial security;
- Manufacture of explosives for industry; storage, use and distribution of such explosives;
- Manufacture of pyrotechnical products and distribution of class IV and V pyrotechnical products;
- Fire warning and extinguishment operation;
- Installation, repair and maintenance of fire safety devices;
- Geometric measurement (*markscheider* work);
- Restoration of cultural monuments;
- Geodesy, cartography;
- Work related to hydrometeorological and geophysical processes;
- Field of hydrometeorology;
- Pharmacy, manufacture of pharmaceuticals, medical technology services (maintenance);
- Custom manufacture of prostheses and orthopaedic products;
- Growth of narcotic and psychotropic plants;
- Operation related to narcotic and psychotropic products;
- Care of infectious diseases;
- Sea and waterway transports and air transports;
- Motor vehicle transports using a vehicle registered for more than 8 passengers, unless it is used for one's own purposes;
- Freight operation (forwarding);
- Rail transport operation;
- Hazardous transport operation;
- Collection, use, neutralisation, transport and transfer of hazardous waste;
- Production and sales of equipment in the game business;
- Money game operation;
- Private security company and detective operation;
- Refinement and sales of coloured scrap metal and metallurgical scrap;
- Pawn shop operation;
- Production of noble metals and jewellery containing noble metals;
- Purchase and sales of grain and grain products;
- Sales of antiques;
- Organisation and implementation of lotteries;
- Fuel distribution point operation;
- Employment of Russian citizens abroad;

- Manufacture of audiovisual products;
- Auditing (licence not required after January 2007);
- Investment fund operation, administration of investment funds and non-government pension funds and pension insurance and related investment operation;
- Cosmic operation;
- Health care operation;
- Sales of electrical energy;
- Air safety work;
- Travel agency and travel organising work (licensing not required after July 2007, when a monetary security system is taken into use);
- Construction of buildings and building technology and other project work and designing and engineering work except for temporary and secondary operation (the licensing requirement is being eliminated).

In the case of operation in the chemical field, operation with a danger of explosion and operation in dangerous industrial sites, e.g. construction in such a place, the licensing authority in the Murmansk region, for example, is the Rostekhnadzor technological and ecological inspection administration (Управление по технологическому и экологическому надзору Ростехнадзора по Мурманской области), street address: Kolskii Prospekt 1, tel. + 7 8152 254 691.

The above-mentioned list of licensed operations does not include operations that were freed from licensing beginning on 1.1.2006. One should remember that the licensing law does not touch foreign trade, customs operation, environmental protection and use of natural resources, and use of intellectual property. These are regulated by their own laws. For example, in land use and use of natural resources one must contact the regional administration's natural resources department, which gives instructions and regulations for land use, including extracting soil resources and modifying bodies of water. Licensing of tourism operation ends in the summer of 2007, when monetary security becomes effective. Tourism companies registered in Russia must pay a 10 million rouble security payment before practicing foreign tourism operation. The security payment for domestic tourism is noticeably smaller.

The licence application for licensed operation must include:

1. The company's full name and abbreviation, type of company, address, location of licensed operation, company's state register number (company ID in Finland), extract from the trade register;
2. Individual company's name, person responsible for the company, place of domicile, address at which licensed operation is managed, state register number (company ID), extract from the trade register;
3. Tax liability ID (extract from the tax register);

4. Type of licensed operation that will be practiced (the code can be found in the licence law, for example);
5. Company's establishment documents; either original documents or copies certified by a notary;
6. Receipt of advance payment of the licence application submission fee;
7. Copies of documents (qualification certificates, education, etc.) that enable the company (person) to operate in the licensed field in question.

The applicant receives a dated record number as proof that the application has been submitted. The licence office has the right to verify the authenticity and correctness of the documents and the entrepreneur's possibilities to operate in the field. According to the law the licence fee cannot exceed three times the minimum wage stipulated by law (at the time this was written the minimum wage was about 120 roubles). Experience has indicated that up to 1,000 roubles, or about €35, has been charged for licences. The application submission fee is 300 roubles, or around €8. The licence registration fee is 100 roubles, or about €3. Copies of the licence permit and information searched from the licence register cost 10 roubles, or about €0.27.

The licence decision arrives within 45 days along with a postal money order. The licence itself arrives three days after the licence fee has been paid. The payment must be paid within three months. Otherwise the licence will become void. A lost licence certificate can be replaced, but it costs. The licence decision can be appealed. If there are changes in the operation, address or name, the licence holder is obligated to immediately inform the licence office about the changes.

On special grounds a licence can be obtained via a simpler and quicker procedure in the following fields of operation:

- Use of fire hazardous production sites
- Repair of cultural monuments
- Sea, inland waterway, air and rail transports
- Forwarding of hazardous materials

The law on administrative offences specifies the penalties for practicing licensed operation without permission. The fine is substantial and confiscation cannot be avoided. Illegal business operation can be penalised (according to the law) with up to a 300,000 rouble fine or a fine calculated as working hours or a 4 – 6-month loss of freedom.

A complete list of licence grantors can be found at www.mbm.ru. Good information about licences can also be found at www.licensed.ru. State offices grant licences according to the field of operation. For example, the ministry

of internal affairs MVD grants security company permits, the ministry of health grants medical permits, the ministry of culture grants cultural monument repair permits and the ministry of transport grants transport operation permits. According to surveys of companies, it is not very easy to acquire operating permits and product certificates in Russia, or the process has even been made more difficult. Up to every third company felt that the authorities set up artificial barricades and presented illegal demands when applying for operating permits and certificates (SVKK ry 2005, 87).

8.2 Certification

The purpose of certification, which is specified in the Federation's legislation, is to prevent poor-quality, dangerous and counterfeit products from getting on the market. Counterfeits and pirate products form a considerable problem on the Russian markets. It is difficult, or even impossible, for the consumer to notice the difference between an original and a counterfeit. Certification also ensures a minimum level of consumer safety. The specialist authority responsible for certification is the Federation's technical regulation and metrology office (Rostehregulirovanie). Russia's certification system currently includes numerous non-government commercial operators, so over the years the system has become quite disorganised. This disorganisation and lack of supervision is indicted by the fact that, in practice, a certificate can be purchased without any inspections of the actual requirements related to production and products. The state is responsible for inspections, but it does not have time to supervise everything. It has proved to be nearly impossible to remove a poor-quality product from the market. For this reason, in practice, the courts have had to assume the role of the technical regulator. In Finland the consumer office has this role.

Quality certification is voluntary. Nevertheless, voluntary certification is worthwhile. It indicates that a product meets requirements. It also brings added value to marketing and raises its image in the eyes of consumers. Russia's consumer institute (RIPI) recommends a voluntary certification system. RIPI, which is an independent institute, has the right to certify and inspect certificates, and use of the institute's services is recommended.

Russia has 19 different kinds of mandatory certification systems, of which the primary one is GOST, based on Gosstandard's statute. It certifies products and construction materials for private consumption. The technical properties of products are regulated in the law of 27.12.2002, for one (Federation's law no. 184). Russian legislation and statutes contain very detailed lists of products requiring mandatory certification. A complete list can be found in the 23.2.1998 state committee's statute on standardisation, metrology and certification, which was revised on 27.9.2001. Certification can also be handled by a certifying body in Finland. Some certifying companies in Finland co-operate with Russia's largest certifying company, ZAO Rostest (www.rostest.ru).

More information about certification can be obtained on the Kola Peninsula from Murmansk's regional administration (e.g. the regional government's tourism portal has good information about travel arrangers' certifications), the Northern chamber of commerce and Murmansk's standardisation, metrology and certification centre:

ФГУ "Мурманский центр стандартизации, метрологии и сертификации"

Ulitsa Festivalnaja 25, Murmansk

Tel/fax: +47 789 10781, +47 789 10843 (Norway's line)

Tel: +7 8152 47 23 56

Fax: +7 8152 28 60 00

E-mail: mcsm@mcsm.ru

www.mcsm.ru

8.3 Work permit and occupational safety

8.3.1 Work permit and residence

The legal status of foreign natural persons is regulated by the law on the legal status of foreign persons in Russia (25.7.2002). The most important regulations concern temporary and permanent residence permits, foreigners' job contracts, invitation procedures, registration and deportation.

Russia's immigration service (FMS) is in a key position in the work permit process. Immigration service offices are found in most population centres. There are 23 local offices in the Murmansk region, so geographically it should be easy to take care of business everywhere in Russia. FMS decides on recruitment of foreign labour on the basis of the regional labour administration's expediency statement. In the first phase FMS makes a decision on whether an organisation (company) has the right to invite a foreign employee(s). The decision specifies the effective period of the right to invite and the number of foreign employees allotted to the company in question. After this decision FMS makes separate decisions on the part of each employee's work permit. If the employer wishes to employ a foreign person in so-called ordinary work in which the need for a non-Russian specialist is not very great, the employer must first ask FMS for a quota to employ a foreigner. The immigration service grants a work permit on the basis of this quota.

A company inviting an employee needs a statement on the expediency of hiring a foreign employee from the region's labour administration. This procedure requires a certificate of the company's registration from the tax inspection office (copy certified by a notary), a certificate indicating the company is included in the tax list, certified by a notary, and three identical copies of a labour permit application signed by the manager of the company. In addition to the above-mentioned documents from the tax authority, the permit

application must include the company's establishment document (*ustav*), draft job contract, a receipt of payment of the permit fee to the Federation's immigration office and a positive statement from the State labour service office (DFGSZN). More information about this procedure can be obtained from the regional administration's labour department. The invitation to work is granted a local official of the ministry of internal affairs upon application by the employer. In addition to the application, the employer presents a permit to use foreign labour and other necessary documents for each employee.

A work permit for a foreigner is obtained from FMS, or the immigration service (more information about the procedure at www.ufmsmur.ru). To get a work permit the employer is obligated to deposit a sum of money as a pledge in an account opened for this purpose to guarantee that the foreigner is able to leave Russia. It may take six months to obtain a work permit. A work permit is usually granted for one year at a time, so visas should also be one-year visas. In applying for a work permit, the following are required:

1. Filled out work permit application
2. Copy of the entry card
3. Certificate of approval of the foreign employee's education
4. Passport or other ID
5. Health history data
6. Health certificate (HIV)
7. Certificate of wage payment

Authorisation of the labour administration, i.e. a special permit to use foreign labour, is not necessary in the case of a foreigner coming for a special task, such as a director or a department manager. However, a personal work permit is also required for such a task. An application for a work permit is submitted to the nearest Russian embassy in conjunction with the visa application. Most often these work permit matters are left to be handled by the Russian partner. It is worth following the employment situation and labour policy in each field of operation to ensure that changes do not happen unexpectedly. For example, may it be mentioned that a law was passed in Russia in the spring of 2007 according to which less than 40 % of the staff of a retail store can be foreigners. In practice this law affects the employment possibilities of tens of thousands of former Soviet citizens in Russia.

The possibility to employ a foreigner does not touch all sectors of economic life. The law on the status of a foreigner from 2002 does not allow a foreigner to obtain a work permit in the following places:

- State or municipal service;
- A vessel sailing under the flag of the Russian Federation;
- Military aircraft of the Russian Federation or other non-commercial aircraft;

- Captain of civilian aircraft;
- Sites and organisations that maintain the security of the Russian Federation (armed forces, institutions of state secrecy, organisations that work with radioactive and atomic products);
- Other tasks where Federation's restricts access by foreigners.

A foreigner does not need a work permit in Russia in the following cases:

1. A person permanently residing in Russia;
2. A person residing with a temporary permit;
3. Employees of diplomatic embassies and foreign consular employees in Russia;
4. Employees who are rented to install and maintain equipment brought to Russia;
5. News correspondents accredited by the Russian Federation;
6. People studying in Russia who work during their free time;
7. Teachers;
8. Citizens of Belarus

It is absolutely important that a foreign employee's visa and work permit mention the same company as an employer. Only the visas and work permits of embassy employees may have different company names on the visa and work permit, because the visa comes with the name of the accrediting organisation. Organisations that accredit embassy people include the State chamber of registration (GRP) and the Chamber of trade and industry (TPP). A foreign employee of an embassy receives a work visa. A private visa is granted to the employee's family members and a business visa is granted to a non-accredited foreign employee.

A residence permit eliminates the requirement to have a work permit. A foreigner living in Russia permanently or temporarily does not need a work permit. The law specifies that a temporary residence permit can be granted to a foreigner within the framework of the foreigners' quota ratified by the Russian government. The government specifies a yearly quota for the entire area of Russia. This quota is not the same as the aforementioned employment quota. The duration of a residence permit is three years. However, the law contains a group of exceptions to the rule, so in practice the quotas do not have much significance. A foreigner can submit a residence permit application to the Russian consulate in his/her own country. The handling time of the application is no more than six months. There are numerous grounds for rejecting an application or voiding a valid temporary residence permit. For example, are prior deportation, false information given by the applicant, a sufficiently serious sentence in Russia or breaching the rules of a residence permit are grounds for rejection. There are still other obstacles to a residence permit, such as a lack of funds for living in Russia if someone who has resided in Russia already three years does not have a place of domicile. Further

reasons for a negative decision could be a foreigner permanently leaving for another country or if the applicant resides outside of Russia over six months. A foreigner temporarily residing in Russia can also apply for a permanent residence permit. A permanent residence permit is granted for five years and it can be renewed for another five years. The reasons for voiding a permanent residence permit are the same as for a temporary residence permit.

The employer of a foreigner may be a natural person or a juristic person with the necessary permit to use foreign labour. Correspondingly, a foreigner has to have a permit to work in the company in question. A foreigner does not have permission to work anywhere except the place where he/she has the right to live or reside. An invitation is given by officials of either the ministry of internal affairs or foreign affairs or their local offices. State officials, international organisations and their representatives, juristic persons, Russian citizens and foreigners permanently residing in Russia may also be inviters.

8.3.2 Termination of a job contract

Rarely is it realised that termination of a job or other contract must be handled in such a way that causes as little risk of future information leaks, for example, as possible. Controlled termination of a job contract also does not cause a PR risk for the employer. Termination of a job contract in quarrelsome and tense circumstances significantly increases the possibility of crime and information leaks directed at the company.

A person leaving a workplace may take with him/her sensitive information that he/she has had access to on the basis of his/her position at the workplace. Such information could be related to the company's customer base, for example. A customer register is an important file for both existing competitors and the departing employee if he/she establishes his/her own company in the same field of operation. The employer must ensure that the person does not take information that is important or even crucial to the company in the form of paper or electronic documents. The employee must be reminded of the obligatory nature of the confidentiality agreement made during employment and the period of effectiveness of confidentiality mentioned in the agreement.

Return of the company's other property (phones, keys, paging devices, ID cards) must be ensured by means of a receipt procedure. It is the task of the company's management and people responsible for security to make sure the person's account usage and access rights are removed. The departing person should be interviewed if possible, so he/she can provide feedback about development needs and experiences. Well-arranged departure routines create a basis for positive co-operation with the person later and decrease the possibility of phenomena detrimental to the company arising in the future.

8.3.3 Occupational safety

Both legislation and increasingly also practical working life in Russia have begun to take an earnest attitude towards questions of occupational safety. The employer's liability is brought up at the latest when something regrettable happens. The same office questions of operating facility safety and liability hold true in a company's staff safety as in Finland. Large customer flows in a company have their own impact on the staff's safety risks. The company's staff must be insured against accidents, for example in the form of collective workplace insurance. In addition, the company must remember to take care of mandatory health insurance and mandatory pension insurance. The employees must be registered in a social fund and a pension fund. There is also a choice of broader voluntary insurances for health care, for example. They correspond to Finnish occupational health care services and their prices are negotiable. Good instructions can be found on Rosgosstrakh's and Ingostrakh's pages. Rosgosstrakh has the most extensive network of offices and representatives, which covers the entire country. Russian law does not obligate employers to take out accident insurance for employees, but a collective insurance is a recommendable way to take care of the matter. Reinsurance packages are also available for sea freight, other freight and extensive property damage, for example.

The employer must be familiar with Russian occupational safety norms so that the authorities do not find reason thereby to intervene in the organisation's operation. The operational safety norms are field-specific occupational safety regulations, which are listed in detail at <http://truddoc.narod.ru/>. The pages also contain detailed professional title-specific instructions on employees' rights and obligations.

According to the Russian Federation's labour legislation (TK, Labour codex), in recruiting employees or in changing their job description, employees must be informed about the health-related effects of their work. Employees must be trained and instructed in safe work methods, and the employer is obligated to insure employees in case of accidents and occupational diseases. Employees have the right to health examinations and if necessary, extra doctor's examinations. According to paragraph 212 of Russia's labour codex, the employer is obligated to see to the safety of the workplace, train and instruct employees to use safe work methods, prevent accidents, provide protective equipment needed on the job and inform about the risks of the job.

Certificate GOST 12.0.004 – 90 SSBT specifies the provision and content of safety instructions. A record of workplace safety training given to the employees must be entered in a special training logbook. Basic instructions includes general information about the organisation, occupational safety legislation, primary risk factors at the workplace in question, personal protection procedures, questions of crime safety, fire safety issues, prevention of terrorism and first aid skills. Refresher training should be arranged twice a year.

Training should be arranged even more often if work methods or risk factors change significantly. Occupational safety must meet currently effective norms with regard to cleanness and order, also (sanitary norms).

The employer's obligations also include ensuring that the workplace quality testing has been done (*attestatsija*) and a certificate has been granted as stipulated by Russia's ministry of labour in 1997. Certification of a safety quality system is considered one of the most important methods for supervising the level of safety and ensuring occupation safety in Russia (Petrov 2007, 61). In the certification process the safety of the workplace is examined with respect to factors of danger and possible detrimental effects of work methods on employees are assessed. The level of protection used by the employees is also inspected. Safety certification of a workplace must be done by a special testing commission at least every five years. An occupational safety certificate offers both the employees and the company the possibility to receive state aid and compensation according to the dangerousness and detrimentality of the work. An occupational safety inspection may even result in having to close down a workplace if occupational safety issues have been neglected.

Russia's labour codex grants women special protection to enjoy safe working conditions. Women may not be employed in certain heavy or dangerous jobs specified in the labour codex. The working conditions of pregnant women and women caring for under-three-year-old children or invalid children are specified in particular detail.

A job contract can be made with a person who is at least 16 years old, but someone under 18 may not do dangerous or heavy work or overtime or night work. Persons under 21 can be employed only after they have had a health examination. The labour codex also specifies vacation and free time on the basis of the demandingness of the work. In the far north, which also includes the Murmansk region, employees receive additional benefits like a longer vacation. The required content of a job contract is specified in detail on the labour legislation.

A good source of information in occupational safety issues is www.tehbez.ru, which provides detailed instructions on occupational safety by field. The same address also provides information about fire safety norms. A list of workplace and transport warning signs (chemical hazard, fire hazard, evacuation symbols, etc.) can be found at <http://www.atiis-ars.ru/>.

9 HIRING A SECURITY COMPANY

9.1 Background checks are important

Security companies in Russia can roughly be divided into guard companies and detective firms. Their tasks differ from each other, but many companies offer both guard and detective services. Guard companies (*ohrana*) focus on protecting property, freight and people. Detective services (*detektiv*) acquire and examine information and offer analysis services. The law on private guard and detective activity ("О частной детективной и охранной деятельности в РФ") regulates guard and detective operation in Russia. Over the years many guard and detective companies have become well-rounded experts in security that offer fire detector technology, alarm centre services, crime prevention solutions for buildings (e.g. metal door installation) and valuable goods transport and bodyguard services.

Guard companies and guard activity in Russia are roughly divided into three classes according to their basic functions: outsourced organisations closely associated with the militia administration (*vnevedomstvennaja*), private guard companies and corporate in-house security services. The militia administration's (MVD) security organisations primarily focus on guarding public premises. Private guard companies are commercial providers of security services for the private sector and corporate in-house security services concentrate on the internal and external security of their parent companies.

Companies in the field of security and guard companies do not necessarily have only a positive image among entrepreneurs. The roots of Russia's security field partly originate in the organised crime of the 1990s (Aromaa & Lehti 2001, 60). Guard companies can no longer afford to have such an image, and they have attempted to indicate their reliability and viability in the competitive market. In the 1990s and 2000s guard companies have recruited people with a background in security service, whose professional skill also includes corporate espionage. Because of these issues, it is in order to also check the background of guard companies. According to Kauko Aromaa and Martti Lehti (2001, 60 – 61), who have studied organised crime in St. Petersburg, in practice a guard company can only be assessed according to its operation, not its background or connections. A good guard company provides functional services for a reasonable price, adheres to agreements and lets the customer company take care of its business in peace. If one goes back far enough, it is always possible to find either former security service officers or persons with questionable connections in the background. A stably operating, reliable guard company can be found among companies that have experience in international operation and can present credible references. It is also good to know that in Russia's circumstances a guard company always controls the operation of other guard companies (competitors) (Loginov 2006, 23).



In the process of selecting a guard company, in the first phase it is worth relying on the recommendations of a reliable acquaintance company and in all cases on the authorities' views about prospective guard companies. The internal affairs administration MVD and its regional departments (UVD) supervise guard and detective service providers and maintain licences related to these companies. When a decision has been reached concerning a guard and/or detective company, said company's licence must be verified before making an agreement. There are a number of security companies in Russia that operate without a licence (Loginov 2006, 23). It is also necessary to find out how many years the company has operated and what type of employees work and have worked for the company. It is also good to know whether the employees possibly are athletes, former security service employees, militia-men or persons with a prosecuting office background.

Priority should be given to a security company with references from foreign companies or recommendations from these companies or foreign or Russian authorities. In Finland the ministry of internal affairs' supervisory unit in the field of security maintains a register of guard company permits (www.intermin.fi/intermin/hankkeet/yksityinenturva/). A corresponding list can best be found in Russia by contacting the militia administration directly. The official list of companies with a guard company permit that is available to the public on the Internet in Finland is a unique form of service for selecting credible companies in the Barents region (and Scandinavia). For example,

a corresponding list is not available directly from the Internet in Sweden, but it is quite easily obtained by contacting the provincial government, which supervises guard companies.

The following is a checklist that should be gone through carefully before using the services of a guard company. These issues should be examined before making an agreement:

- Period of validity of the operating licence. A licence can be obtained first for 3 years, after which it can be extended for 5 years at a time;
- How many licensed employees does the firm have, and is the company's staff capable of handling the task;
- What is the educational background of the security company's staff? At least the management should have a higher-level degree;
- The service price schedule. Cheap is not necessarily good, it may bring additional risk to the client company. The employees do not necessarily have motivation or professional skill, and devices and security equipment may be deficient;
- Possibility of using radios and communication devices and their modernness (over 100 MHz = modern device). Each radio phone must have a permit. A radio is the surest and quickest device in emergency situations;
- Does the firm have motor vehicles? They are absolutely necessary for quality operation. Does the company have special vehicles for valuable goods transports and experience in such transports;
- What is the clothing principle in different situations (a uniform indoors, civilian clothes outdoors when acting as a bodyguard);
- When asked, a stably operating guard company will tell a client how many sites it handles. All names may not necessarily be revealed;
- It is worth asking for references from former and current customers. In Russia even Russian companies use foreign customers as an indicator in quality assessment. If a guard company has foreign customers, it is an indication of stable, reliable operation;
- It is worth asking in which professional unions and associations the company participates or is advertised. Participation indicates the company's experience and activeness in the field. In particular, membership and active participation in the activities of foreign associations indicates that the company strives to keep its operation in accordance with generally and globally approved standards. For example, the cover organisation www.ansb.ru ;
- If everything is OK so far, an agreement is negotiated with the management of the guard company. Of course, it should take the company's tasks into careful consideration;
- A detailed guarding plan should be compiled with the company;
- Any difficulties of one's own company should not be concealed from the guard company. They know or will very quickly find out things.

If something is concealed it may affect the price or in the worst case be grounds for annulment of the agreement.

9.2 Agreement with a security company

A model agreement template is appended to this booklet, which can be used to check the content of an agreement made with a guard company. The content of the agreement takes into consideration any security needs brought forth by a security assessment. The following issues should be taken into consideration when making an agreement with a Russian guard company:

- Period of validity (termination, term of notice, time for presenting new terms, min 3 weeks);
- Arrangement of guard work (hours of work/week, guard sites and amount of work at each site, management information channels, contact person);
- Terms of payment (wages, vacation time, agreement on overtime);
- Terms of technical equipment and clothing (equipment supplied by the guard company, vehicles, radios, client's equipment);
- Guard posts and accompanying documentation, including logbooks and guestbooks;
- The client must provide the guard company with information about the most important/active customers and visitors and their vehicles;
- The guard company provides information about customers who have used similar services as the client;
- The client must know who will come to protect the site and the management must discuss with each person;
- The guard company must not place people at the site who are related to the client's employees;
- The client company's staff must be able to meet the staff of the guard company, with the exception of employees whose identity the guard company wishes to keep secret from the general public;
- The client must ascertain the guard company's employees' professional skill, operational readiness and capability, language skill, education and ability to handle observed information;
- The directors of the client and guard companies sign the agreement;
- The agreement must mention that technical equipment is used to support guarding in co-operation with the client and proposed by the guard company;
- Special valuable guarded sites must be mentioned in the agreement (large amounts of material), and the number of guards that must always be present (at least two);
- Possible abnormal situations and their management must be reviewed together;
- The agreement must specify what is done in case of fire, and what are the obligations of the guard company's employees. Guard

companies have the right to install fire detectors. A fire isn't a natural catastrophe, it must be mentioned separately in the agreement;

- Liability of the guard company/the client's insurance company in case of material damages if the client's company is attacked and this causes destruction, or if an employee of the guard company is found (by a court) to be guilty of neglect;
- The agreement should also mention that the client and authorities (UVD) have the right to supervise the guard company's operation;
- Communication equipment that are used and their suppliers and operating permits must be mentioned in the agreement;
- It must be remembered that a guard company does not have the right to collect compensation for the client from offenders for material damage caused by outsiders. Only the court has the right to enforce payment of compensation;
- The security company must have valid liability insurance.

In making an agreement it is necessary to verify the period of validity of the guard company's licence. The agreement period must end before the guard company's licence expires. The recommended agreement period is one year at a time. The licence is valid in a certain region, and the client company's point of operation must be located in that region. In addition to the licence, the state register number of the company's juristic person must be entered in the agreement. The guard company must also be able to indicate that it is listed by the tax authority. The locations of the guarded sites and lists of documents found at the sites, the routes of circuit security, the rights, obligations and work schedules of the guard company's employees (total working time) must appear in the agreement. It is recommendable that the following documents are found at the guard posts:

- Commission agreement between the client and service provider;
- Guarding instructions (basic information about the site, the site's special requirements, protection of property and access control, guard's obligations, ensuring general security at the site, operation during official inspections, operation in abnormal situations, tasks that are forbidden from guards). The instructions are approved by the client and service provider together;
- Diagrams of the guarded sites, including maps and lighting diagrams;
- Co-operation agreement between UVD, i.e. the authority that supervises guard company operation, and the service provider;
- UVD must be notified when guarding of the site begins;
- Copies of permit (licence), guard company's registration, UVD's approval of guards' work clothing and UVD's guard inspections at the site in question;
- List of contact information, including emergency numbers;
- Fire protection instructions and first aid instructions;

- Instructions for protecting against terrorism and explosives;
- Contact information and addresses of the client company's management, law enforcement authorities, fire department and rescue service;
- Guard's ID card, personal permit (guard permit) and passport copy;
- Logbooks (visitors, changes in duty, inspection rounds, inspections of technical equipment, arrival and departure of goods);
- List of names and verifications of people with the right to conduct different actions (inspections, material reception);
- Model templates of access permits;
- Receipt books for receiving premises, property, keys and service material in guard change situations;
- Diagrams of storage places for guarding equipment and keys;
- Description of guard tasks.

What does it cost to use a security company? As a rule, the expenses of physical and technical security solutions do not exceed 15 – 20 % of profits. Of course, the price also depends on the extent of the tasks. The following different sectors of guarding should be taken into consideration when making an agreement:

1. Guarding of rooms and buildings
2. Protection of equipment and property
3. Protection of staff
4. Protection of transports, especial valuable goods transports
5. Protection of security
6. Compilation of security plans

The tasks given to a guard company may vary according to the tailored needs of the client company. When considering business operation there is no need yet for physical guarding, but a guard company can be used to check the backgrounds of potential partners. One can also agree with a guard company on measures to be taken in case of possible extortion or corruption. Guard companies usually have methods for defusing an extortion situation or a demand for a bribe, for example, through negotiation. The assistance of a guard company does not, however, eliminate the need to notify the authorities about what happened. Information related to a demand for a bribe may be given anonymously using the regional administration's tip-off phone, for example (see the chapter Fighting corruption). Several Russian business guides warn against turning to crime organisations if problems arise. It is still regrettably common to request services from crime organisations. A commission may involve collecting a debt or ensuring security.

A commission given to a guard company may additionally involve searching for suitable, safe premises and finding out their ownership background, for example. When actual business operation become sure the guard company

can help in compiling security plans and technical security solutions (Security guide 2005, 28 – 29). Co-operation that begins in phases and proves to be good can continue once actual business operation is started. Russians themselves usually rely on the services of guard companies/security firms in the following cases:

1. Collection of delayed or unpaid payments;
2. Guarding of personal or family safety after threats or extortion;
3. Theft of freight shipments;
4. Office, vehicle, home or cabin burglaries;
5. In conjunction with theft of commercial information (theft of documents, copying, eavesdropping/recording of persons or calls, bribery of employees);
6. Storeroom theft and burglary and theft in stores;
7. Arson, destruction of property.

This list of Russians' manner of operating with guard companies differs from the view according to which hiring a security company must have a preventive purpose. Once a mishap has happened the cost of restoring the situation is doubled. It is very important to the client company that a guard company's employees adapt to and partially blend in with the work atmosphere and "environment" of the client company. An indifferent attitude by the guard company, a lack of working discipline and confrontations with the client company's employees are grounds for annulling the security agreement.

There is reason to agree on methodology with the entire staffs of both the guard company and the client company in cases where someone posing as an official comes to inspect the company's operation, for example in the form of a tax audit or fire inspection. The possible criminal dimension of an "inspection" should always be taken into consideration. The inspector's authorisation must always be verified from higher superiors and the office in question. A certificate of a completed inspection must immediately be left in the company and later a record of the inspection must be received from the authority in question. The name and workplace of the inspector must be entered in the company's guestbook or visitors' book. Responsibility for recording visits and checking identification must be agreed on with the guard company. If a law enforcement official arrives at the guarded organisation for some reason the guard must be able to check his/her identification and report the arrival to his/her superior.

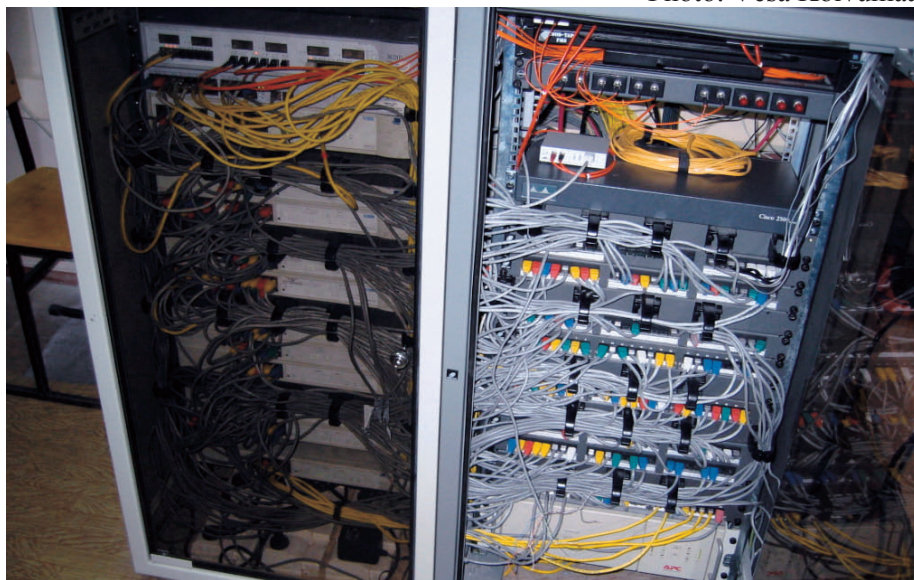
10 INFORMATION SECURITY

10.1 Security awareness must be increased

Information security is probably the most difficult sub-area of security to outline. The concept is broad and somewhat unspecified. It is not always possible to know what is meant by information security or how it can be enhanced. It is hard to grasp information security unless it is splintered into parts. Administrative information security, personal security, office security, equipment security and data processing security specify the concept in more detail. Specification and splintering are important because information security is not a visible security issue like the other sub-areas are.

In recent years many specialists have published literature on information security (see e.g., Miettinen 1999), providing good, generally applicable tools for developing a company's information security. There is no reason for this booklet to go into the general principles of information security, much less detailed lists of measures, because it would only be repeating issues covered already many times in the literature. The purpose of a guide to business security in Russia is to bring forth the special Russian characteristics of the policies of information and its protection.

Photo: Vesa Koivumaa



Information security guarantees the confidentiality, possession, integrity, authenticity, availability and beneficiality of information. Miettinen (1999, 44 – 47) emphasises that in the end information security is the responsibility of the management, even though the entire staff must be committed to the implementation of the company's information security programme, policy

and practices. Information security is a part of business culture. It is quality work in the company's daily operation as a part of integrated management. Information security protects data, computer programmes, physical property, premises and staff (see e.g., Security guide 2005, 34 – 40).

According to the ministry of trade and industry's survey of information security among SMEs, information security issues are poorly handled in small companies with less than five persons. The technical side of information security, i.e. firewall and virus protection, is arranged the best (over 90 % of the companies). However, insufficient attention is paid to administrative information security. Only one out of seven companies has a written information security plan and one-fifth of the companies have compiled an information security policy. Information security risks are also poorly assessed (KTM 2007).

If information security is a multi-tiered entity of issues in the Western business security mind-set, it is so in Russia, also. Russia's information sector is regulated by over fifty normative documents. Access to information is restricted in about twenty sections of society in Russia. Most of the norms are familiar from other European legal praxis: state secret, commercial secret, inviolability of private life, personal life secret, family secret, personal data, postal mailing, telephone conversation, documentary correspondence secret, professional secret, confidential information, official secret, banking secret, insurance secret, communication secret, secret of adoption, medical secret, preliminary investigation information and secret of legal procedure, secret of voting, secret of confession, meeting of judge secret, meeting of jury secret, notary's secret, advocator's secret, information on donor and recipient, military secret, content of discussions of constitutional court judges; immaterial secret (know-how).

10.2 Information security mind-set is built under state control

The information security doctrine is the highest political document in Russia, which guides the actions of Russia's legislative machine and executive administration in ensuring information security. The information security doctrine specifies the state-centred concept of information security and deals with methods for ensuring information security. The information security doctrine gives general rules of methodology for implementing security and reinforces the organisational basis of security regulations. The doctrine specifies types and sources of threats and administrative tasks and methods for ensuring security. The main tasks of the Russian Federation's government are specified in the doctrine. The organisational framework for achieving information security goals are specified in even more detail.

The Russian Federation's information security doctrine is the Russian state's official view on the goals, tasks, principles and main policies of the Federation's information security. The doctrine's main themes include ensuring the

state's security and the state's intervention in the principles of owning, producing and using information.

The Russian Federation's law on international exchange of information (passed 5.6.1996) on its part regulates the actions of physical and juristic persons in international exchange of information. According to the law, information security is the state and level of protection of society's information environment, which takes into account individual, organisation and state security. According to the law the Russian state does not restrict exporting of open information. Open information is specified as normative material such as legal documents, information about environmental conditions and possible emergency situations. Open information also includes meteorological, demographic and health-related information and other comparable information significant to ensuring the security of individuals, foreigners and population centres. Information that is restricted from international exchange of information includes state secrets and other confidential information, information related to general Russian national property and archive information if it is not marked as freely available. The spread of information brought from abroad is also restricted by law if it is intended for illegal purposes, such as destabilisation of the societal and legal systems or incitement against ethnic groups. Public spreading of false, forged and unreliable information brought from abroad is forbidden. This also touches advertising, the level of which is closely monitored in Russia.

The Russian Federation's law on information, information technology and information protection (ratified by the president 27.7.2006) is based on the tenet that information is a free legal virtue. According to the law an individual (physical person) and an organisation (juristic person) have the right to search for and receive all information in any form and from any source in accordance with the conditions specified in other laws of the Russian Federation and in this particular law (Sassali 2007).

A physical person has the right to receive information that directly touches his/her rights and obligations from state bodies, local autonomous bodies and officials working in them in the order specified in the Federation's laws. An organisation has the right to receive information that directly touches the organisation's rights and obligations from state and local autonomous bodies. An organisation also has the right to receive information that is necessary for co-operating with said bodies in order to achieve the goals set out in the organisation's charter.

The Federation's law on information, information technology and information protection gives all people, regardless of nationality, free access to:

a) normative, legal documents that touch the person's rights and obligations and regulate the organisation's legal status and the powers of state bodies and local autonomous bodies;

- b) information concerning the condition of the environment;
- c) information that tells about the operation of state and local autonomous bodies and use of budget resources, with the exception of state secrets and official secrets (employment secrets);
- d) information that is gathered into open library databases, museums and archives and state and municipal information systems, which are created and intended for individuals (physical persons) and organisations;
- e) other information not restricted by the Russian Federation's legislation.

State bodies and local autonomous bodies are obligated to provide access to information related to their operation. According to the law the information can be provided in either Russian or the national language of the republic. A person who wishes to access open information is not obligated to explain the purpose or necessity for receiving the information.

The fees charged for information provided by state or local autonomous bodies are specified in the Russian Federation's law on basis of payment. Decisions and actions (lack of action) of state bodies, local autonomous bodies, societal organisations and officials that violate the right to access information can be appealed to a higher body, higher official or the court. Losses must be compensated according to the methodology of civil law if:

- Access to information is prevented;
- Information is not provided without delay;
- Intentionally distorted information is given;
- Requested information is not given.

Information must be provided without charge if it touches:

- a) operation of state and local autonomous bodies, which said bodies have placed on the information-telecommunication network;
- b) information related to rights and obligations set forth in Federation's laws;
- c) other information specified by law.

Access to information is restricted when the objective is to protect constitutional order, state security and national defence, as well as ethics, health, and the rights and legal interests of juristic and physical persons. Adherence to the confidentiality of information is obligatory, and access to such information is restricted by a separate Federation law. Information related to state secrets is protected according to a special Federation law on state secrets. A Federation law also specifies what information is comprised of business secrets, official secrets and other secrets obligates such information to be kept confidential. The same law also specifies the liability for revealing such information.

Information that a physical person has received in carrying out professional duties, or an organisation has received in carrying out certain modes of operation (professional secrets), must be protected if the Federation's law obli-

gates these persons to enforce the confidentiality of said information. Information related to professional secrets may be turned over to a third party in the manner specified by the law and/or by court decision. A physical person may not be required to relinquish information about his/her private life, personal secrets and family secrets. No one is allowed to receive such information without the permission of the person in question unless otherwise stipulated in the Federation's legislation. The Russian Federation's law on personal data specifies access rights to physical persons' personal data.

Russia's law on personal data (ratified by President Vladimir Putin 27.7.2006) forbids collection and processing of personal data concerning race, nationality, political views, religious or philosophical beliefs, state of health and intimate life, except in cases specified in chapter 10, paragraph 2 of the law on personal data, i.e., under the following conditions:

- The person in question has given written permission;
- The personal data are generally available;
- The information is necessary to protect the life and health of the person in question or another person;
- To make a diagnosis for medical preventive purposes, handled by a medical professional who is sworn to secrecy;
- Handling of personal data of members of a societal or religious organisation, handled by said organisations in accordance with the Federation's law, if said handling achieves the legal purposes mentioned in the organisations' rules (basic documents) on condition that said personal data are not spread without written permission from the persons in question;
- For purposes of a court of law;
- For purposes derived from the law on security, operative detective work and enforcement of a legal decision.

From the standpoint of protecting information related to individuals, Russia's legislation is at quite a modern level. Problems are not caused by the deficiency of legislation, but by a lack of protection of information systems and modernity of information storage and distribution. Russians traditionally do not trust the security of information networks, for which reason use of the Internet in banking operation, for example, is in its early stages in Russia.

May it be mentioned that information on environmental pollution, fire safety issues, the health-related epidemiological situation, food safety and other factors with detrimental effects on safe operation of production plants and people's safety in general is not considered a business secret in Russia (Law on business secrets, paragraph 5).

According to a decision of the Russian government (No 35 5.12.1991, revised 3.10.2002), commercial secrets do not include the following information, which is turned over to the tax and law enforcement authorities:

- Company's establishment documents;
- Documents providing the right to business operation (company register data, information about existing patents and licences);
- Documents indicating solvency;
- Bookkeeping, if the information is needed to verify payment of taxes and other mandatory payments to the state;
- Size of staff, wages, work conditions and job vacancies;
- Documents indicating payment of taxes and other mandatory fees;
- Information about environmental pollution, violation of the anti-monopoly law, occupational safety violations, sale of products that are hazardous to health and other violations of the law.

In the process of privatising state and municipal enterprises, according to the aforementioned government decision commercial secrets do not include the following information, which may be turned over to law enforcement and tax authorities and the employee collective of the enterprise:

- The quantity of the enterprise's property and funds;
- Others' investments in the enterprise and debts;
- Monetary and agreement-based liabilities.

The above-mentioned information is primarily open to everyone. The law on commercial secrets specifies that secrets do not include information about establishment documents, licences, accounting, number of employees and the structure of the staff. Wage payment matters and occupational safety issues are also open information. Information concerning environmental pollution, fire safety, radiation and health situation and product safety is public. Also for background checks it is good to know that an employer's unpaid wages and social payments are public information. It is also not possible to conceal persons who have the right to act without a juristic person's letter of proxy. The public documents mentioned here speak their own language of the status of a company. The degree of publicity of non-commercial organisations is even broader. Information can be obtained about the quantity of their profits and property, their cost structure and the amount of free work done in the organisation (Fleishman 2006).

The law on commercial secrets allows such information to be labelled secret that concerns production operation (e.g. equipment, material and stores), production structure (individual administrative decisions, personal data), scientific and technical production data (methods), finances (content of accounting, balances, income, debts), plans (e.g. production expansion), investments, purchase and sales of product brands, marketing strategies, prod-

uct maintenance, sales methods and new (planned) services. The law allows some interpretation of what is actually or potentially valuable information from the standpoint of the company in question. Information about the customer base, partners (domestic and foreign clients, subcontractors), negotiations, agreements and goods suppliers are commercial secrets. Naturally, the company's security issues, such as alarm and guard systems, and methods for protecting commercial information are secret information. The company is obligated to make sure issues that are commercial secrets are classified in the company according to their access rights. The company must also be able to ensure that secrecy is implemented in practice. Questions of liability in commercial secrets in the company's partnerships must be laid out in the agreements. According to the law, secret folders and documents must be labelled "business secret" (Коммерческая тайна).

10.3 Practical view on information security

One way to approach information security is to divide information processing into operational procedures with which the existence of information is regulated. These operative classes, each being integrated with information security, are information *collection*, information *storage*, information *transfer*, information *destroying* (deletion) and information *recovery*.

The first operational procedure is information collection. The organisation *collects* (acquires) information that is directly related to the organisation's operation and goals. Essential from the standpoint of information safety is the types of sources from which the information is acquired and who acquires the information. For example, sources of information collected from the Internet may cause problems in the collecting organisation's information systems if various harmful programmes are hidden in the information. Visits to the site are registered there (by the site administrator), whereupon the acquiring party (computer) can be traced. If the information is acquired via a subcontractor, this agreement party may cause a security risk by revealing to a third party what information the company is currently interested in. The information may be gathered into electronic information systems or paper archives.

Information *storage* (saving) must happen in such a way and into such a place that outsiders and intruders cannot gain possession of the information. The information must remain intact, usable and reliable as long as it is needed by the organisation. Preservation of the information is ensured by means of backup copies located in a fireproof place protected against intruders, possibly even in a protected building or space separate from the organisation. This information can be stored in electronic form in information systems or as paper documents. The latter storage solution increases the need for physical guarding and security solutions. Backup copies and storage bring with them different kinds of space solutions that may be missing from the information system structures.

Information security risks associated with the *transfer* of information in electronic form are minimised by means of encryption programmes. The right to use encryption programmes and encryption in Russia must be verified through the security service FSB. The most powerful encryption programmes are not allowed because the authorities must be able to monitor telecommunication, if necessary. The security authorities monitor telecommunication on the basis of terrorism laws, among others. Permit practices resemble the corresponding encryption programme licensing systems of the United States. The authorities interfere if the encryption systems cannot be opened by the state authorities. The need to transport secret information on paper must be minimised. In this computer age it is easy to forget that transporting paper documents causes at least as large an information security risk as electronic transfer does.

Information must be *destroyed* (deleted) in such a way that no memory traces are left on backup copies, hard drives, films, etc. The hard drives must be removed from computers that are taken out of use and delivered to a company that is specialised in destroying information. Mechanical crushing of hard drives has been found to be the surest way to delete information in such a way that it cannot be recovered. The surest way to destroy paper documents is to use a paper shredder that cuts the paper into sufficiently small strips in crosswise directions. The resulting waste paper should be burned in a previously checked, reliable combustion plant in the presence of the owner of the information.

Information *recovery* is possible if the saved information is not irreversibly destroyed, for example mechanically. There are companies in Finland that are able to recover information from damaged computer hard drives. This technology is also developing in Russia. Backup copies of information or archive printouts are the best ways to prepare for information recovery should the actual operational disks be damaged.

The information security principles of Russia's Internet University (Internet University 2007) include preserving the usability, integrity and confidentiality of information and securing the infrastructure that supports these goals. According to the Internet University, the threats to computerised information systems and information are:

Active threats

- Unauthorised intrusion into information systems, both internally and externally (corporate espionage, hackers);
- Different types of harmful programmes (viruses, Trojan horses);
- Theft of equipment and support systems.

Passive threats

- Malfunctions and crashes of information systems;
- Power failures, natural catastrophes.

The Russians themselves have taken a very practical, if also a technical and supervisory approach to the information security of business operation (see e.g., Jushuk 2005). Even in Russia, information security is not only protecting information in computers, although it is a very important part of information security. The level of a company's information security can be raised considerably with inexpensive, relatively simple methods. Often it is not a question of using encryption programmes that are hard to understand or expensive information security solutions. Leaks of confidential information can be prevented and restricted using relatively clear-cut, inexpensive methods. In the first stage the company's premises are classified e.g. into three classes on the basis of the level of information security needed. The first class includes all open spaces (customer spaces) whose level of information security can be kept low. Office space primarily off-limits to customers and other areas used by the staff belong to the next information security level. Spaces with the highest level of protection are, for example, computer rooms, store-rooms for valuable goods, rooms containing important documents and archives and meeting rooms where confidential discussions are held.

Classification of the operating premises into security levels is also a prerequisite for planning access control and access rights. Classification of the access rights of the operating premises also helps in planning the staff's identification practices, which include access classes and ID card colours. According to the security classification of the premises, visitor reception spaces are set up in the zone with the lowest level of information security. Visitors are never left alone. If possible, visitor reception spaces are entered through security ports with metal detectors. Everyone who has travelled in Russia has noticed the seriousness with which access control is arranged in stores. Today book stores and shopping centres are most often entered through detectors. Usually they are meant to prevent shoplifting, but Russia is increasingly investing in preventing more serious crime, like terrorism, with the help of metal detectors.

From the standpoint of the confidentiality of information handled in business operation, different threatening scenarios of information leaks are emphasised in Russia. Company information may be lost through the following technical leakage points:

TABLE 2 Technical leakage points in an organisation's premises.

1. Listening devices within structures (walls, furniture, ventilation)	8. Directional microphones	15. Ground leaks
2. Papers left in a printer or copy machine, unprotected diskettes	9. Staff's information leaks	16. Leaks through fire detector devices
3. Video imaging, also from a distance	10. Unauthorised copying	17. Leaks through electrical wiring
4. Laser listening via window vibration	11. Terminal radiation	18. Use of heating, gas and water pipes
5. Production waste	12. Phone tapping	19. Computer diskettes, copies removed from use
6. Computer viruses, etc.	13. Measurement of electromagnetic radiation	
7. Theft of packages that contain information (e.g., folders)	14. Connecting to communication lines	

Unfortunately, an organisation's own employees have been found to cause the greatest risk of information leaks. Information may leak either unintentionally as a result of carelessness or intentionally to an external party with the intent to benefit. The company's management and security system have to control the firm's employees' access to confidential and secret information documents and databases containing such information. Each person, regardless of his/her position or relation to the firm's management, should only have access to information necessary for his/her job.

The confidentiality, integrity and usability of databases should be checked regularly, and at the same time the degree of secrecy of information and databases should be specified. Information becomes outdated quickly, so encryption updates are necessary. An encryption level classification should be created for the information system and a corresponding access right classification for the employees whose backgrounds have been carefully checked. Information is still often stored in manual folders in Russia. Important folders should be kept in fireproof safes. Supervision of handling of manual information involves creating a set of folders that contain important, confidential information. These folders are circulated among the people who need them against their receipt. The folders may also contain important bulletins for the staff members.

Protection of information technology and information in data networks is a part of information security. Computers must have access codes, preferably verified by each employee's personal electronic access card. Encryption programme solutions must be used to ensure the protection of local data networks against outside intruders. Virus protection and firewalls must be used like elsewhere in the world, and their continuous updating must be ensured.

Maintenance agreements for ADP devices, fax machines and copy machines guarantee that spare parts and service are available without delay. The backgrounds of device maintenance persons must be checked and the company's supervisor must be present while devices are serviced.

It was already mentioned that meeting rooms must be placed at the highest level of information security. A sound and signal isolated meeting room should be built for important negotiations, where outside employees are restricted from bringing mobile phones or other technical devices with which it would be possible to listen to the room. Eavesdropping and illicit viewing are issues that are not discussed much in conjunction with business operation in Finland, but they are downright commonplace issues in Russia. Even Russian security guides written for small companies regularly remind of the extent and commonness of this phenomenon in Russia. The guides give a wide variety of instructions for fighting against technical listening and viewing. The hermeticity of meeting rooms should be regularly checked with special technical devices. Technical devices are used to scan possible listening devices and discover devices installed in the walls. A thorough technical security inspection also includes current measurements of the room's phone lines and electrical wiring in case of extra people on the line. The room's through holes (pipes, computer cables, heating radiators, etc.) and adjoining rooms and rooms above and below should be checked to be totally sure of the security of the most important rooms. State embassy checks are regularly done this thoroughly, but usually only the largest companies invest in this type of activity. However, it is probably good to know that it is recommendable to conduct technical security inspections at least occasionally.

Although here we spoke about meeting rooms, one must remember to more often inspect the company's public spaces, WCs and hallways, where listening devices may be installed at any time. The local security company knows who conducts such security inspections. Service ordered from Finland is a viable alternative.

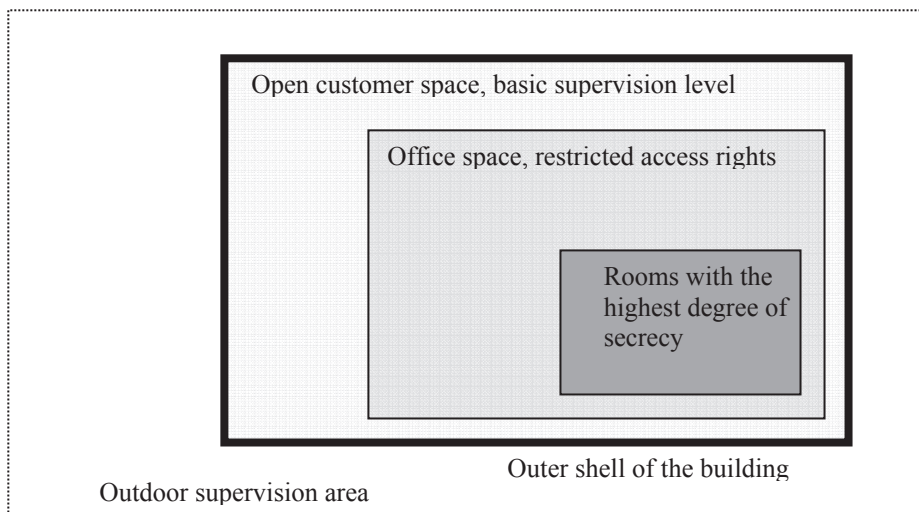


DIAGRAM 1 (Information) security classification model for an organisation's premises, modified from Miettinen's diagram (1999, 95).

Information security is taken into consideration in everyday office work, for example, by minimising and regulating copying (copy accounting, personal codes). In addition paper shredders are purchased and used in a way that promotes security. Only the company's management and person responsible for security may destroy secret and confidential material. Final destroying of the material is done by a reliable specialised company. When the company removes computers from use, their hard disks must be destroyed by mechanically crushing them or bringing them to Finland to be destroyed by a specialised company. Papers containing significant information must not be left lying around near fax machines and copy machines. The list of sent faxes in the memory of a fax machine must be regularly deleted so that telecommunication and addresses are not revealed to outsiders.

Information security naturally also includes special protection of confidential and (at a different level) secret information if such information for some reason needs to be transported outside the company. Physical supervision of sensitive documents and equipment must be continuous. Documents that may be valuable from the standpoint of a competitor or an espionage or criminal organisation must not be left in hotel rooms or hotel safe boxes without reliable supervision. If one wishes to follow information security practices very strictly, use of fax machines or one's own computer on a network should be avoided in hotels, company service buildings, Internet coffee shops and other similar public places. The company's blank documents, agreement templates and stamps must be kept in a place that is protected from outsiders.

The company's information security plan should also take a stand on personal material and disciplinary sanctions for revealing confidential material.

Questions of liability regarding confidential information must also be arranged in the case of temporary employees. The entire working community must be aware of the objectives and methodology of the company's information security plan. Motivation and the staff's commitment are necessary methods for raising security awareness. There are good international literature sources that deal with increasing security awareness, motivating the staff and thematic security training (see e.g., Roper, Grau & Fischer 2006).

The company should be careful about allowing temporary employees whose background has not been thoroughly checked to access confidential information. The company's management and people responsible for security should supervise their actions more closely than the actions of permanent employees. Temporary employees should be given clearly visible ID cards with restricted access rights. Colour-coded cards generally increase the effectiveness and noticeability of supervision. Subcontractor employees must also have an ID card in a visible place. They (their colours) indicate what their task is. Visitors must be escorted to important sites and their continuous supervision must be arranged.

The most important practices with which the level of information security and other physical security can be significantly raised were mentioned above. The purpose was not to list all of the many details. Here we presented the measures that especially often are repeated in Russian information security literature when speaking of practical measures carried out within a company. Information security is guaranteed with numerous small but simultaneous measures. Also in protecting information security, the company's staff is both in a key position and forms the most significant risk.

11 FIRE SAFETY AND RESCUE OPERATION

11.1 Fires are a common problem

Fires are a common problem in Russia. Gas and oil heating and the use of gas for cooking in homes increase the susceptibility to fires and explosions in residences. The fire safety regulations of Russia's emergency ministry (Emercom's decree 18.6.2003) provide detailed instructions for fire safety measures in residences and workplaces. Companies and their management are required to take care of fire safety. Companies, public buildings and residential apartment buildings must have valid rescue plans and fire prevention instructions. The staff at sites that are especially susceptible to fires, such as sawmills and constructions jobs, must be given training in what to do in an emergency. The fire department's emergency number must be placed in a visible place in buildings, stairways, offices, residences and storage rooms. According to the emergency ministry's decree, a separate place must be set aside for smoking. Smoking is forbidden at industrial sites where flammable materials or food products are handled.

Russia's fire safety norms are derived from the 1994 fire safety law (revised in 1995) and fire safety statutes, instructions, standards and regional fire safety laws and regulations. According to the fire safety regulations all organisations must have at least a general organisation-wide rescue plan that covers the staff's procedures in case of a fire, takes stock of and specifies fire safety equipment and their location, indicates evacuation routes, provides supplementary instructions and specifies when fire drills are to be held. According to the fire safety instructions, organisations must have specific places for smoking, procedures for making electrical equipment safe in conjunction with a fire, instructions concerning the staff's procedures in case of a fire, a person who is responsible for fire safety and in-house fire protection training specified for the organisation (Petrov 2007, 176).

Emercom's regulations include a detail specifying that if over 10 people work or stay on a floor simultaneously, an evacuation plan (instructions) and a procedure for notifying of a fire must be posted in a visible place on that floor. An evacuation plan contains written instructions and a diagram. For this reason, for example international hotels in Russia have put a visible effort into fire safety and smoothly executed evacuation. Anyone who has travelled around the world may even note that Russia is quite progressive in informing about fire safety. The author of this booklet has noted that in London, for example, there is no guarantee of visible fire safety instructions in hotels.

In Russia, if over 50 people stay in a building or room, in addition to an evacuation plan, an evacuation drill must be arranged twice a year. Special

additional fire safety requirements are specified if physically disabled, blind or deaf people stay in a room. Obligatory carefulness is also extended to the neatness of a company's premises if there is danger of fire.

The company must make sure fire detectors and extinguishers and rescue routes are in condition. The organisation must also have a plan in case of a power failure. The plan and practical structures must have a solution for finding initial extinguishing equipment and exit routes in the dark. The above-mentioned Emercom's regulations also specify the fire safety issues of stores and construction sites in detail. The company's management is responsible for fire safety, but at the practical level the contact person is the local fire inspector.

An active searcher can find good information and instructions from Russia's fire safety regulations. One important detail is that Emercom publishes a black list on its web pages containing sites whose fire safety is deficient or neglected. The nation-wide list occasionally mentions sites in Murmansk, also. The list of sites with a poor level of fire safety includes residential apartment buildings, for example (see Emercom 2007). The same list indicates the party responsible for fire safety issues at the site in question. An abundant number of residential buildings and schools with deficient fire safety is found in the Karelian Republic region. There is reason to check the black list if one intends to buy/rent apartments for the company's employees, for example, in Murmansk or elsewhere in Russia. However, one should not rely completely on web-based information. Of course it is always best to verify the fire safety of a building from the local fire inspector.

The risk of fires and gas explosions increases in winter when electric heaters are heavily loaded and gas consumption is at its peak. Every winter Russia's emergency ministry's local offices warn about the dangers of electric and gas equipment in homes and companies. The risks of these devices are of a completely different magnitude than in Finland. Even if we don't mention fire safety directly, power failures and problems with district heating supply are commonplace in Russia. The difficulties are emphasised especially during freezing temperatures, when the troubles they cause are also the greatest.

11.2 Rescue planning in co-operation with the authorities

Russia's authorities are strict about the fire safety of organisations. In Russia there are 100.1 deaths from fire per million inhabitants, while the corresponding figure in Finland is 21.6 (Myllyniemi 2000). The fire safety norms are quite complicated, and it is not possible to present an exhaustive list here. The details depend on things like the building's material, the type of use of the premises, the number of floors in the building and the nature of neighbouring buildings. It is not worth memorising these things; up-to-date information can be obtained by contacting the local fire inspector. Fulfilment of fire safety requirements should not be underestimated, because incomplete

fulfilment creates an additional reason to hinder business operation in possible future inspections. Quality guard companies also have information about fire safety issues and norms. Often security companies also have a licence to install fire safety equipment. The capacity to participate in fire safety planning should be verified when hiring a guard company for one's own company.

Fire inspections are everyday matters in Russia, and they have proved to be justified. For example, the prosecuting authority (procurator's office) in the Murmansk region has conducted fire inspections in various public sector buildings. In these inspections it has been noted that there are serious deficiencies in the operation of fire hoses in stairways, the markings and operation of fire extinguishers and the reach of firefighting vehicles, to name a few. Quite often exit routes and hallways are clogged and filled with flammable goods. Company premises do not necessarily have handheld fire extinguishers or there are not enough of them. These neglects usually result in administrative consequences, for instance fines.

The company's management is responsible for compiling and updating the company's rescue plan. The company's employees and others who participate in the implementation of the rescue plan must be informed of the plan. Having the company's staff participate in the compilation of the rescue plan in as early a stage as possible ensures – in addition to commitment – the staff's automatic action in case of an emergency. The plan or its summary must also be delivered to the region's rescue authority, which in practice is the local Emercom office, in accordance with the instructions of the Russian authorities.

Compilation of a rescue plan, which is an essential part of business security, begins with a mapping of predictable danger situations. Various tools have been developed for analysing risks directed towards the company, its staff and customers. One example on the Internet is found at <http://www.pk-rh.com>. In the rescue plan the company's security management classifies the risks directed towards the company in order of importance and probability and specified methods for managing each risk.

After identifying the risks of the workplace it is necessary to plan their management or elimination. It is not possible to eliminate all risks, so the company needs to find cost-effective methods for minimising risks. The rescue plan includes clear operating instructions in case of an emergency. The rescue plan is linked to the risk analysis where the analysis deals with fire and major accident risks and serious crime risks (bomb threat, terrorism), where quick rescue is needed. Naturally the company's risk analysis is more than merely mapping the challenges of fire and rescue procedures, as became apparent earlier in this booklet.

Rescue instructions include protecting oneself in an emergency and instructions for leaving the building. The preparation regulations of both Finland and Russia stipulate that in case of a fire or bomb threat it must be possible to evacuate the building as quickly as possible. Every working point in the company must have instructions on what to do in case of a fire or bomb threat. For example, in case of a threat received by phone, there is a clear operating code for ensuring one's own safety and identifying the person making the threat. The company must also have instructions and regular drills in case of threatening letters (hate-mail), mailed BC letters (so-called powder letters) and attempted robbery.

In case of a bomb threat, powder letter or fire, it must be possible to leave the building as quickly as possible and go to a prearranged, practiced gathering place. It must be possible to immediately warn those in danger using an in-house communication system, for example. According to Emercom's fire safety regulations, just like in Finland, exits and routes to them must be kept open and clearly marked. The possibility to protect oneself and protection procedures indoors in case of an accident caused by a hazardous material like a toxic chemical must be clarified. Russian rescue authorities have up-to-date lists of sites with dangerous operation in the locality and hazardous transports that pass through the locality. It is necessary to obtain this information for the company's security plan.

The rescue plan must take into consideration the need for preparation caused by dangerous sites. In an emergency the staff takes care of rescuing people and showing them the way to exit routes, sends an in-house alarm and reports the event to an emergency number, extinguishes and guides professional help to the site. The rescue staff may obligate the company's management or other company employees to provide additional information about possible new risk factors that are not known by the rescuers. For example, any chemicals temporarily stored in the building and the company's premises may form previously unknown dangers to the rescue authorities.

General instructions for identifying bomb letters are used world-wide. The appearance of bomb and powder letters is rare in Russia, and the topic is not covered in detail here. However, below is a model of how to proceed in case of a bomb threat:

Procedure in case of a bomb threat by phone

- **REMAIN CALM AND FRIENDLY!**
- **DON'T INTERRUPT THE CALLER – PROPOSE NEGOTIATION**
- **TRY TO KEEP THE CONVERSATION GOING!**
- **AUTOMATICALLY SWITCH ON THE CALL RECORDER!**
- **BEGIN TRACING THE CALL!**
- **ASK:**

- when will the bomb explode ?
- where is it ?
- what does it look like ?
- why has the bomb been installed ?

Wording of the bomb threat:

- The call came / did not come through the exchange
- IDENTITY OF THE PERSON MAKING THE BOMB THREAT:
man, woman, boy, girl
- VOICE OF THE PERSON MAKING THE BOMB THREAT:
high/shrill, quiet/weak, low, clear, mumbled, soft/pleasant
- SPEECH OF THE PERSON MAKING THE BOMB THREAT:
fast, slow, clear, distorted, vulgar, stammering, babbling, other,
what _____
- ACCENT OF THE PERSON MAKING THE BOMB THREAT: lo-
cal, foreign, accented, other,
what _____
- ATTITUDE OF THE PERSON MAKING THE BOMB THREAT:
peaceful, excited, other,
what _____
- BACKGROUND NOISES: noisy machinery, street noises, music,
people's voices, office machine noises, other, what

THREAT RECEIVED BY:

Date	Time	Name
-------------	-------------	-------------

Every workplace must have clear, visible operating instructions in case of different accidents or threatening situations. Below is a rough categorisation of operating instructions that a company should have in case of an accident, a dangerous situation or most common risks in business operation:

- Instructions for reporting an emergency, including phone numbers of different authorities;
- Procedure for making an in-house alarm;
- Information during accident situations;
- Serious traffic accident involving a company employee;
- Fire;
- Actions taken during a power, water or heating failure;
- Action in case of a gas leak and danger of a gas explosion;
- Mishap, sudden attack of illness;

- Serious active crime (robbery, other immediate threat);
- Bomb threat by phone (observations about the caller);
- Procedure in case of a threatening or extortion letter;
- Procedure in case of a powder letter;
- Procedure in case of an information system malfunction;
- Instructions for defusing/debriefing a work community crisis

In addition to these one must remember to tailor the instructions on the part of special situations caused by the company's field of operation. A food products company needs to prepare for possible poisoning threats and a transport company for possible hijacking threats. In practice, preparation means the company's staff must have access to inspected, functional initial extinguishers. They must know how to use them in an actual situation. Fire alarms, automatic sprinkling equipment, fire and smoke detectors, backup power supplies and exit route guides and security markings must be kept in condition and up to date. In addition to rescue and clearing equipment, personal protection and special equipment determined by the company's field of operation must be available in marked locations. The rescue authorities know the location of the nearest shelter and its usability in case of an emergency. The shelter and its capacity must be taken into consideration in the rescue plan.

In 2005 Murmansk's regional administration together with Emercom compiled an evacuation plan that covers a 30 km zone around the Kola nuclear power plant. The plan will be executed if a serious emergency occurs in the nuclear power plant. Persons within the zone will be evacuated as a co-operative effort with the region's companies, which fact must be taken into consideration in the civil defence plans of companies located near the zone, for example in the tourism sector (Kirovsk). More information can be obtained from the city's rescue authorities. In addition, companies operating anywhere in Russia must take nearby dangerous sites, such as chemical plants, nuclear power plants (nuclear waste plants) and gas and oil plants, into consideration in their civil defence plan. More information about these can be obtained from Emercom's local units.

12 CRIME SAFETY

12.1 Internal and external challenges

Due to the numerous different types of crime and criminal situations it is a demanding task to provide detailed instructions for preventing crime. Crime prevention in advance is naturally the most advantageous way to fight crime. Once a crime has happened, possible further measures must be chosen. In complainant offences the victim can choose what to do once a crime has happened; should it be reported to the authorities or should the consequences be quietly suffered? In business life it may have become practice to report ordinary street crime (theft, burglary and vandalism) to the authorities, but to remain quiet about corporate espionage, for example, which is considered troublesome from the standpoint of the company's public image. Progress in crime investigation depends much on how quickly the authorities receive information about the crime.

The threat of crime to business operation may be both external and internal by nature. Challenges posed by the company's staff are directed towards the company's physical and immaterial property, which again is linked to information security. The main reason why a company's critical information leaks to outsiders (competitors) is found in current or former employees. The company's working atmosphere and the employees' level of motivation are in a key position when attempting to prevent internal crime in the organisation. In Russia, the interviews and background checks that are part of the process of choosing the company's employees are considered the most important methods for preventing crime.

In some production plants internal crime has become a real problem. For example, loss of metals, especially coloured metals, from production plants is common in Russia. In their operation, large metal smelting plants rely on their own security services, whose primary task is to prevent internal theft of metal at the smelting plant. Material loss is also lowered by supervising shipments of goods arriving at and leaving from the company.

Crime risk management must take into account the following main items:

- Finished products, office equipment (ADP), vehicles and other property → persons responsible for receiving and dispatching;
- Staff reliability → prevention → background checks, see above;
- Increasing security awareness, each person given only what he/she needs to know;
- Compilation of a security programme, commitment of entire staff

Freight arriving at and leaving from the company needs to be continuously supervised. The liability of the receiver is verified with documents. In maintaining internal security, access rights and access control to a great extent

solve the problems of protecting the equipment that is most important from the standpoint of information security and production. Some matters belong to the knowledge of only a small group of people. The management of the company does not need to reveal the time of money transports or issues related to money storage, for example, to the staff. In these matters silence is golden, but chattering is a real find for a thief. This is the mind-set of Russian business security (Loginov 2006, 13).

Burglaries are by far the greatest challenge in threatening scenarios coming from the outside. For example, tens of burglaries of residences and offices are reported daily in the Murmansk city area. As a rule the challenge is that the more difficult it is made to access a company from the outside, the more probable it is that crime gangs attempt to enlist the company's staff for their own purposes. Criminals strive to discover the company's weakest points and paths for intrusion.

Extortion (Crime codex § 163)

Extortion is considered to be a demand to gain possession of another's property or property rights or to perform other property-related actions by threatening with violence or intent to destroy or damage the other's property, likewise by threatening the other or his/her family with intent to spread scurrilous information and other information that may significantly damage the rights or legal interests of the other or his/her family.

Technical protection (strong windows and doors), effective guarding and a crime detections system offer acceptable protection. The militia in the Murmansk region have publicly warned e.g. of certain ethnic groups who have control of the drug market in the city area. Statistics indicate that property crime is also constantly increasing. Such warnings from the authorities give reason to carefully consider the security of storing and transporting valuable goods, for example. Valuable goods should always be placed in a safe. Valuable property should not be visible to the street through the windows of an office (or residence). Valuable goods visible in a vehicle also invite burglaries. There is still much cash going around in Russia, so storing and transporting money poses a special risk.

A company in Russia has to operate under the close scrutiny of competitors. As mentioned at the beginning of this booklet, one of the first tasks of a company already when doing a market analysis is to identify the most important competitors in the region and possibly in the whole country. Knowing one's competitors, their nature and their way of operating provide the keys to arrange the company's economic security and crime prevention.

Common problems caused by crime in Russia are

- Promised payment for shipment is not received at all, or is not received in time;
- Freight theft, including the vehicle;
- Security threat to oneself or one's family;
- Burglaries of residences, offices, cabins, vehicles;
- Theft of commercial information, phone tapping, enlisting of employees;
- Burglaries of storerooms and production plants

In Russia competitors gather information about companies by means of corporate espionage, for one. These methods include enlisting staff members for monetary compensation, technological methods and possibly bribing officials who have key information about the company (patents, communication channels). Protection against corporate espionage should not even be left for a local security company to ponder, the management of the point of operation must have methods at hand that only the management knows about. An entire branch of literature on competitive intelligence has sprung up among business textbooks (see e.g., Jushuk 2005). More about these issues towards the end of this booklet.

12.2 Initial phase security investments

Security investments are the biggest during the initial phase of business operation. Among the first measures is to purchase a proper locking system. The previous owner of the premises may have copies of the keys to the premises, so it is very important to change the locks. A safe is also part of a credible company's accessories in Russia. Naturally, the safe must be placed behind the most secure locks, primarily in the director's room. Nevertheless, it is not recommendable to store large amounts of cash in the office.

Ordering and installing security work for metal doors, window frames, ventilation channels and wall structures between floors reinforce the company's shell protection. The background of the installation company must be in order. The client must also make sure no extra devices (eavesdropping, illicit viewing) are installed in the shell protection. Metal doors should not attract attention, but they should be disguised with a cloth, panel or leather coating. In double door solutions the inner door should be metal. Detailed instructions for security locks are also available, which specify the distance between locks and reinforcement of the door jamb (lock area). A reliable security company can give the best instructions in these matters, also.

Fire protection devices, like alarms and initial extinguishing equipment, must be installed in places specified in the fire protection plan. In these matters it is worth asking for advice from the local fire inspector. Fire safety equipment

installations are granted warranties, but subsequent maintenance agreements have to be made separately.

Renting a guard company is an essential part of a company's security investments, as explained earlier in this booklet. Some large Russian companies, for instance in the metal and mining industries, have solved their security guarding by establishing their own security service within the company. Such a solution is quite massive, and does not often come into question among SMEs. In Finland VAKES provides instructions and regulations for companies' burglary protection (see e.g., www.fkl.fi).

The staff's security awareness is the most important resource in business security. An external party can train the staff in security issues. Important tasks include practicing first aid skills and preparing for critical situations. This training may take place in Finland.

12.3 Acquiring basic information is important

The organisation's security person can become familiar with the locality's and region's crime situation already before the organisation's operation has started. The company must be aware of and list the worst competitors and criminals that cause the greatest potential risk. It is worth keeping up with the development of the locality's crime situation. Information can be obtained from the crime militia, Finland's embassies and corporate associations and networks and gathered together. The area's media are a very good source of information. Russian newspapers typically write about crimes and criminals and groups of organised crime by name in much more detail than they do in Finland.

The problem with official crime statistics is their incomparability with Finnish statistical practice. Finns should remember that crime statistics presented in public by the militia most often touch criminal law offences, which only tell the partial truth. Events listed under administrative law offences are not presented even though they are found in the statistics. By only presenting statistics under the criminal codex, crime statistics appear low in Russia. Because the militia leaves some reported crimes unregistered, this creates an additional problem in compiling and comparing statistics (Koistinen 2006, 99). Crimes that are most easily compared are offences against life and health, because there is no unclearness in interpreting them and in actuality they are all entered in the statistics. Statistics on serious crimes give a nearly true picture of the situation, and these annual statistics make it possible to draw conclusions about changes in the amount of serious crime.

Anyone, either a random tourist or someone living in the area, may come across ordinary street crime. Methods for preventing street crime are similar regardless of which country a person lives in. Metro tunnels and underground walkways should be avoided at night. The risk of becoming a victim of pick-

pocketing or even robbery is higher at railway stations, airports, market squares, tourist attractions and of course, restaurants and bars.

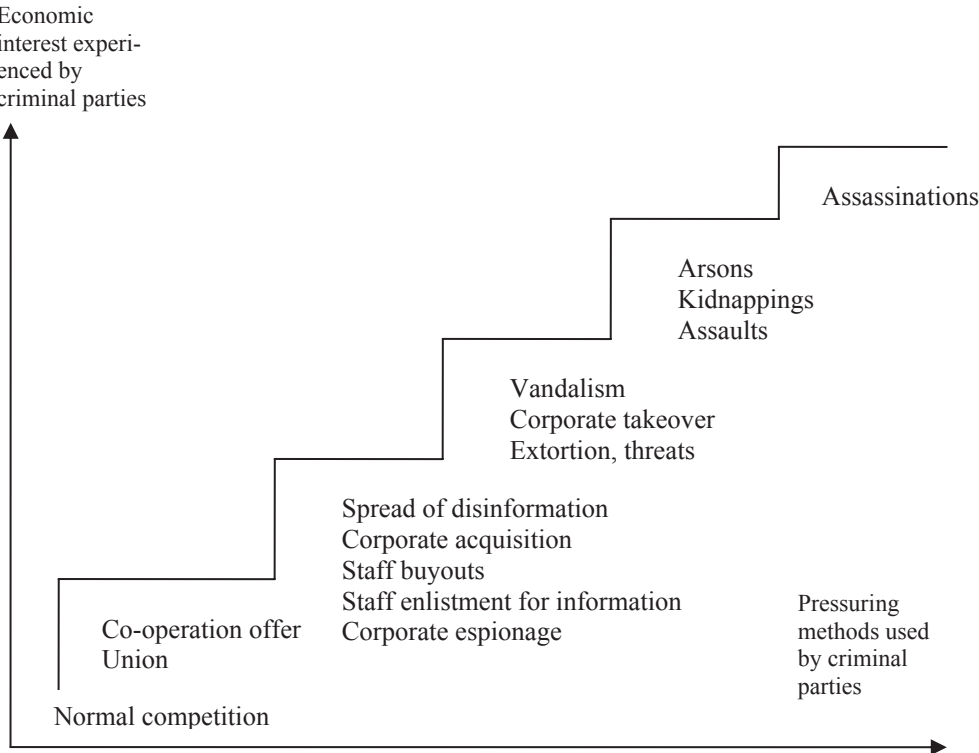


DIAGRAM 2 Interaction between economic interest and criminal methods.

Taking note of unusual phenomena near business operation or residence may help in preventing crime. Previously unnoticed vehicles or persons may loiter near the company premises. Also other forms of noticeable interest in the business operation, like photographing or observing a residence or company through the window, may be a sign of preparing a crime. Heightened interest before arrival of valuable goods transports is a very alarming indicator. Requests for technical information or floor plans of a building or company from the municipality's (district's, city's) technical office may also be a noteworthy sign (a warning example is Kuznetsov 2007, 42). Other things that point to preparation of a crime are questioning of the company's employees and neighbours and illicit intrusion into the company's premises to test the operation of alarm and guard systems.

The way in which e.g. a competitor may react depends the immediate threat or economic challenge he/she experiences. If the challenge is minor, ordinary information seeking methods are used. There may be an attempt to buy a

member of the competitor's staff or carry out other normal competitive actions. Perhaps there may be an attempt to entice customers away from the competitor. The firm may also possibly be purchased or taken over by the management. In the most serious cases extortion, threats, theft, damaging acts and sabotage enter the picture. Of course in the latter case the worst alternatives are murder attempts or arson.

It is recommendable to become familiar with the political stands of influential people in the region and locality. By following political rhetoric it is possible to determine whether some group is against foreign business and what kind of support there may be for foreign business operation. It has been especially interesting to follow election campaigns, in which persons with obscure backgrounds occasionally participate. At times the candidates for municipal and district offices and city mayors include persons about which the militia even publicly issue warnings. Law enforcement authorities are also active during regional and state Duma election campaigns.

12.4 Organised crime

Security officials' concern over organised crime is justified, as organised crime has an influence in many sectors in Russia. The most typical special areas of organised crime are vehicle theft, corruption, economic crimes, drug crimes, money laundering, smuggling, gambling and information technology crimes. Traditionally, organised crime in Russia is comprised of gangs formed by ethnic groups, but various groupings that depend on the situation are becoming common. Organised crime groups are made up of hierarchical organisations, in which the highest management stays at a distance from actual field. The gang leader is represented by trusted persons who manage those who do the dirty work.

According to Europol (2005), Russian organised crime groups that are also influential in Europe include Moscow's Solntsev mafia and St. Petersburg's Tambov mafia. These organisations are strong and well known in Russia. Despite having names that refer to specific localities, these gangs include several different nationalities or regional groups. According to Europol, Russian crime gangs influence in the EU area, for example in illegal human smuggling. The Baltic countries, in particular, are used as a transit area in smuggling people into Europe from the third world. Arranging illegal entry into the country is not an unknown phenomenon in the north, either. Citizens from third-world countries, mainly in Central Asia, the Near East, the Caucasus region and African countries, are continuously attempting to go to the West through the regions of the Republics of Murmansk and Karelia. This migration is controlled by organised crime and the main actors are probably located in Moscow and St. Petersburg.

Illegal transport of vehicles into Russia from the West is increasingly the work of crime gangs. According to Europol, vehicles are stolen from Europe

by disabling their stopper devices and brought to Russia and elsewhere in Eastern Europe with counterfeit registration certificates and modified identification markings. Finland is one transit country in this operation. According to Europol, Russian crime gangs are also specialised in money laundering and fraud. According to the National Bureau of Investigation (annual report 2005), organised crime in Russia and the Baltic region also participates in activities like double invoicing, receipt forgery and product counterfeiting.

Photo: Pekka Iivari



Thus, organised crime has also penetrated the double invoicing activity that takes place at the Russian border. In double invoicing Finnish customs is shown export documents containing actual purchase prices. Russian customs is shown counterfeit documents in which the prices are a fraction of the actual price. Thus, full customs tariffs and value-added taxes are only paid by honestly operating importers. The Finnish party or exporter operating in Finland is not guilty of committing a crime. Finnish sellers should be wary of entering any shady agreements with the intention of circumventing customs tariffs and taxes in Russia.

Upon discovery, double invoicing is investigated in Russia by law enforcement authorities. Double invoicing distorts competition, and this activity is even visible as differences between the foreign trade statistics of Finland and Russia. The differences between figures reported Finnish customs and Russia are significant especially in importing to Russia (Ollus 2006). It is good practice to transfer responsibility for customs clearance to the Russian trade part-

ner. Such a customs clause in the agreement avoids Russian customs officials' actions that could make exporting difficult.

One recent phenomenon is smuggling of valuable goods to Russia from the West via Finland. In August 2005 tons of mobile phones smuggled from Finland and Germany and on their way to Russia were confiscated. The intent was to have them cleared in customs as inexpensive mobile phones.

According to Europol, the main actors in crime related to business operation are found in the company's management. Management-level activity covers over half of discovered crimes. Employees form another critical part of crime. One-third of crimes are committed by employees. Mass crime comprises the most significant share of crime recorded in statistics. Organised crime participates in only one out of twenty crimes in the European Union area. Goods suppliers and customers form a very small portion of the threat of organised crime.

The prominence of crime caused by the staff is linked to the company's size, area of business and business culture. Staff crime is more common among large companies than in small ones. On the other hand, crimes against small units caused by the staff are most significant from the standpoint of the company's operation. The most common form of staff crime is theft by employees. This problem comes up particularly in grocery shops and construction companies. Some construction companies have noticed that giving tools against a receipt is a good way to prevent staff crime (Aromaa & Lehti 2001, 92 – 95). Using the company's property, tools, transport equipment and labour force for private purposes is the most common offence, which both the staff and management may be guilty of in a company. Ordering goods from a favoured party as a service in return is also an activity that at the least does not increase the economic efficiency of the organisation. Malpractices in matters related to travel expenses are also on the rise in Russia (Loginov 2006, 78).

A company's crime risk increases if the company's management is concentrated in one person without efficient supervision. Especially in Russia, the bookkeeper and manager are in a crucial position in crime prevention. The risk of crime grows very high if their recruitment has been unsuccessful or if it has been based on insufficient information.

Low work ethics in a company increases the danger of in-house crime and malpractice. A difference between the lifestyle and known income level of employees is also a noteworthy signal. A lack of background checks of potential customers and suppliers or poorly conducted checks are serious neglects.

12.5 Crime prevention

A company can reduce risks caused by crime through its own operation. All organisations should arrange their internal supervision in an effective but discreet way. Internal supervision should not give the picture that everyone in the company's staff is suspected of something. Such an atmosphere will only increase the risk of crime. The staff must be told of the existence of internal supervision at a joint staff meeting. At the same time they should be told the reasons for efficient supervision, which stem from ensuring the continuity of production and the success of the company. Internal supervision benefits everyone. That way no one is suspected without reason if something does happen. When the staff is aware of the preventive significance of supervision, everyone's commitment to maintain internal security can be obtained.

The staff's training and coaching should include instruction on how to detect crime prevention issues and guidelines for correct operating methods if someone suspects a crime is being committed or planned. Naturally, the training should emphasise the importance of careful action in preventing crime. Computers/databases should not be left open when leaving one's work site, papers containing company secrets should not be left visible, care should be taken with locking, etc. The company should arrange security days twice a year, where evacuation and fire prevention measures are practiced, but also the basics of crime prevention are reviewed. The company's prevention and feedback mechanisms of crime prevention should be linked to the company's broader quality operation and regularly updated quality document. For more in-depth training in crime prevention the company should rely on professional crime prevention experts.

Nevertheless, the company's own staff forms the company's single most important factor of stability. The staff is the quarter that is best and most quickly able to identify internal malpractices, which include theft. Some malpractices may come to light only after a long time. The staff must be encouraged to give feedback and they must be granted the possibility of reporting risks anonymously. Regular monitoring of goods flow and stock accounting must be arranged to be without loopholes. The right to use money and goods and the procedures involved must be verified at least as often. Receipt counterfeiting is even easier in Russia than in Finland, so one needs to be prepared for monetary malpractices.

On the other hand, the company's staff may lack the ability and will to address management-level malpractices. The management's involvement in bribery by outsiders is also a form of staff crime. The security risk of the staff can also be significantly reduced by familiarising the staff with the company's security factors. The staff must feel that their work is important. They need to feel they are a part of the company, a key factor in its production and services. The employees and entire work community need to be told why cautionary measures are taken. This prevents misunderstandings. The staff

will assist if their interests correlate with those of the management. Never can it be overemphasised that security measures also enhance the employees' security and ensure the company's future. Then the staff is able to fix attention on essential security issues.

Today employees must be required to be tactful and friendly towards other employees, customers and even competitors. This rule also works the other way. The company's management must be interested in the employees' opinions. It is especially important to listen to those who are responsible for the company's security. They know the company's weak points.

Co-operation with the authorities, other security operators (e.g. guard companies) and companies operating in the area provides information for the development of one's own company. The task of the company's management is to keep in regular contact with the locality's militia administration, rescue agency and of course, the management of the guard company in order to preserve good relationships, provide and receive feedback, and expand possibilities for co-operation. Regular exchange of information between companies and authorities is a part of normal co-operation, where current issues and crime risks are discussed. Building co-operation with different authorities is time-consuming, but mutually beneficial. Relationships develop by phases, and the objective must be to achieve permanent trust. The rapid staff turnover in Russia poses a challenge to forming relationships with the authorities. Just when one has learned to deal with one head official, he/she is replaced by another. However, this should not be allowed to affect organisational relationships. Forming relationships with new people is easier if the official organisation is familiar and prior contacts have been natural.

If a crime has happened, it must be immediately reported to both the crime investigation authorities and the insurance company. After a crime has happened the event and possible things leading to it must be gone over with the staff. Covering the matter with the staff may reveal valuable information for preventing similar events. Going over technical security items may reveal information leaks, for example. At the same time new technical ways to prevent access to documents may be found. Even though a crime (e.g. burglary) has not happened, it is necessary to test the condition of alarm equipment, crime detection and access control equipment. The availability of backup power must be verified so that crime detection device also work in case of a power failure. Illegal intrusions into the information network and buildings must be analysed and learned from. Weak points in physical and technical protection must be identified, preferably by oneself but possibly with the help of an outside expert.

General risk minimisation includes:

- Distribution of supervision, not the responsibility of one person;
- Malpractice information systems (feedback to staff, management);
- Interviews of departing employees (negative experiences, development ideas);
- Inspections and investigations;
- Continuous checks and updates of methodology;
- Support of a culture and atmosphere that oppose malpractice.

Many kinds of security instructions have been given in Russia to significant company managers, for example, in situations of heightened threat (kidnapping, extortion, murder). If a real danger is imminent, the management must enter and leave the building through different doors and at different times each day. If the organisation has only one entrance, it must be guarded 24 hours a day. Trips to the office should be avoided at times when one would have to be there alone. Unwanted people must be identified as quickly as possible. Such persons could stay near the building or in the hallways. The guards must be given the task of finding out who such people are. In case of extortion attempts the office (and/or home) should be equipped with a recording device that records the event. Even though a copy is delivered to the militia investigating organised crime, the original recording must be saved.

If a direct threat is directed at the staff, they should avoid unnecessarily being in front of a window. Their work point should be placed away from the window if it is possible to observe them from outside or a neighbouring building. It may be advisable to cover the window to prevent observation. Valuable object must not be visible through the window. On the other hand, covering the window should not cause a situation where an intruder is able to operate without fear of detection.

A reserved attitude should be taken towards all photographing, videotaping or interviewing at home. The time and duration of requested visits and the need to photograph must be determined in advance. Guarding must be arranged during the visit. No more people than agreed must be let inside. These guidelines also apply to interviews and visits at the workplace if the visitors are previously unknown.

12.6 Economic crime

In 2006 economic crime caused losses of 100 billion roubles in Russia, and over 50,000 people were convicted of economic crimes. The most common forms of economic crime are illegal business operation, contrived bankruptcy and company takeovers. The main tasks of Russia's ministry of internal affairs in preventing economic crime are fighting corruption and product counterfeiting and ensuring recovery of lost property (Nurgalijev 2007).

Russia's criminal law defines economic crime as a form of crime whose objects are ownership and production relationships and the economic rights of people, juristic persons, municipalities and the state. Economic crime is divided into offences against property (burglary, fraud, robbery, etc.), against economic operation (e.g. illegal business operation, illegal bank operation) and against the benefits of economic organisations (e.g. commercial bribery).

Photo: Pekka Iivari



Some of the most important economic crimes are fraud (crime codex § 159), e.g. loan fraud and illegal business operation (crime codex § 171), intentional bankruptcy (crime codex § 196) and tax offences. Product forgeries are nevertheless the most common and visible form of economic crime in Russia. According to Global Economic Crime Survey 2005, during the previous two years (2003 – 2004) nearly half of the companies operating in Central and Eastern Europe said they had been targets of economic crime. This is 25 percent more than in a similar study conducted in 2003 (Pricewaterhousecoopers 2005). Being a target of economic crime has traditionally been a sensitive topic that is not mentioned much in public in Russia. The above-mentioned Global Economic Survey noted that openness related to this topic has increased lately.

Corruption is the most feared area of economic crime, and in recent years fighting corruption has become a national project. However, Russian companies feel the most significant detrimental factor is abuse of office and overstepping of authority when dealing with the authorities. In addition to corrup-

tion and abuse of power, the most significant forms of economic crime against companies are seizure of shares and securities, falsification of accounting, abuse of inside information, product forgeries and money laundering.

It is very difficult to uncover companies' and organisations' internal malpractices, and most of them are unsolved or even unnoticed. The fact that about half of corporate financial offences are made by companies' upper management depicts the magnitude of this internal risk. Recovery of damages has also proved to be difficult. Over 70 percent of companies suffer the damages without compensation. Experience has shown that internal audits are the best aid in uncovering economic crime. Statistics indicate that a company's internal factors in economic crime are smaller in Russia than in Western countries. Studies show that this does not depict the actual situation regarding sources of crime, instead it indicates that companies' in-house crime prevention mechanisms are undeveloped. The most important factors leading to discovery of crime are:

- Internal and external source of information
- Internal audits
- Chance
- Tax and law enforcement authorities
- Security service
- Anonymous contact person in the management
- Staff changes
- Risk management systems

The aforementioned truths well reveal why in fighting economic crime special attention should be paid to developing internal control mechanisms. The company's management, including the accountant, is in a significant position in risk categorisation. Their actions can have an impact on a large share of economic crime. If the local management comes from Finland, the need to ensure the security of the staff (the person) is emphasised. In this conjunction it must be remembered, though that serious crime against foreign business managers is minimal in Russia.

Distributing responsibility for inspection among internal and external parties significantly decreases the possibility of economic malpractice. Fixed-term right to sign, use a bank account, take care of property and execute other authority provides additional opportunities for internal supervision. During the Soviet era staff rotation was one of the most important forms of supervising and preventing crimes (like corruption). The significance of staff rotation in crime prevention is still discussed in Russia (see e.g., Loginov 2006, 86). As poorly managed, unscheduled operation it may even increase the risk of crime due to possible lack of motivation among the staff and management.

Economic crime is a significant form of crime also in the regions of Russia. In the first two months of 2007 alone, 381 economic crimes were uncovered in the Murmansk region, which is 23 % more than in the corresponding period of the previous year. According to the Murmansk region's economic crime militia, this form of crime is growing strongly. Here it is important to note that according to the militia, economic crime is increasing the most in foreign trade. Economic crime is increasing the least in real estate trade and industry (Butjaikin 2007).

Counterfeit money is the branch of economic crime that both entrepreneurs and tourists will most likely encounter in Russia. There are counterfeit roubles, dollars and euros in circulation in Russia. In recent years some of this money has been brought to Finland. As far as traffic from Russia to Finland is concerned, the authenticity of bills and coins can be verified at border checks. If a company has become or is in danger of becoming a target of economic crime, a report of the offence should be made to the militia administration's economic crime department. The police contact person at the Finnish consulate should be kept informed of the event.

As became apparent in the above presentation, economic crime is linked to corruption. In addition to economic crime that targets business operation, corruption also causes damage to mutual interest in the form of abuse of state and municipal funds.

13 FIGHTING CORRUPTION

13.1 World-wide situation

Corruption is a broad entity of phenomena comprised of social, economic and political factors. The world-wide view on the content and concept of corruption is quite unanimous, but different countries have different views on prevention measures and their impact. Corruption disturbs society's political, economic, social and environmental development. The institutions of a democratic system lose their legitimacy if they are used for private benefits. Politically responsible leadership cannot develop in a corrupt society. Corruption significantly slows the growth of national wellness and fair distribution of wealth. Public resources in a corrupt society are not channelled well enough into infrastructure investments like schools, hospitals, roads or energy and public utility networks, which are so-called non-profitable, but necessary for the functioning of the society. Corruption also slows the formation of stable and predictable market and competition structures, thereby hindering investments in that sector. Corruption blooms in a society where *laissez-faire* joins with temptation. In such a society institutional supervision and control are missing or very weak, the decision-making process is obscure and the civic society is thin.

The most damaging aspect of corruption is its corrosive effect on the ethics of society and the social network. Trust in the political system, its institutions and leaders collapses among the people. Frustration and general (political) apathy further weaken the civic society. This again paves the way for authoritarian leadership and placing primacy on one's own benefits among officials in public structures. This forms a vicious circle that creates corruption, which has proved to be very difficult to break.

The damage caused by corruption cannot be measured with money, because the sums of bribes offered and paid are not systematically recorded. No one knows exactly how much money is spent each year to bribe officials. What's more, corruption does not always involve monetary investments, as other goods are used as instruments of bribery. Even if it were possible to measure the monetary amount of bribes caused by corruption, it still does not indicate the indirect political, economic and social losses caused by corruption.

Transparency International (transparency.org), which monitors the spread of corruption world-wide, has noted that corruption is not only a problem of the "poor south", the phenomenon is also strongly present in the "affluent northern" states. Corruption scandals are brought to light even in Germany, France, Japan, the USA and Great Britain, countries that one would expect to be free from this phenomenon. People are exactly as corrupt as the system allows. Administrative transparency and the media's status as a watchdog

serve as immediate mechanisms for fighting against and preventing corruption. In developed Western countries, especially in the Scandinavian countries, the societal culture that forestalls corruption is well developed, which is apparent from analyses produced by the aforementioned Transparency, for one.

According to Transparency International, in 2006 Finland was the world's least corrupt state. Immediately after Finland were Iceland, New Zealand, Denmark, Singapore, Sweden and Switzerland. Russia was in 127th place along with several African countries, even though Russia was in 95th place the previous year. Last were Iraq, Myanmar and Haiti, in 163rd place. According to the Global Corruption Barometer 2006, the police in Europe and North America are most often targets of bribery. The police as a profession are most often bribed in Africa and Latin America, as they also are in the former Soviet republics in Eastern Europe and Central Asia. World-wide, along with political parties and other political systems, the position of the police among professions as a target of corruption is overwhelming. In Russia the militia's share in corruption is strongly apparent.

World-wide it has been noted that people are very suspicious of governments' ability and desire to fight corruption. Only one out of five believe governments are capable of combating corruption. On the other hand, one out of six believes governments promote rather than fight corruption. In the USA and Great Britain 20 % of the people believe the government promotes corruption. Corruption is also believed to be present in the politics of the USA, Japan and even Iceland. Corruption in the developed Western countries is focused more in the direction of political parties.

Discussion about corruption often focuses on the party that accepts bribes. However, this is not the whole truth. To get a more complete picture it is necessary to determine which parties are more prone to offer bribes and thereby gain benefits. Transparency.org has studied the index of proneness to pay bribes on the part of the 30 leading industrial countries. The study lists the proneness of companies within each industrial country to pay bribes in their foreign operations. Swiss, Swedish and Australian companies are least prone to pay/offer bribes. Russia is located in 28th place. China and India are in the last two places.

There are numerous projects ongoing world-wide that are attempting to get a true picture of the extent of corruption and seeking tools with which to fight corruption. For example, in 2001 Lithuania investigated attitudes and personal experiences related to corruption by means of a questionnaire and proposed practical measures with the help of the Finnish and British consulates and the World Bank.

13.2 Corruption in Russia

Corruption has long historic roots in Russia that go back at least to the time of Peter the Great in the 1700s. Peter the Great attempted to use forcible measures, even the death threat, to eradicate corruption, but with poor results. The fight against corruption continued with Czar Nikolai I's establishment of a committee with the task of concentrating on the problem of small wages and corruption. Corruption increased in the courts of law in the mid-1800s, when Russia adopted jury courts.

Padding one's own personal income at the cost of performing one's official duties is the most important reason for high corruption also in today's Russia. After the revolution the Soviet Union initiated a vigorous campaign against corruption. Getting caught could even result in a death sentence. Regardless of the severe penalties and numerous efforts to fight corruption, it still lives on in Russia. It is one of the main characteristics of bad government. The political situation in North Caucasia and corruption that permeates everything are often mentioned as the two worst problems in today's Russia. They are considered the primary obstacles to Russia's development as a constitutional state and also a democratic country. According to a study conducted by INDEM (Indem.ru) in 2001, health care services, dealing with the traffic police, construction and repair work, higher education (getting accepted, transfers, exams, etc.) and social payments/paperwork were societal services in everyday life in Russia where it was necessary to give bribes in order to receive services. In 2005 their order had changed somewhat, but the amount of corruption had remained high or even slightly increased in 2000–2004. This is also clearly apparent from Transparency International's studies.

Although corruption has not decreased, social awareness of corruption and its impact has grown. According to experts, the current reasons for corruption are found in the errors of the transition phase and associated privatisation. President Putin has actively tried to include corruption and the fight against it in the government's agenda. The World Bank and the European Union have implemented extensive programmes against corruption and attempted to assist Russia's government so that corruption could be eradicated. In part the renewals have increased people's awareness and understanding of the problem of corruption, but the government has not been able to effectively address it. One reason for the lack of success of the renewals is the fact that corruption has permeated everyday life. The understanding that giving up corruption would cause the functionality of the service network to collapse is very widespread and accepted in Russia. On the other hand, corruption is increasingly being considered a negative phenomenon in Russia. With its anti-corruption programmes and regional anti-corruption measures the Russian government wishes to limit this negative phenomenon.

In 2006 Russia's procurator's office uncovered 6,546 cases in which bribes were accepted and 4,517 in which bribes were offered. According to Russia's

opinion poll centre (VTsIOM), 43 % of Russians feel the biggest cause of corruption is officials' greed and lack of ethics. According to 35 % of the respondents this is due to the state's inefficiency and a lack of laws. Eighteen percent feel the reason is the low level of the legal culture and respect for the law. The fields most susceptible to corruption in the everyday life of the Russian people are first of all the police and especially the traffic militia (acquiring a driver's licence, vehicle's technical condition, road traffic control), higher education (acceptance and exams), conscript service issues and repairs of residences. Based on the sums used for corruption, the turnover of the so-called corruption market is the greatest in the health care field, higher education, police operation and the court system. In addition to the traffic police and higher education, functions that are especially susceptible to corruption include conscript service (avoiding it) and official functions associated with basic education, assistance and protection provided by the militia, and acquiring housing and building plots. In recent years an increasing number of municipal and state officials in the central administration and regional levels have gotten caught for corruption.

According to the Indem fund, the average Russian business person paid a bribe twice last year. Last year as much as seven percent of the profits of companies in Russia were lost to corruption. Corruption hinders companies in more ways than lost income, since bribing does not support continuity and predictability. The typical bribe in Russia is €100. The country's custom is also visible abroad, where Russian companies look for partners that are accustomed to bribing.

Accepting a bribe (Crime codex § 290)

Accepting a bribe either personally or through a middleman in the form of money, securities or other property or benefits to carry out (or not carry out) an action for the benefit of the briber or his/her representative when said action is part of the acceptor's public duty or if the acceptor is able through his/her official position to promote said action, shield it or quietly approve it.

Offering a bribe (Crime codex § 291)

Offering a bribe to a competent person either personally or through a middleman.

The most corrupt in Russia are various state offices that grant licences or export quotas, privatisation authorities and persons responsible for transfers of budget funds to regions, for example. The amount of bribes equals 10 – 30 percent of the value of the business operation in question. According to experts' estimates, around \$240 million worth of bribes are paid in Russia per year, which is of the same magnitude as the annual income of Russia's state budget.

In Russia, corruption is a lifeline for organised crime. Up to half of the income of crime organisations is invested in corruption. It appears that corruption has even increased in Russia in recent years. Even in the CIS region the fight against corruption has not brought very good results. However, if business partners are selected correctly, a company will not necessarily face corruption in its business operation.

In 2006 Russia approved both the UN's anti-corruption agreement and the European Council's general penal agreement concerning corruption. Russia has been exhorted to also approve the corresponding civil agreement. The anti-corruption programme work currently ongoing in the regions and the state level is considered to have begun with President Vladimir Putin's speech at the Federation Council's meeting in May 2006. At the meeting Putin emphasised the primacy of fighting corruption and the significance of the phenomenon to national security. Another factor that nudged the matter forward was the discovery of extensive fraud in Russia's customs committee and the resulting reforms of Russia's customs administration. Outside pressure to go on with the corruption project came along with the responsibility of the chairmanship of the G8 countries.

The president's administration has expressed readiness to implement practical measures. On 24.11.2006 President Vladimir Putin signed an edict with which an anti-corruption council was formed within the president's administration. It has an advisory role, and through it the president shapes the directions of priority in fighting corruption. The six-member council has representatives from the government, the Duma, the Federation Council, the constitutional court, the Supreme Court and the court of arbitration. The head procurator's situation report is heard once a year and the council also compiles a separate report for the president every year. The council does not investigate concrete crimes or conduct inspections related to official offences.

Fighting corruption in economic life is implemented at the Federation level through an administrative reform programme for 2006 – 2008 set up by Russia's ministry of economic development and trade. The programme, which emphasises the significance of relations between administration and business life in fighting corruption, expresses concern over the relative weakening in recent years of many indicators that depict the business climate compared with corresponding indicators in Central and Eastern European countries and many CIS countries. Focusing of legislation is one of the most important measures in this sector. Licensing operation has been one of the factors in Russian government that has generated corruption. Licences are purchased or granted and extended based on fabricated grounds. When the legislative renewal in 2002 dropped the number of business forms requiring a licence, the number of associated corruption cases also dropped.

Various national-level studies have found the following sectors to be particularly problematic:

- Public administration's acquisition
- Business licences and permits
- Fire inspection and building supervision system
- Presumptive taxation, tax audit

The World Bank's document dealing with Russia mentions Finland as an example of fighting corruption, with particularly mention of legislation that improves the transparency of administration, openness in the preparation of laws and informing the people in advance about matters being prepared by the administration. Another good example that is mentioned is the principle of public hearing in land use planning, where documents are made available as announcements for public viewing on bulletin boards of municipal administration buildings and in the media. This administration's manner of operating is still unknown in Russia.

13.3 Fighting corruption in the Murmansk region

According to information provided by the Murmansk region's internal affairs administration, the number of corruption crimes is rising. While the total growth in Russia was about 13 %, there were 50 % more corruption crimes in the Murmansk region in the beginning of 2007 compared with the same period in the previous year. According to the Murmansk region's UVD, the growth in the number of discovered crimes is explained by more effective investigation. In 2006 72 cases in which officials were accused of corruption in the Murmansk region were brought to court. During ten months in 2006 128 reports of corruption-related crime were made in the Murmansk region. They involved suspected bribery, offences in office and offences against the state administration and local autonomy. In all, more and more persons in high posts in the Federation's administration in the Murmansk region have been found liable in corruption cases. In addition, small entrepreneurs have increasingly reported cases to the militia.

Education and health care are the most corrupt branches of administration in the Murmansk region. Teachers at schools and universities are caught for accepting bribes. The bribes are not only money, they may be goods or commercial inside information and securities. Monetary bribes paid to teachers or doctors amount to 2,000 – 30,000 roubles. The average bribe is about 15,000 roubles, which is more than the total average in Russia. Corruption cases are usually handled in the militia by the UVD's UBEP, i.e. the department against economic crime.

The corruption charge against the mayor of the city of Kandalaksa is probably one of last year's best known cases against the highest offices in the Murmansk region. The recently elected mayor, Vihorev (LDPR party) tried to bribe a councillor of the city council with 15,000 roubles to vote in a favourable way. Last year's corruption cases against known officials also include the Rostehnadzor, i.e. the technology and environmental inspection

agency's electrical inspection department case where Director Rodinin demanded 18,000 roubles from an entrepreneur to avoid problems in electrical inspection matters. In addition, on 9.11.2006 an employee in the UVD's UBEP's department responsible for loan fraud (!) was arrested.

In March 2007 the Murmansk region's procurator's office completed a preliminary investigation concerning a bribery case against the Murmansk region's traffic militia's (GIBDD) Kola district inspector and the traffic group's assistant director. The militiaman attempted to bribe another militiaman when he stopped a fish shipment belonging to the first militiaman. The documents of the vehicle transporting the fish were not in order. In the situation 7,000 roubles and 100 USD were offered to free the vehicle from the traffic militia's checkpoint. Both militiamen were caught.

By the middle of March 2007 the Kandalaksa militia together with the procurator's office started 5 preliminary investigations related to attempts to bribe the traffic militia. Drivers have tried to bribe employees at the traffic militia's checkpoint on the St. Petersburg-Murmansk highway with sums of 500 – 3,000 roubles so that preliminary investigations of traffic offences of the drivers would not be started.

One bribery case in the Murmansk region (in the spring of 2007) touches an inspector of the Petsamo district's traffic militia, who was found to have demanded a bribe of 3,000 roubles from a person driving under the influence of alcohol. The person turned to the Murmansk region's internal affairs administration's (UVD) security department (OSB). The inspector was condemned to 2 years of conditional imprisonment with a probation period of one year. Also in the nearby region the Kostamuksha procurator's office is accusing an official in the City of Kostamuksha's economic and construction administration of accepting bribes.

Below is an excerpt of bribery cases around Russia published by the Regnum news agency during a period of three days (20.3. – 22.3.2007) (see Butjaikin 2007):

- A case raised against the Murmansk region's traffic militia (GIBDD) goes to court
- A preliminary investigation of the district bailiff (*sudebnyi pristav*) of the Jaroslav region was started
- There was an attempt to bribe an investigator of the organised economic crime department in Voronezh
- The director of the Kargat district in the Novosibirsk region is suspected of bribery
- Two employees of Sverdlovsk's traffic militia (GIBDD) were bribed
- A traffic militia employee was sentenced for bribery in Udmurtia
- In 2006 the court in the Tomsk region sentenced 26 people for corruption crimes (receiving and accepting bribes)

- A wide web of corruption among customs officials was uncovered in Sverdlovsk
- A lawyer in Stavropol is suspected of abetting bribery
- A Tshuvass state university professor was arrested and accused of accepting bribes
- An official in Tomsk forged apartment sales documents for a bribe
- The director of the Federation's property office in Kalmykia privatised and illegally sold Federation property
- Two militiamen were arrested in Tjumen for extorting a bribe
- A gang that forged VIP licence plate numbers and complete registration documents and illegally sold emergency markings for vehicles was sentenced in Moscow. The gang included former foreign intelligence, internal affairs ministry and traffic militia employees
- An official in the Soviet district of Krasnojarsk was imprisoned for accepting bribes

For comparison, may it be mentioned that 500 corruption crimes were revealed in Tsheljabinsk in 2006. The crimes involved 272 officials and private individuals. According to Tsheljabinsk's UVD, corruption is most common in teaching, municipal housing, building plot distribution and use of budget funds. In 2006 315 bribery cases targeting officials were uncovered in Tatarstan. The number was 4.3 % higher than in the previous year. According to a sociological study conducted in Tatarstan, 56 % of the people were in a corruption situation in 2004, and 37 % in 2005. In 2006 568 corruption crimes were investigated and brought to court, and 379 people were sentenced. Altogether 8 corruption crime cases were raised against members of parliament and election organisations.

Commercial bribery (Crime codex § 204)

Illegal relinquishment of money, securities or other property to a person who works in the management of a commercial or other organisation, likewise illegal provision of property-like services as a return service for completing (or not completing) a task for the benefit of the bribe-giver. The crime is even more serious if it is repeatedly committed by a group of persons and premeditated, or by an organised group.

The regional government of Murmansk allotted 2,952,000 roubles to an anti-corruption programme in 2006 – 2008. The fight against corruption in the region progresses as a part of the national programme, for which purpose an inter-office council against corruption and economic criminalisation (MSPK) was established, chaired by an assistant governor from Murmansk's regional government. The Murmansk region has seen development of legislation as one of the most important methods for fighting corruption. A law concerning fighting corruption is becoming effective in the Murmansk region (О противодействии коррупции в Мурманской области).

In addition the inter-office council against corruption and economic criminalisation handles co-operation and co-ordination between the region's executive bodies and local autonomous units in anti-corruption policy. The council is implementing a preliminary project study of corruption and preparing a competition for a scientific sociological study on the topic with respect to the Murmansk region. Additionally, Internet pages for a regional government portal (<http://www.gov-murman.ru/anticorr/>) and a tip-off phone (phone no. 486400) for reporting corruption were established.

Murmansk's regional government's corruption programme includes the following measures, among others:

- questions related to organising state commissioned procurement
- anti-corruption mechanisms in staff policy
- analyses of degrees of corruption
- arranging anti-corruption measures in the most corrupt sectors
- development of internal supervision and analysis of corruption risks
- development of transparency of administration

The Murmansk region's government has sought to lower the threshold of uncovering corruption by adding informative activity. The regional administration requests notification of corruption, regardless of what level of state government it occurs in, to the following numbers located in the regional administration's information and administrative unit co-operation department:

- phone +78152 486 245 (office hours)
- fax +78152 486 231
- e-mail vzyatkamnet@amo.murman.ru
- tip-off phone +78152 486 400
- postal address: prospekt Lenina 75, 183006 Murmansk

Notification may also be sent anonymously by e-mail to mail.ru, mail.yandex.ru, mail.rambler.ru

The tip-off or complaint must include the following information:

- concretely what type of violation of rights is in question
- time and place
- how the crime happened
- how you feel the crime was an offence in office
- is there any material evidence
- are there any witnesses
- how you can be contacted for more information

The militia administration's (UVD) internal security department is also the correct address if you come across corruption in the militia. The regional administration's information and administrative co-operation department monitors corruption in the Murmansk region related to the region's executive

administration's operation. The following offences by officials should be reported to the department:

- breaches of agreements related to state acquisitions
- competition offences
- malpractice related fulfilment of agreements
- fabricated agreements
- goods counterfeiting
- price distortion
- unclear payment of deliveries, wages, etc.
- bribes, gifts, other valuable goods
- participation in business operation, transfer of user rights
- shares in firms
- abetting bribery
- wrongful use of the region's budget
- officials' trips abroad using funds of physical or juristic persons
- use of state property for something other than official business
- spreading of confidential information
- use of official position for election campaigns and the interests of political parties

14 ECONOMIC SECURITY

Economic security (экономическая безопасность) in Russia is both a company-level and state-level concept that appears frequently, not only in business discussions but also in conjunction with national security. Economic security is a newcomer in the vocabulary of economics, and its meaning is not established. At the business level economic security is a situation where a company's (organisation's) financial administrative position is not threatened and continuity is guaranteed. At the state level economic security refers to the entity formed by the state's productive resources (human activity) and natural resources (independent of humans), which maintains the state's external and internal capacity to perform. Economic security is an economic state that guarantees stable economic growth, satisfaction of economic needs and control of national resources.

Real estate reserves and financial resources contribute to economic security. Most typically economic security is emphasised in the significance of oil and gas reserves and mineral wealth to the Russian economy. These resources form a significant share of Russia's national security. Thus, Russia strives to keep the most important resources of national security completely under its own decision-making power. The population's standard of living and quality of life, the rate of inflation, unemployment, the economic structure, economic criminalisation, the technical foundation of economic life, research and development expenses, economic openness, competitiveness, dependency on imports, GNP and the national debt are indicators of economic security at the state level. In business operation economic security is comprised of the management's ability to see the most important factors and the threats and opportunities that affect the organisation's economic endurance.

Who, then, are the key persons who create and maintain economic security within an organisation? In Russia the accountant along with the company's management is in a key position in successful business operation. An incompetent accountant can cause irrecoverable damage to the company. Indifferent and incompetent management quickly results in matters being transferred from the hands of the company to the responsibility of the tax inspection agency. Saving in the quality of the accountant may backfire as higher tax payments. It is worth paying for a good accountant, otherwise it will be necessary to rely on the services of specialists and consultants. A good auditing company can provide hints on where, why and on the basis of which documents that company can save, or alternatively lose money. Money used for consultation comes back and the management can use the acquired information to monitor the accountant's expertise. Internal and external threats may undermine economic security. The following threats are perhaps exotic to

Finns, but they are common phenomena in Russian (international) business culture; corporate espionage, competitive intelligence and takeovers.

14.1 Corporate espionage

Corporate espionage and closely related industrial espionage are not excluded threats in domestic or foreign business operation. Corporate espionage refers to aggressive information acquisition directed towards a company's success factors, like patents, staff, marketing, customers and economic situation and also the company's weak points with the purpose of benefiting a competitor, authorities or some other quarter. Corporate espionage involves using illegal methods to acquire a company's information resources for one's own use. The goal is, for example, to avoid expensive R&D costs by acquiring a shortcut to the market. Corporate and industrial espionage are illegal information acquisition methods that lead to criminal sanctions if one is caught using them. Corporate and industrial espionage should be kept apart from competitive intelligence, which is based on legal methods and happens as a part of normal competitive situations.

Photo: Pekka Iivari



There is strong discussion in Russia about corporate espionage (*delovaya razvedka*) and commercial intelligence (*kommercheskaya razvedka*, competitive intelligence, business intelligence) and competitive intelligence (конкурентная разведка, konkurentnaya razvedka). It must be remembered that when the Soviet Union disintegrated and for several years thereafter, a significant number of espionage professionals with good language skills, analytical skills, technical skills and good connections to the state administration moved from the KGB, i.e. the state's espionage sector, to the business world. These people brought with them an active information acquisition culture to the business world.

Corporate espionage is counted as one of the most important factors affecting economic security. The most common methods of corporate espionage are creation of an information supplier system within a competing company or in its immediate vicinity. An information supplier or agent system is used to acquire secret and confidential information about the company and its area of business. The company's financial situation is monitored and information crucial to competition is stolen. Information acquisition is often directed towards the organisation's management. Compromising information about the managers or owners may be obtained in order to pressure the company to make decisions agreeable to a competitor. Threatening with crime issues that regrettable from the standpoint of publicity comes into question as one dirty extortion method. Corporate espionage may also appear as simple vandalism, for example destruction of information or equipment. A new phenomenon is spying related to the company's logistics, production of hazardous materials or foreign contacts, with the goal of acquiring information for the purpose of planning and implementing terrorist strikes.

Thus, corporate espionage is continuous and systematic acquisition, processing and analysis of information needed for optimal decision-making. Corporate espionage processes include:

- Initially, acquiring such information that is not yet knowledge;
- Arrangement of information, changing it to knowledge, saving and analysing it;
- Information synthesis and productisation as an achievement of corporate espionage;
- Strategic and tactical decision-making;
- Decision-making becoming concrete operation and results

Certain indicators of illicit activity within a company:

- Staff working at unusual times of the day;
- Telecommunication to foreign addresses in large volumes and at unusual times of the day;
- A person travelling abroad alone and often taking care of tasks that do not appear directly connected to the company's interests;
- Work meetings with people not known by the others and not introduced to the others;
- Bringing documents outside of the workplace.

The processes of corporate espionage can in themselves be applied to many kinds of information processing and conversion to knowledge. A person with a background of corporate espionage may be a good defender of his/her own organisation.

14.2 Competitive intelligence

Corporate espionage starts from collecting basic information about a competitor using legal methods, thus initially resembling competitive intelli-

gence. Later this acquisition of information becomes illegal activity, or spying. Competitive intelligence methods are well suited to the legal initial phases of corporate espionage. The line between it and the methods used in background checks is also subtle. Competitive intelligence consists of collecting at least the following information.

- Official data on the management and shareholders, addresses;
- Management's background, possible crimes, nature;
- Relations with influential people;
- Contacts abroad;
- Juristic and actual addresses, contact information, company registration number;
- Bank information, accounts;
- Management's and establishers' presence in other firms, their property;
- Company's goods flow, transport routes, storeroom locations;
- Financial, staff management and management's situation;
- In-house information transfer mechanisms;
- Internal business structure (distribution of responsibility, relations between superiors), unofficial internal influential relations;
- Investigation of internal and external market risks and customer relations;
- Illicit use of trademarks and unfair competition;
- Effect of underground economy on business operation;
- Relatives of people in the company employed by a competitor;
- Information leak points.

Information acquisition should also happen in the opposite direction. One should not only allow competitors to gather information about the company's operation. An entrepreneur in Russia should have an extensive file of the most important foreign and Russian competitors. According to Kuznetsov (2007, 94), gathering information about competitors serves the company's economic security.

Monitoring various sources of information belongs to the information acquisition phase. As already mentioned, analysts feel most of the information that concerns the competitor's intentions, even secret plans, is available from open sources. Competitive intelligence does not require a large budget. An alert competitor utilises at least the following sources, which are constantly monitored:

- Media, special literature, unconsidered statements in interviews, job vacancies;
- Unconsidered statements and speeches in other public places, like modes of transport (airplane);

- Internet, which provides information about products, people, companies, plans, customers, new products, etc.;
- Exhibitions, conferences, seminars. Here it is possible to make observations about a competitor's future customer relations, sales network, strategies or planned product innovations including test data and possible partners;
- Free discussions with the competitor's colleagues, customers and partners may reveal new information about the competitor;
- Turning directly to law enforcement, tax and register authorities (see background checks). The authorities provide information about the company's addresses, establishers and registration;
- It is customary to acquire a new product from the market to determine the structure of the product;
- Special computer programmes are available with which it is possible to acquire, arrange and analyse information and make predictions;
- A large company leaves many kinds of traces in customs and abroad;
- There are also an undetermined number of former employees, consultants and experts who at some time have been in contact with the object of information acquisition.

Also helpful in information acquisition:

- Joint operation with other companies;
- Negotiation situations;
- Visits to the company;
- Interviews, articles, advertisements;
- Outside consultants;
- Co-operation with the intent of acquiring information;
- Various inquiries, questionnaires conducted for scientific purposes;
- Free discussions with the staff.

Information analysis is at least as demanding a part of competitive intelligence as is information acquisition. Again there are many methods that facilitate analysis. Analysis is also used to determine a competitor's weak points. It is not enough that a product is first-class and there is a demand for it, it is necessary to create logistics for its distribution. The distribution system is the weak link of some companies. By acquiring the logistics company for itself a competitor has simultaneously gained possession of the product and its distribution. A company's vulnerability increases if its success relies on one or a few rare specialists. A competitor may find it best to buy the specialists for itself.

What benefits can competitive intelligence give a company? According to Jushtshuk (2005, 65–75), the purpose of intelligence is to predict the future and avoid being taken unawares. First of all intelligence must anticipate changes in the market. Monitoring market changes also includes anticipating

changes in the most important suppliers and the customer base. Naturally, competitive intelligence also anticipates competitors' operation. The third purpose is to reveal the emergence of new potential competitors that could challenge one's own operation. Fourth, intelligence is used to find ways to learn from the errors and successful solutions of other companies. Fifth, competitive intelligence has the task of acquiring and monitoring information related to patents and licences. Patents, or rather a lack of them, gives outside companies the possibility to patent methods used by others in one's own name if a product or method was not originally patented. Immediately after the fall of the Soviet Union, many foreign companies familiarised themselves with innovations used in the Soviet Union and patented them abroad.

According to Kuznetsov's broad view, at least the following should be known about a competitor:

- Full company name, juristic address, phone and fax numbers;
- Register number, registration date and address, the juristic form in which the company was established (OOO, ZAO, AO, OAO, TOO);
- Management's names, addresses and work backgrounds;
- Possible court procedures and property pledges related to the company and its management;
- Articles in newspapers, magazines and other publications;
- Banks used by the company and modes of payment;
- Company's financial situation during the past 3 years, investments, liquidity, debts;
- Names, locations and areas of business of subsidiaries, parent companies and affiliated companies;
- Partners and their areas of business;
- Connections to the underworld;
- Future outlook;
- Work organisation (technological level, know-how);
- Strategic and tactical plans and goals;
- Maintenance channels and modes of delivery to customers;
- Marketing instruments, price of work.

Furthermore competitive intelligence provides new information about the soundness of beginning new business operation and the possibilities of continuing business operation in chosen fields of business. Intelligence acquires information about new technologies, products and processes that may have an impact on the company's operation. Information is also acquired about political and legislative changes and other steering societal factors with an impact on business operation. Information about the development and functionality of new management methods in practical business life and their applicability in one's own operation is of no small significance. This is also investigated with well-arranged intelligence. Other tasks, sometimes even

crucial, are determining channels that leak confidential information and discovering a competitor's weak points and correctness of advertisements.

Legal analysis of a company is also intelligence, but permissible. Regardless of whether it is a question of state or corporate intelligence activity, a good analyst acquires most of the important information (according to some estimates up to 80–90 %) from open sources. The rest is produced using illegal intelligence methods that are already corporate espionage. Western security guides warn of many forms of market studies, for example, that are sent to companies in the form of questionnaires (see e.g., Roper et.al 2006, 287–288). Behind these questions may be a competitor's (or a state's) intelligence operation.

Signs of a groundless market study or questionnaire

- The questionnaire's Internet address is abroad;
- The questionnaire is conducted by a foreign company;
- The recipient has never met the sender;
- The questions touch clearly secret or confidential issues (pricing, customers, market plans, agreements);
- The questionnaire is sent to an individual employee rather than marketing or management;

Business security culture also includes determining the state of one's own company and threats caused by a competitor using competitive intelligence methods. The company's internal information acquisition seeks to prevent undesirable surprises coming from a competitor or some other quarter, for example someone operating inside one's own company. Systematic information acquisition by means of competitive intelligence involves resources and is one of the tasks of large companies' security organisations.

14.3 Takeovers

In a takeover a firm, its shares or its building plot ends up in someone else's hand in an ostensibly legal manner. In Russia a takeover is a known and recognised business domination phenomenon. Most company takeovers are done using legal but very aggressive methods. Takeover comes from the Russian term *zahvat*, which could also refer to seizure. Seizure again refers to an illegal operation. Such has also taken place in takeovers. Takeovers are divided into horizontal and vertical operations. In horizontal cases market area expansion happen by taking over a competitor. A direct vertical operation targets a potential or actual customer, while in a reverse vertical takeover a potential or actual supplier is placed under supervision. In addition to wider markets, vertical integration seeks a smaller cost price for products, a better possibility to plan stocks, new product and marketing methods and more efficient logistics. Igor Tunik and Vadim Poljakov (2007, 45), who are familiar with takeovers in Russia and the ICS countries, say that about 10,000 takeovers (*zahvat*) have been recorded in the CIS countries (incl. Russia)

during the past six years, in which 567 operations involved homicide. According to Tunik and Poljakov, this is only the tip of the iceberg. The bigger the company that is taken over, the more the raider is an ostensibly legal quarter, such as a known company or businessperson. Clearly criminal takeovers happen in small companies.

The most common methods and the most difficult to prevent in takeovers are changing controlling share ownership in a direction that is disadvantageous for the company being taken over. An apparently qualified majority share ownership is formed by means of an extraordinary general meeting to which shareholders that support a takeover, i.e. new management and ownership, are invited. The other shareholders are left uninvited, ostensibly by oversight, by "mistakenly" announcing the wrong meeting place or by denying that the invitation was not sent on time. Takeovers are also implemented by threatening with or using violence. Law enforcement officials are called in by the raider to forcibly remove the old management on the basis of the apparent general meeting.

Corrupt courts and militia are used to prevent shareholders from entering the meeting place on various pretexts. In addition, the old management is commanded, or asked, to voluntarily sell its shares to the new group of owners. According to statistics, in 70 % of takeovers the controlling shares are transferred to the raider, and 90 % of takeovers happen through share purchases (Tunik & Poljakov 2007, 30; 50). Majority share ownership or possession of controlling shares is just a method used to place one's "own" people in the management. Buying shares offers the possibility to participate and vote at general meetings. The actual goal is to acquire managership.

The objective of a takeover is to gain possession of the company (shares), building plot and building. The raider assesses whether the company is interesting from the standpoint of his/her own operation. He/she also assesses which methods should be applied in the case in question. A valuable piece of land causes most takeovers in Russia. Other motives for takeovers are redirection of company's business, elimination of competition in the market and enticing market outlooks (Tunik & Poljakov 2007, 24).

An actual takeover is preceded by long-term, detailed intelligence and analysis work that digs up the company's weak points. These weak points are used as a basis for deciding on the most usable ways to attack the company. Authorities (tax authority, militia, procurator's office) may be employed to obtain information in the form of company audits. The most important weak points are related to division of ownership of share capital, incurring of a debt and possibly also challenging a privatisation process. More detailed tactics are also formed in addition to the primary takeover strategies. The most often used tactics include seizure of debt capital and initiation of a contrived bankruptcy process. One administrative enticement is to promise the vice-chairman of the board a promotion or a good price for his/her shares. Some-

times the quarter planning a takeover needs to do a lot of work, for example in tracing the company's shareholders or beneficiaries (e.g. heirs), possibly even abroad.

Factors that make a company susceptible to a takeover

- Complex, scattered company ownership;
- Self-directed, uncontrolled management;
- Poor motivation of the management;
- Erroneous market analyses;
- Uncontrolled incurring of debt;
- Insufficient supervision of debts;
- Unfair treatment of minority shareholders;
- Unfair distribution of dividends.

Often the raider has used a supplementary issue of shares as a way to shift ownership to those who indicate loyalty to the new management. Old shareholders are also exhorted to sell their shares to new people. The raider may have found out the shareholders of a closed company (ZAO) from inside the company. Gaining possession of the shareholder register is one of the primary ways for a raider to achieve his/her actual objective. Having the company incur a debt is also considered a usable method for transferring ownership, for example by gaining possession of the debt or obligating the debtor to immediately pay the debt. Loan security often consists of property, so the property is transferred to the party that is able to pay the loan. The new owner may also offer to free the debtor from the debt in exchange for company property. If the old shareholders refuse, an extraordinary meeting can be convened where the company is placed in bankruptcy. The new owner then purchases the share capital and property for him/herself. In Finland a takeover and the preceding signals are called a cornering operation, which also has a fully legal basis.

Signs of a prospective takeover:

- Proposals to shareholders to sell their shares;
- Offers to pay debts;
- Information acquisition, e.g. from former employees;
- Artificial audits (tax authorities, other law enforcement officials);
- Direct threats;
- Proposals concerning board membership

Statistical information shows that every third takeover is achieved through share speculation. Thus, a takeover does not necessarily happen by illegal means. Wide publicity and juristic pressure are ways to prevent takeovers. Other furthering factors include relations with high-level law enforcement officials (see e.g., Russian Internet discussion on the topic at: <http://forum.rosinvest.com/showthread.php?t=59>).

A metal production plant operating in Russia had owners recorded as OOO Metal Company and its person living in Russia. The actual owners hid behind an offshore company registered in the Seychelles without direct contact with the metal company. They were only linked via XX Company registered in Hungary. XX Company had no operation, but money flowed into its account. XX Company's owners decided to invest this money in OOO Metal Company. Thereby XX Company became an owner of the metal company. The owners of the metal company wanted to protect it against a possible takeover by transferring small shares of the metal company OOO firms registered in Russia. The owners and directors of these OOO firms were nominal persons who were needed e.g. for reports to the tax authorities. However, the establishment documents of the OOO firms did not mention how the shares owned by the nominal persons would be transferred to the right owners of the metal company, if necessary. The right owners did not have methods with which to control the nominal directors of the OOO firms, in whose companies the metal company shares comprised varying proportions. Raiders made use of this situation. The raiders used fully legal methods to gain ownership of the metal company shares in the OOO firms and installed their own man to manage them. All that was needed was to purchase a majority share of XX company registered in Hungary to gain full control of the metal company (Source: Tunik & Poljakov 2007, 68 – 69).

Two milk product manufacturers competed in a certain area. One of them wanted to get rid of its competitor. The task proved to be difficult. After a thorough analysis it was determined that it would be difficult to take over the company via share purchases. The company also had no debt and it paid its taxes on time. There were no delivery problems, either. The raider decided on an extraordinary operation: The local waterworks company was coaxed to "repair the pipe-work" on the main pipeline entering the target company. The repair lasted a few weeks, considerably hindering the target company's operation. It was not able to meet the agreements made with clients and goods suppliers, whereupon it became liable for damages. The raiders had already agreed with one of the damaged parties that the target company would be placed under bankruptcy for breach of agreement. A strong competitor was brought to its knees within a few months (Source: Tunik & Poljakov 2007, 76 – 77).

Unestablished share capital, incurring a debt, an enticing business outlook, disputes between shareholders and stiff competition increase the risk of takeovers. A takeover can be preceded by a dirty publicity campaign and reports of offences of the target company, which turn the public and politicians against the management of the company. Using publicity and nowadays also the Internet to smear a company's image is increasing, not only in takeovers, but also in traditional competition. One of the purposes of a publicity campaign used in a takeover is also to create discord among the staff and shareholders. Unpaid wages or frustration among staff members that own company shares increases readiness to sell shares to the benefit of a raider. The company's management may be imprisoned even for a long time due to a preliminary investigation. During this time managership unavoidably slips into the hands of other people. The intent is to make the company ripe for selling shares to a competitor. It may not even be necessary to acquire a majority of shares; a visible position in the management is enough to allow the takeover to continue. Even temporary managership, for example while a legal proceeding related to a general meeting is ongoing, may be enough to permit completion of a sale of a valuable piece of land belonging to the company, for example. Even though a court determines that the decision of the general

meeting was made out of order, the land may nevertheless be already lost. The raider's objective was reached.

There may be one or several so-called buffer companies between the actual raider and the target company, which first acquire the share package and then sell it to raider. Arranging an extraordinary general meeting with one's own resources while leaving out the other shareholders is a method commonly used by raiders to transfer a company to new management. Getting rid of the management by assassination is naturally the worst possible method. Today, however, the primary methods used to transfer property are the courts, execution authorities and confiscation. Forged general meeting protocols and register markings are also commonly used takeover methods.

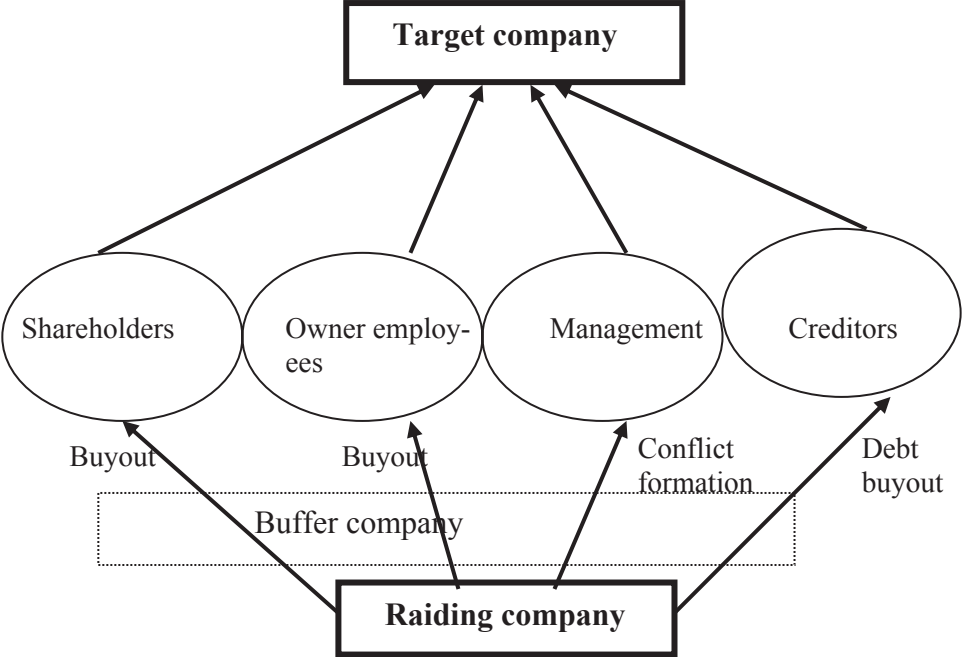


FIGURE 3 Takeover methods.

According to Aromaa & Lehti (2001, 75), the backgrounds of takeovers that took place in St. Petersburg in the 1990s were not linked to organised crime, although underworld methods were used. In two cases against Finns, one takeover was done by the Finnish company's Russian business partner and the other by the company's Russian staff led by the local Russian director.

There is no single recipe for protecting oneself against a takeover that can be applied to all companies. The methods of defence depend on many factors, such as the degree of advancement of a takeover and the structure of the company's decision-making and ownership. The main rule is that protecting oneself against a takeover is based on methods that are analogous but opposite to the methods used against the company by the attacker. Most important is to first of all identify ongoing aggression and initiate defensive measures

without delay. There are companies in Russia specialised in protecting against takeovers, and under the circumstances it is not rare to use their services. In any case paying for the services is less expensive than losing the company or its strategic reserves. Prompt action by the management and owners of the defending company is crucial in this situation.

A defence operation may fail if the possibility of a takeover has not even been considered. A lack of defence strategies and tactics takes the management and owners unawares and delays initiation of protective measures. Unsuccessful countermeasures may be caused by a delayed counterpurchase of shares, giving the raider a chance to acquire a controlling share. The company's security management alone may not have methods for thwarting such operations or protecting the company against them. Nevertheless, it is the task of the company's security service to identify increasing intelligence operation against the company as early as possible. All information flow cannot be monitored, since most of the information can be found in public sources. Authorities like the tax inspection agency, the share register, the real estate register and law enforcement authorities form a group whose operation can essentially be monitored and identified in an early phase (Tunik & Poljakov 2007, 138). Another even more important direction of monitoring and anticipation is inside the company itself. Property management must be arranged in the company's basic rules in such a way that a possible raider is not able to manipulate property without the shareholders' approval even if managership were transferred to the raider. Granting extensive property management authority, e.g. buying and selling, to the company's management, forms a major risk if such an exceptional situation arises.

Of course, centralised management of shares would be a strong strategic method of protection, as also specifying a limit to the share purchase price, making it impossible for an outside raider candidate to make an unhealthy price bid. During a takeover process it must be possible to quickly issue supplementary shares and temporarily freeze property. Anonymity of ownership and secrecy of the share register shield against attempted takeovers. Hiding behind holding companies and investment funds is also used as a protection method in the Russian business environment. The internal protection system is facilitated if each employee has clearly defined tasks. This is especially important among employees working with confidential and secret information. The most dazzling defence operations are implemented in the form of counterattacks. The target company has initiated a takeover operation directed at the raider, the success of which is based on information gathered about the raider in advance. In this type of countermeasure one must be certain that it is the raider who is making the takeover, and that the actual orderer of the job is not hiding behind the raider.

A company's structural changes provide long-term protection against takeover attempts. Nominal and "dead" shareholders and nominal directors must be eliminated. The establishment documents and rules must include the

names of all administrative bodies. No one must have the role of a grey eminence operating the background.

15 ENVIRONMENTAL SAFETY

15.1 Ecological mind-set as a competitive factor

Ecological or environmental safety is understood as a state of protecting people, society and the state against environmental effects originating from humans. The concept also includes protection against natural catastrophes. Environmental safety is a state of society in which a balance has been achieved between growth and consumption of natural resources. In recent years Russia has begun to value protection of the environmental state, although practical measure most often lag behind. It is a question of both money and attitude.

Promotion of environmental safety is considered an increasingly significant competitive factor also in Russian business operation. The environmental efficiency goals of production include lowering the consumption of water, electricity and gas or raising unit efficiency, decreasing waste and emissions created by production, and developing waste recycling. Decreasing accident proneness and risks serves to protect both the work environment and the natural surroundings. With an environmental pass a company can indicate that it takes care of the area's ecological state and the environmental friendliness of its production and operating processes.

A company's environmental policy programme indicates the company's commitment to an environmental mind-set. The company's eco-pass, which indicates achievement of certain minimum standards, can be made a part of the environmental programme. The standards include sustainable use of raw materials, waste recycling, observance of emission norms and taking care of the surrounding social environment.

15.2 Norms

The Russian Federation's environmental doctrine functions as the state's highest politico-normative environmental protection document. The government approved the doctrine on 31.8.2002. The doctrine is an extensive description of integration of environmental protection, living and industrial functions. Russia has a significant number of normative documents and laws pertaining to environmental safety (<http://ecoperm.ru/base.html>). The Federation's most important law is the law on environmental protection (об охране окружающей среды), which was passed on 10.1.2002 (No 7-F3). Environmental standards related to one's own special field must be found out through the regional administration's environment and natural resources committee and with the help of the locality's environmental inspector. The environmental protection norms are not a significant security factor for small companies, but familiarity with environmental laws is important for units that are

establishing production plants. The use of construction materials and chemicals is supervised.

Business operation is regulated by various environmental norms that depend on the field of production. Emissions have upper limits, location of waste is regulated and cleanness and hygiene are monitored especially carefully in the food products industry, among others.

Photo: Vesa Koivumaa



Russia has environmental certification procedures, of which some comply with international practices and some have Russian quality monitoring. The most important environmental standards directed towards production are norms that deal with emission formation, emission quantities and emission limits. A company's environmental safety zones belong in its standardised documents. The company's environmental safety plan also includes transports and the ecological impact of fuel and other storage.

Russia has the following quality standards for environmental safety:

- GOST R ISO 14001-98 and ISO 14001-96 (environmental management)
- GOST R 12.0.006-2002 (occupational safety)
- OHSAS 18000 series (occupational safety and health)

Tourism business is directly linked to environmental values. Sustainable use of the environment is a prerequisite for utilising a tourism product. A company that practices tourism activity is obligated to acquire permits from the authorities, e.g. for shooting rapids. Tourism may not damage plants and trees. Waste may not be left on shores and campfires may not be built anywhere else than in specified places. Travel in national parks without permission from the park management is forbidden. Russia's everyman's rights resemble Finland's practices. In Russia everyone can travel freely in nature (except in the above-mentioned permit-based areas and other places where travel is forbidden) and gather wild berries and fruits. Fire safety rules and precautions must be observed. Open campfires are forbidden in forests and natural surrounding during forest fire danger and dry seasons. Campfires are only allowed in specified places (Oikarinen 2005, 19).

16 BUSINESS CULTURE

16.1 Familiarity with Russian culture as the key to co-operation

Writing about culture, and particularly culture differences, is a challenging task. In doing so it is possible to become labelled as some sort of chauvinist or discriminator. Culture is difficult to measure, but cultural differences are clearly visible. One should never attempt to compare the superiority of cultures or customs with respect to each other. However, differences should be identified. Culture, also business culture, grows and gets its strength from history. Business culture cannot be changed all of a sudden, probably not even over a period of decades.

Familiarity with the business culture of the locality, region and country are the key to an organisation's success. Familiarity with the culture is becoming a critical factor if one intends to practice long-term operation in a foreign environment. In examining difficulties that Finnish companies have come across in Russia, for example understanding business culture and ethics, local employees' lack of work experience in a Western company, and the employees' lack of professional qualification, teamwork skills and initiative are significant factors. It is interesting that also the Russians are clearly interested in Western and Finnish business culture. Russian entrepreneurs interested in the Western markets who have been interviewed during the Doing Business Safely in Russia project increasingly bring up the subject of business culture instead of talking about corporate legislation or information security, for example.

What comes to Russian workplace culture, one can definitely say in general that the Russian worker is not accustomed to voluntarily assuming responsibility. Authority granted to him/her does not always correspond to obligations. The middle management of a unit again is in a difficult position in terms of obligations. This may partly be so because, in Russia, an organisation must have a clear director who specifies what is to be done and who is to do it. Modern business education strives to present different leadership models, but education in Russia does not always correspond to rapidly changing market conditions. Thus, hierarchy is visible more clearly and steeply than it is in Finland. Power also means distance from the performing level. The attributes of power and wealth, like luxury cars, security men and motorcades are displayed with pleasure. Unofficial networks of social contacts, even in the formal office environment, are a clear contrast to this cult of a distant director. Compared with a Finn, a Russian needs a much smaller social space. Thus, the distance to another person is closer, and personal contact, handshaking and kisses on the cheek are natural behaviour in Russian culture. Also, a work collective's habit of shooting for the same target creates a bal-

ance to the strong hierarchy and unconditional leadership in the Russian work culture.

The office and bureaucracy culture is easily brought to business operation, which is apparent in the formalities of agreement negotiations, ceremonious signing of communiqués and letters of intent, and perhaps the heavy administrative culture with its stamps and decision-making levels. According to the office culture style, minutes of negotiations must always be drawn up. An unsigned document is not trusted. A person-oriented approach should be taken in addition to a item-centred approach in negotiations. Finns are nearly completely item-oriented and they consider it odd to emphasise or even mention the pivotal position, weight of opinions and excellent views of the person responsible for decision-making in a negotiation. One should not go to extremes in praising the other party's decision-maker. Someone present may feel it expresses a lack of confidence in the others. Small talk also belongs. Russians are known for being family-centred. Finns more rarely discuss or ask about the family or the health of the spouse and children. Unofficial discussion may take place in an unofficial place (restaurant, vehicle), but it does not lead to an agreement. Official matters are always finalised and agreed at the office.

On the other hand there may also be uncertainty about who directs. Is it the owners' council, administrative council, owner bank or an outside unclear quarter? The management of a company (state organisation) expects a foreign visitor to acknowledge the hierarchy and directorship. A Russian expects matters to be agreed on with the highest director. Hierarchy also includes the principle of parity. Directors negotiate with directors and assistants with assistants. Hierarchy and unclearness in the overall directorship system have also caused problems. Uncertainty about the organisation's future and the employee's personal income bring additional pressure to the work atmosphere and the development of work productivity. Development plans are not necessarily implemented or supervision of their implementation is incomplete. Understanding culture must be taken seriously. There are big differences in the mind-sets of Finns and Russians as parts of the organisation.

16.2 Features of Russian culture

Russian business culture is an integral part of Russian customs. The Finland-Russia Society published a condensed general presentation of this topic in 2003. Sociability, sentimentality, generosity, hospitality and love of home/family are cultural features associated with Russians. Russians are interested in the person, not so much the organisation that the person represents. A network of unofficial contacts ensures that matters are taken care of smoothly instead of the formal relationships of a rigid, bureaucratic power apparatus. Time is a relative concept for a Russian. A Russian as a private person or even as the director of a company does not make a fuss about the promptness of a meeting. A Russian does expect a guest to arrive on time, so

it is worth adhering to what has been agreed. On the other hand, negotiations may last longer than was scheduled in advance (Finland-Russia Society 2003, 20). Before travelling to a negotiation with a potential partner, the agenda should be sent to the partner to allow him/her to prepare for the correct issues. In this conjunction it is good to remember that faxes and e-mail are the best modes of contact, because the mail is often unreliable.

One visible thing is Russians' discriminative attitude towards us and them, meaning foreigners. This was apparent in the past, for example in higher hotel prices for foreigners. The community mind-set (us, *nashi*) still has a strong position in Russian culture in both private and working life. The director is responsible for the company's matters, takes care of relations with the outside world and protects his/her own people. The director is the director, and his/her assistants may sit quietly to the end of a meeting. The company again is more widely responsible for societal obligations than in Finland. Russians are used to the fact that industrial combines maintain schools and day care centres and sponsor the militia's operation, for example. Employees' commitment to one employer is loose, and workplaces are changed quite easily in Russia. It is also common to work for two different employers. This places demands on the level of a company's information security in the form of confidentiality requirements. Business culture in Russia is changing along with the rest of society. The rate of change varies by region and changes happen unevenly. Sometimes also unexpectedly. Changes in laws reflect well the rate of change in society. At any rate predictability is not a good term for explaining the present situation. True, predictability has improved since the turbulence of the 1990s.

Embracement of international operating culture is in full swing in Russia. The share of English vocabulary in the Russian language is probably the greatest in exactly the business and IT sectors. This indicates the newness of international economic life and signals that there are still not many international experts. Even those with experience in international operation are relatively young. Still, the rate of change is many times that of Finland.

One cannot necessarily get along in Russia with only Finnish or Western business experience. Initially it is necessary to rely on local know-how. On the other hand, one should not blindly trust local knowledge of society. Russians themselves are not always versed in their own area's legislation, the twists of officials' operations, staff changes or the crime situation. Small companies' knowledge about agreements often needs improvement and often it may be difficult to observe agreements. However, in business operation one must respect local regional and overall Russian culture. Existing economic circumstances should be respected and specialists' expertise should be utilised when agreements are made. Economic circumstances include relatively undeveloped bank operation and valuation of cash. In Russia it is not enough to sign an agreement. The agreement is not valid until it has been

verified with the company's round stamp. Indeed it does not have any juristic significance. The stamp symbolises Russian business and agreement culture. To increase its credibility in the eyes of authorities and Russian entrepreneurs, a Finnish company should have a round stamp made.

Daily customs include many things that are foreign to Finns. For example, at the end of a (group) trip programme in Russia it is customary to give the guide and the driver a tip that is 10 % of the fee. Also in restaurants a tip indicates that the customer was satisfied with the service. A gift is always followed by a reciprocal gift. A Russian finds him/herself in a sticky situation if he/she does not have a reciprocal gift at the moment (which in itself is rare, since a Russian will even give the tiepin from his own shirt as a reciprocal gift). There are certain customs associated with giving and receiving a gift, which should be learned before travelling to Russia. A business gift typically contains the company's logo. Business culture definitely includes a business card. The business card should contain the information in both English and Russian. Conservative dress (dark suit) rather than free dress is recommended for official and semi-official negotiations. At least in official situations, one should not rely on jeans and a sweater, which again in Sweden are acceptable basic dress. Women have their own dress etiquette.

Photo: Vesa Koivumaa



There are also rules on where and what kinds of jokes can be told (Russians have a sense of humour) and in what situations one may talk about politics. Presentations should be clear and quite straightforward. Russians themselves speak carefully and they have a habit of handling issues through metaphors. Sometimes they are very symbolic and conceptual, but at other times they are concrete and direct, if necessary. Body language and facial expressions form

a large part of Russians' manner of expressing themselves. Finns are quite monotonous in their non-verbal communication.

The cryptic term *dusha*, soul, soulfulness, which is claimed to steer Russians' behaviour, is often linked to Russianness and Russians. This behaviour is rambling and sometimes prone to extremes. Sensitivity extends to superstition. Russians are said to be at least a little superstitious. If you leave something behind, it means you will return. An even number of flowers means bad luck. A living person is given only an uneven number of flowers. A mutual emotional experience and feeling of sameness create a positive atmosphere in forming business relationships.

Finnish history is surprisingly well known, at least in the circles where Finnish officials and entrepreneurs spend time. Literature, films and the changes in Russian society are good topics for conversation. Russians are willing to participate in discussions where differences and similarities between the countries are compared. Russians read a lot and are familiar with both classic and historic literature and modern documentary publications. Here seems to be a clear cultural difference (or different use of time) compared with Americans, for example. As a whole Russians are interested in history and are well versed in the last century's conflicts between Finland and Russia. Although in the Soviet era Finns were warned against dwelling on history, today it appears these are good conversation topics in free-form situations. Many Russians have acknowledged Mannerheim as nearly their own national hero. Well, as long as it does not end up as drunken harping.

Good information is available on business customs, so this booklet will not go into the topic any further. May it be said in this conjunction that the Russian trade representative in Finland (www.rusfintrade.ru) is a good first source for a Russian who wishes to become familiar with Finnish business culture and customs. Finns should also be aware of what the Russians write (or what they write to the Russians) about Finnish trade customs and cultural circles and how these features are compared with each other.

17 WORKING WITH THE AUTHORITIES

Centuries' practices since the times of the czars to the Soviet era have become stratified in Russian official culture. It may justifiably seem to Finns that handling a matter does not begin until the papers have yellowed on an official's table. Hierarchy and a lack of haste are characteristic features that form a stark contrast to someone accustomed to the Scandinavian low organisational structure. This slowness is partly a myth, as various laws mention maximum times for handling matters. For example, handling times for licence applications were mentioned earlier in this booklet. Of course, one should remember that the Finnish administrative culture is a mixture of Swedish and Russian traditions. Today the Finnish public sector operates exceptionally efficiently compared with most countries in the world. That's why our expectations and demands on public administration are always hard, regardless of where we are in the world.

Societal relationships and especially relations with the authorities are a part of the everyday business environment in Russia. Russian public administration and social life are penetrated by official involvement. Public discourse on streamlining administration and cutting the amount of people working in administration is non-existent in Russia. Nevertheless, the technification of society and administration is inevitably bringing development in the direction of a more compact administrative structure. Many matters can be advanced by fostering relations, not necessarily with offices, but the people working in them. Russia has a saying: "law enforcement officials work against us with our money". As Finns we should not take this altogether literally, however. Much depends on one's own obedience to the law and openness. Finns have this ability and this feature of the Finns is also known in Russia. The tax authority and the militia belong to the core group with which one should have open, good relations. Openness does not necessarily guarantee anything. One needs to be prepared for inspections.

Although Finns trust in Finnish authorities, Finns must understand that the Russians themselves have a mistrustful, stiff attitude towards the militia and perhaps also other authorities. Trust in the militia's operation has remained at a low level for years, while the situation in Finland is the opposite in terms of the attitude towards the police. Mistrust is partly upheld by law enforcement officials' powerlessness before large webs of fraud, terrorism and street crime. For example, Russians are warned of the acclimatisation difficulties of militia groups returning from war fields like Chechnya, which have appeared in conjunction with normal maintenance of order.

In past years the tax police carried out efficient audits in companies. The tax police no longer exist, but tax inspection units still monitor companies. When

discussing with a representative of an authority one must always be aware of the possibility that matters connected to company secrets may leak onward. Sometimes powerful competitors and crime organisations use corrupt officials as a front through which they can gain possession of valuable information. The state's pronounced role in business operation, its regulation and operation as an entrepreneur raise the risk of corruption and may endanger the economic security of business operation. Mere information is not always enough; the goal may be to topple a competing company by means of official actions. An official may expect to receive a bribe that would bring a favourable result to an audit. Bribes should not be given. In such a case the security service FSB is the right address to report actual or attempted malpractice by an official. If the event is not reported, it is probable that similar pressured audits will continue in the future. According to a decree passed on 6.3.2007, information about a company's rights in case of a tax audit can be obtained from Russia's tax inspection office (and the office's web pages) (FNS 2007).

Various provocations, like auditors having drugs brought into the office, are tested methods for getting the management into trouble if all else fails. Stolen goods may be "found" in the storeroom, etc. The procurator's office again is the highest supervisor of official operations, which also gladly receives information about officials' arbitrariness. On the other hand, in Russia loud objection to officials' arbitrariness may lead to termination of business operation. A middle road can be found for this problem, also. Recording video equipment in the company and the office are good defensive tools in case officials attempt to employ dishonest methods.

Most audits by the militia and tax authorities concern accounting. They are looking for possible offences related to use of funds and accounting. If offences are found, the company is liable for administrative offences, rarely criminal offences. The accountant is also in the line of fire. In doing business with the authorities it may become apparent that the rate of change in legislation is so fast that even the authorities have a hard time keeping in pace. Information about the latest laws is not necessarily available, much less about its application. A law is effective only after it has been publicised. In the Murmansk region, for example, the Murmanskii Vestnik newspaper published legislation passed by the regional Duma and the regional government.

The probability of ending up in the above-mentioned type of trouble with the authorities is smaller than that of normal business operation continuing. They were brought up here only to indicate what all one needs to be mentally prepared for. The authorities may also be indispensable as advisors and as defenders of business operation. Contacts with the militia, fire and rescue authorities and the tax authority also show the region's and locality's other entrepreneurs that relations are good and the company has a strong position among law enforcers. Nearly without exception the upper management of the organisations in question act according to good service principles and respect for the law. Nearly all who are guilty of malpractice are lower-level officials.

The management and officials of regional administration and cities/districts should be included in the list of important co-operating parties. The region's and locality's political influence and the permits for business operation, environmental issues and land rent, for example, are in their hands. Contacts should be made on the personal level. Regularly sending the company's annual reports to the appropriate authorities, for example, keeps relations warm.

18. SUMMARY

The purpose of this guide has been to open new types of, even international, viewpoints in the discussion on Finnish business security. In many places Finnish (Western) business security tenets can be applied in the Russian business environment. For example, information security, crime safety, fire safety, staff safety and office security are solved using similar methods regardless of the location of a company. In Russian business security, ensuring the economic security of a company is emphasised, which includes prevention of corporate espionage and takeovers and competitive intelligence. Background checks of both companies and individuals before entering co-operative relationships are natural and necessary aspects of risk management together with a command of the agreement culture. Business culture and customs bring their own traits to business security; how work is done and how long-term, confidential relationships are formed.

State regulation, societal security objectives and authorities' operations in Russia's circumstances bring dimensions to business security that must be taken into consideration when planning a long-lasting presence in the Russian market or operation with a Russian business partner.

One of the main offerings of this booklet is the observation that abundant open and public information about business security issues is available in Russia. For example, this booklet lists many public sources that can be utilised to get ahead in checking backgrounds, for example. Careful background work in Finland, familiarity with the region's and locality's network of authorities, and linking companies and authorities working in the security sector with development of business security create strong prerequisites for safe, successful business operation in Russia. There is abundant information about business security, but it is scattered and strongly commercialised. Finnbar-ents' Doing Business Safely in Russia pages at (<http://www.finnbarents.fi/safelyinrussia2>) provide both wide-ranging and detailed security information for those interested in Russian business operation and security questions.

REFERENCES

- Aromaa, Kauko – Lehti, Martti 2001.** Pietari suomalaisyritysten turvallisuusympäristönä 1994—1999. Oikeuspoliittinen tutkimuslaitos. Helsinki 2001.
- Biznes Tezaurus 2001.** Анализ состояния внешней среды малого предпринимательства в России (на примере шести пилотных регионов). Venäjän pienyritystoiminnan ulkoisen ympäristön analyysi kuudella pilottialueella. Osoitteessa http://www.rcsme.ru/libArt.asp?id=3614&r_id=134&l_id=1. Moskva 2001. 22.2.2007.
- Butjaikin, Sergei 2007.** За 2 месяца в Мурманской области выявлено 380 экономических преступлений. Kahden kuukauden aikana Murmanskin alueella paljastettu 380 talousrikosta. Osoitteessa <http://www.regnum.ru/news/799354.html>. 20.3.2007.
- Emercom 2007.** Palovaaralliset asuin kohteet Venäjällä. Luettelo Emercomin nettisivuilla. Osoitteessa <http://www.mchs.gov.ru/article.html?id=14191>. 6.4.2007.
- Europol 2005.** EU Organised Crime Report. Brussels 17 Nov. 2005.
- Fleishman, Semen 2006.** Sovershenno Sekretno. Artikkel i lehdessä Biznes zhurnal online. Osoitteessa http://www.business-magazine.ru/mech_new/staff/pub273660. 26.4.2007.
- FNS 2007.** Venäjän veropalvelun käsky: ”Об утверждении форм документов, которые должны использовать налоговые органы при проведении налоговых проверок”. Käsky (prokaz) koskee asiakirjoja joita tulee käyttää verotarkastuksen yhteydessä. Osoitteessa http://www.nalog.ru/document.php?id=25253&topic=ind_pr. 6.3.2007.
- Harju, Simo - Söder, Jouko 2007.** Terveystenhoidon varautumisoikeudet.. Teoksessa Suuronnettomuusopas (toim. Maaret Castrén, Simo Ekman, Matti Martikainen, Timo Sahi ja Jouko Söder). Duo-decim. Gummerus Kirjapaino Oy Jyväskylä: 413 – 420.

- Internet University 2007.** Osnovy informatsionnoi bezopasnosti. Informaatioturvallisuuden perusteet. Osoitteessa <http://www.intuit.ru/department/security/secbasics/3/>. 7.5.2007.
- Jushtshuk, Jevgeni 2006.** Konkurentnaja razvedka. Marketing riskov i vozmozhnostei. Kilpailijan tiedustelu. Markkinariskit ja mahdollisuudet. Vershina, Moskova 2006. 238 s.
- Kaakkois-Suomen TE –Keskus 2005.** Liiketoiminnan harjoittaminen ja yrityksen rekisteröinti Suomessa. Kaakkois-Suomen työvoima- ja elinkeinokeskuksen julkaisuja. Kesäkuu 2005.
- Kauppapolitiikka 8.1.2004.** Venäjän talouskatsaus – kasvua ilman uudistuksia. Ulkoministeriön kauppapoliittinen julkaisu, raportit.
- Kelo, Jarmo – Ahola, Katja – Leino, Ilpo 2007.** Yritykset viranomaisyhteistyössä ja varautumisessa suuronnettomuuksiin. Teoksessa Suuronnettomuusopas (toim. Maaret Castrén, Simo Ekman, Matti Martikainen, Timo Sahi ja Jouko Söder). Duodecim. Gummerus Kirjapaino Oy, Jyväskylä 2007, 200-206.
- National Bureau of Investigation (Keskusrikospoliisi) 2005.** Keskusrikospoliisin vuosikertomus 2005.
- Koistinen, Jarmo 2006.** Rikos Venäjällä. Oikeusvertaileva tutkimus Suomen ja Venäjän rikosvastuuperiaatteiden eroista. Joensuun yliopiston oikeustieteellisiä julkaisuja 17. Joensuun yliopisto. 147 p.
- Koivumaa, Jari – Koivumaa, Vesa 2004.** Turvallisesti Venäjälle. Selvitys lappilaisten yritysten turvallisuusongelmista ja niiden hallinnasta Barentsin alueella. Rovaniemen ammattikorkeakoulun julkaisusarja C 4. 100 s.
- KZOT RF: КЗоТ Российской Федерации.** Venäjän Federaation työkoodeksi. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. N 197-ФЗ. Принят Государственной Думой 21 декабря 2001 года. Одобрен Советом Федерации 26 декабря 2001 года.
- Kerkko, Pertti 2001.** Turvallisuusjohtaminen. PS-kustannus, Porvoo. 368 s.
- Kosonen, Riitta 2007.** Luoteis-Venäjän haasteet ja mahdollisuudet. Tieto&trendit –lehti 12/2007. Tilastokeskus.
- KTM 2007.** PK-yritysten tietoturvakysely 2006. Yhteen veto 8.2.2007. Kauppa- ja teollisuusministeriön julkaisut.

- Kuznetsov, Igor 2007.** Biznes – bezopasnost. Bisnes ja turvallisuus. Dashkov i K, Moskova 2007. 413 s.
- Lapland provincial government (Lapin lääninhallitus) 2005.** Matkailijan taskuopas. Lapin lääninhallitus & Murmanskin aluehallinto, Urheilu- ja matkailukomitea.
- Ljannoi, Gennadi 2006.** Ekonomicheskaya bezopasnost predpriyatiya. Yrityksen taloudellinen turvallisuus. Journal Best of Security, No 7, Heinäkuu 2006. Osoitteessa http://www.bos.dn.ua/view_article.php?id_article=27.
- Loginov, O. I. 2006.** Безопасность вашего бизнеса. Liiketoimintanne turvallisuus. NT Press, Moskova 2006. 206 s.
- Melton, Keith H. - Piligian Craig 2005.** The Spy's Guide: Office Espionage. Feniks, Rostov-na-donu. 181 s.
- Miettinen, Juha E. 1999.** Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Kauppakaari Oyj. Gummerus Kirjapaino Oy, Jyväskylä 1999.
- Miettinen, Juha E. 2002.** Yritysturvallisuuden käsikirja. Käytännön tietoa yrityksille. Kauppakaari, Helsinki 2002.
- Ministry of Internal Affairs 2006:** Elinkeinoelämän ja viranomaisten yhteinen strategia yrityksiin kohdistuvien rikosten ja väärinkäytösten torjumiseksi. Suomen turvallisuus. Sisäasiainministeriön julkaisuja 15/2006.
- Leonov, Ilja 2007:** Ubiitsa pogib ot zatotshki. Murmanskii Vestnik, no 11 (3904) 20.1.2007.
- Myllyniemi, Pekka 2000.** ONNETTOMUUSRISKIT HALLINTAAN – Loppuraportti. Sisäasiainministeriö, 29.2.2000.
- Möttönen, Tuomas 2004.** Turvallisuus ja kilpailukyky. Kansainvälinen kilpailukyky mittareiden valossa. Etla keskusteluaiheita. ETLA No 952.
- Nurgalijev, Rashid 2007.** Ushtsherb ot ekonomitsheskih prestuplenii v 2006 godu prevysil 100 mlrd. rub. Talousrikollisuuden aiheuttamat menetykset vuonna 2006 nousivat 100 miljardiin ruplaan. Osoitteessa <http://www.burocrats.ru/invest/070316172618.html>. 16.3.2007.

- Rumjantseva, Irina 2007.** Tshestnye posadili tshestnogo? Murmanskii Vesnik 11.5.2007, no 85, 86 (3978, 3979).
- Security guide (Turvallisuusopas) 2005.** Turvallisesti Venäjälle. Turvallisesti Venäjälle –hanke. Toukokuu 2005.
- Spiridovitsh, Seija 2007.** Suomen tärkeimmät kauppakumppanit vuonna 2006. Osoitteessa www.finpro.fi. 2.3.2007.
- Oikarinen, Rita 2005.** Venäjän matkailun lainsäädäntöä ja käytäntöjä Murmanskin alueella. Rovaniemen ammattikorkeakoulun julkaisusarja C 7.
- Ollus, Simon-Erik 2006.** Jälleenvienti kasvattaa Suomen Venäjän - kauppaa. Tieto & trendit –lehti. Tilastokeskus 2.2.2006. Osoitteessa http://www.stat.fi/tup/tietotrendit/tt_03_06_venajakauppa.html. 2.5.2007.
- Omsk State University.** Sähköinen oppikirja varjotaloudesta ja talousrikollisuudesta. Osoitteessa <http://newasp.omskreg.ru/bekryash/>. 4.5.2007.
- Petrov, Sergei 2007.** Obespetsheniye bezopasnosti organizatsii i proizvodstvennyh objektov. Praktitsheskiye posobiya dlya rukovoditelei i rabotnikov predpriyatiy i organizatsii. Organisaatioiden ja tuotannollisten kohteiden turvallisuuden varmistaminen. Käytännön ohjeita yritysten ja organisaatioiden johtajille ja työntekijöille. Moskova, NTs Enas. 219 s.
- Pricewaterhousecoopers 2005.** Obzor ekonomicheskikh prestuplenii 2005. Talousrikoskatsaus 2005. Osoitteessa http://www.pwc.com/gx/eng/cfr/gecs/PwC_GECS05_Russia-rus.pdf. 26.4.2007.
- Roper, Carl A – Grau, Joseph A. – Fischer, Lynn F. 2006.** Security Education, Awareness and Training. From Theory to Practice. Elsevier Butterworth-Heinemann, US.
- Russian Central Chamber of Commerce 2006.** Yritysturvallisuustoimintasuunnitelma vuodelle 2007. Osoitteessa <http://tpprf.rbc.ru/img/uploaded/2007032210210285.doc>. 2.3.2007.
- Russian Federation law 25.7.2002.** No. 115-FZ Ulkomaalaisen asemasta Venäjän Federaatiossa. Viimeisimmät täydennykset voimaan 15.1.2007.

Russia's small enterprise fund 2007. Bezopasnost biznesa dlya subjektov malogo predprinimatelstva. Pienyritysrahaston liiketoiminnan turvallisuussivusto. Osoitteessa http://www.nanocorp.info/protection/safety_business/. 13.3.2007.

Samociuk, Martin, - Iyer Nigel – Lehtosuo, Kimmo 2004. Väärinkäytösten torjunta. Käytännön opas. Yrityskirjat. Gummerus Kirjapaino Oy, Jyväskylä. 143 s.

Sassali, Hanne 2007. Suomen ja Venäjän tietoturvalainsäädäntöä. Opinnäytetyö Rovaniemen ammattikorkeakoulu. 60 s.

Siikaluoma, Pasi – Metso, Jari 2001. Suomalaisen rakennusyrityksen etabloituminen Venäjälle. Opinnäytetyö Rovaniemen ammattikorkeakoulun rakennustekniikan koulutusohjelma. 67 s.

SVKK ry. 2005. Suomalaisen yritysten toimintamuodot Venäjällä. Käytännön toimintatapoja ja kokemuksia. Suomen Kauppa- ja teollisuusministeriö. Toteuttaja: Suomalais-Venäläinen kauppamariyhdistys – SVKK ry. Helmikuu 2005.




The Finland-Russia Society (Suomi-Venäjä-Seura) 2003. Venäläinen tapakulttuuri. Perinteitä ja nykypäivää. Suomi-Venäjä-Seura, Venäjä-info, Helsinki 2003.

Tunik, Igor – Poljakov, Vadim 2007. Antireider. Posobiye po protivodeistviyu korporativnym zahvatam. Antiraiders. Yritysvaarojen ehkäisemisen keinoja. Piter. 205 s.

University of Joensuu 2005. Alihankintaopas. Spatia, Maaliskuu 2005.


Verhelä, Pauli 1997. Matkailun ohjelmapalveluiden turvallisuus. Edita Prima Oy, Helsinki.

VISTA Foreign Business Support. Osoitteessa www.vfbs.ru. 20.4.2007.

Safely in Russia II

Emergency Card



Foreign Embassies in St Petersburg:

AUSTRIA: +7 (812) 275-6022
 BELARUS: +7 (812) 273-0078
 BELGIUM: +7 (812) 277-2342
 BULGARY: +7 (812) 273-7347
 CZECH REPUBLIC: +7 (812) 271-4612
 CROATIA: +7 (812) 325-8448
 CANADA: +7 (812) 312-4612
 CHINA: +7 (812) 314-6230
 DENMARK: +7 (812) 324-3755
 ESTONIA: +7 (812) 328-1404
 FINLAND: +7 (812) 312-4612
 FRANCE: +7 (812) 314-1433
 GERMANY: +7 (812) 320-2400
 HUNGARY: +7 (812) 326-6407
 ICELAND: +7 (812) 312-4612
 ITALY: +7 (812) 312-4612
 JAPAN: +7 (812) 312-4612
 LATVIA: +7 (812) 312-4612
 LITHUANIA: +7 (812) 312-4612
 NETHERLANDS: +7 (812) 312-4612
 NORWAY: +7 (812) 326-2400
 POLAND: +7 (812) 274-4701
 SLOVAKIA: +7 (812) 273-3241
 SWEDEN: +7 (812) 326-1433
 SWITZERLAND: +7 (812) 312-4612
 UNITED KINGDOM: +7 (812) 320-2400
 UKRAINE: +7 (812) 312-1048

Date of Birth

Telephone

Address

Citizenship

First names

Family Name

Workaddress in Finland

Workaddress in Russia

In Russia

Insurance company / membership number

Bloodgroup and bloodtype

Vaccinations

Allergies

Working substances in medication

Current medications

Medical conditions

DO

- Always carry your passport, visa and immigration card with you. Police have a right to check the identity of any person and if there is no ID, they have a right to take person to the police office.
- Have your address clearly written on a piece of paper both in English and Russian.
- Ask the taxi price before you take a trip, as there are no meters. Check in advance what is the average price for the taxi in that particular city.
- Exchange currency to roubles in any nearest bank. Passport is needed if you are exchanging money in the bank.
- VISA, MasterCard and American Express cards are usually accepted. But take cash with you as small shops will only accept local currency.
- Have with you a roll of toilet paper. There is a big chance there is no paper in bar and restaurant toilets.
- Bring frequently used medication.

DO NOT

- Get involved into any kind of gambling on the street. There is some con people playing trick games on the streets.
- Walk on your own at night, there are many people looking for easy money.
- Go alone to the bar or disco. If you went, try to avoid accepting drinks from strangers.
- Bring strangers to your room and watch your drinks if you do.
- Get to the taxi if there is someone else present besides the driver.
- Exchange currency on the street. More likely you will get Belarusian, Ukrainian or other "roubles" back.
- Buy alcohol in street side kiosks as beverages there often of poor quality.
- Carry money in a visible or obvious place. There are pickpockets in crowded places.
- Use valuables in crowded places, this includes mobile phones and cameras.

Take contact with your consulate in the following circumstances:

- Crime
- Accident
- Loss of documents
- A problem arises when being stopped by the police.

Take copies with you of the following documents:

- Passport
- Visa
- Migration card
- Hotel registration card

Important phonenumber for emergencies:

- Ambulance: 01
- Police: 02
- Firedepartment: 03

Model

GUARDING AGREEMENT

Agreement on sites to be guarded, which are the responsibility of guard units under the internal affairs authority

— city “ — ” 200 — .

_____ guard company
(department, unit)
_____ in context, hereinafter “Guard
company”, represented by
(internal affairs official)

_____, acting

(name and office)
(company regulations, rules)

based on and _____, hereinafter “Cli-
ent”, represented by
(company name)

_____, acting

(name and office)
(company regulations, rules)

based on, have entered the following agreement:

I. General terms

1. The client relinquishes and the Guard company assumes responsibility for the sites named in the list of guarded sites and plan (diagram) appended to this agreement.

The parties agree on the method of guarding, based on reliability and economy.

Supervision and guarding of the sites in the guarded area shall be arranged according to the following terms and methods:

_____.
_____.

2. The sites relinquished for supervision by the guard company must meet the following requirements:

a) the area’s production buildings, storage rooms, construction sites and access roads as well as the display windows of stores and businesses must be illuminated when darkness arrives _____

_____, to enable guards to supervise them.
(type of lighting)

lighting of the guarded area shall not be arranged in _____ cases.

Storage of materials and goods is allowed in the guarded area at least _____ metres from the fence.

b) the wall and roof structures, attic windows and openings and doors of the storage place for goods and other movable property must be in condition. Metal grates or lockable window shutters must be installed in the following downstairs windows (except for display windows of stores and restaurants):

_____ The client shall agree with the local fire inspection authority on the type of grate.

c) the sites must be equipped with the following technical security devices:

_____ (contact and alarm devices, fire alarms, lighting, fences, locks, turnstiles, automatic gates, guard towers, staff inspection and personal belongings storage space).

At the guard sites the guard must have free access to fire alarms and fire extinguishing equipment.

The technical condition of the supervised sites and their security and fire extinguishing equipment and date when they were taken into use shall be recorded in mutual records compiled in conjunction with the signing of the guarding agreement and they shall be an integral part of said agreement.

3. The Guard company together with the Client and the local fire inspection authority shall inspect the technical condition of the sites, security equipment, among others the fire alarms mentioned in section 2, at least twice a year, and a report shall be compiled and signed by the Guard company, the Client and the fire inspection authority's representative. The record shall mention the date by which any detected faults must be repaired and reported to the Guard company and fire inspection authority.

4. Guarding of the sites shall be arranged on the days and the hours of the day specified in the appended list of sites.

The guard company shall compile a plan for guarding the sites and the location of guarded points and shall present it to the Client.

If internal supervision points are arranged at the sites (rooms, access and check points and within the guarded area), their location and possible changes shall be agreed on with the Client.

The site's access control and disciplinary regulations shall be specified by the site's director, and implementation shall be done by the Guard company.

5. Daily reception of the sites, e.g. the central monitoring system, for supervision and relinquishment to the Client shall happen as follows

_____.

6. Security instructions and installation and user instructions of monitoring equipment supplied by the Guard company obligate the Client. Installation

and repair of the monitoring equipment is paid for by the Client, except when the need for repair is caused by the Guard company.

7. The price of the agreement is

Payment for the guard service shall be paid monthly with the Client's payment order, which shall be sent to the bank 15 days prior to the beginning of the next month.

If the Client does not pay on time, the Guard company shall present the bank a demand for payment by the 25th day of the ongoing month.

II. Guard company's obligations

8. The Guard company is obligated to:

- a) arrange and ensure guarding of the Client's goods and other movable property and monetary funds prevent outside persons from entering the sites;
- b) arrange access control at the sites and monitor transporting of goods in and out, which is based on transport permits. After working hours the Guard company is obligated to inform the Client whether all customers that entered through the gate with a single visit pass have exited from the area;
- c) together with the Client, take into use technical monitoring devices;
- d) service the monitoring equipment and repair defects upon notification by the Client.
Payment for maintenance service by separate agreement.
- e) ensure compliance with fire safety requirements at the monitored sites; in case of fire at the monitored site or if a fire alarm goes on due to a technical fault, the guards shall notify the fire department and begin to extinguish the fire or repair the fault;
- f) receive stamps and seals from the Client in the following cases:

III. Client's obligations

9. The Client is obligated to:

- a) equip the sites with technical monitoring equipment according to the agreement, ensure protection of goods and other movable property and improve supervision of the sites, access control and order at the sites;
- b) before relinquishing the sites to the Guard company, make sure no outside persons were left there and no electrical or gas equipment or other sources of fire were left on;
- c) lock and seal the outer doors of storage rooms, production departments, stores, kiosks and other rooms; also seal the inner doors of entryways; in addition to inside locks, lock emergency exit doors from the outside with padlocks;

close from the inside and seal display windows of stores and kiosks; displayed goods and other movable property in the windows and their serial numbers and prices shall be marked on a list signed by a responsible person and stamped by the Client. One copy shall be placed in the display window, one given to the Client's responsible person and a third to the Guard company.

Money, gem, gold, platinum and palladium jewellery, gold, platinum and silver watches shall be stored in stationary safes or vaults, and at the end of the sales day especially valuable objects shall be brought into a separate storage place, observing other security rules;

- d) install phones at monitored sites equipped with an inner phone network and an outside line for the guard after working hours; make sure the phone and electric line to which the alarm system is connected is in condition;
- e) arrange a separate phone line for connecting alarm system concentrators and protection levels to the monitoring centre;
- f) turn the alarm system on at the end of the working day at the sites and inform the Guard company without delay if they are faulty and remain on site until they are repaired or the Guard company assumes responsibility; 5 minutes after notifying the monitoring centre, make sure the monitoring equipment is on;
- g) inform the Guard company by _____ about basic repair or changes at the guarded site, changes in work schedules and operation, new secure storage places for valuable goods and other functions that may require changes in the guarding plan and guarded sites;
- h) improve and take care of the fire safety of the sites;
Note! If the agreement states that fire safety measures belong to the Guard company, the Client shall comply with its instructions for eliminating fire safety threats and deficiencies.
- i) familiarise the Guard company's staff with the guarded site's occupational safety requirements to the extent that they are connected to the guards' work and take care of the guards' occupational safety;
- j) provide the Guard company with free use of work and supplementary rooms, equipment, communication devices and water, electricity, heating, cleaning and repair services.
List of rooms, equipment and communication devices provided to the Guard company

_____.
- k) arrange weather shelter and places to warm up for the guards;

- l) arrange spaces for guard dogs and monitoring points where dogs are used in the following cases -

- m) inform the Guard company of all offences committed by the guards;
- n) offer housing to the staff doing actual guard work with the same condition offered to the staff of the guarded site. If the company has its own housing, the guards shall be given an apartment therein. The Guard company shall pay the Client for living expenses;
- o) arrange doctor, hospital, recreation and day care services for the guards with the same conditions as the company's own staff;
- p) arrange the same benefits for guards at sites that are hazardous to health as for own employees at the cost of the Guard company.

IV. Guard company's liability

10. The Guard company is liable for damage caused by:

- a) burglary at the guarded sites which were entered by breaking a lock, window, display window, fence or in another way due to insufficient guarding or neglect of goods transport regulations or robbery;
 - b) property damage (e.g. due to arson) by outside intruders due to insufficient guarding;
 - c) fire caused by guards;
- Burglary, robbery, property damage and arson shall be investigated by the authorities.

11. Guards shall report burglary or property damage at the guarded sites to the militia and the Client. The guard shall ensure the security of the site until the arrival of the militia and investigation authorities.

If the Client has made a crime report (written or by phone) of caused damage, the representatives of the Guard company shall participate in damage assessment.

Remaining goods and other movable property shall be assessed as soon as the authorities arrive at the site.

12. The Guard company shall compensate the Client for damage caused by the guards after the Client has presented a statement by the investigation authority or a decision by the court concerning the outside intruder's burglary, robbery, property damage or fire caused by a guard. The amount of compensation shall be verified with appropriate documents and a calculation of the value of the goods and property, checked on the basis of accounting data. Compensation for damage shall take into account the value of the stolen or damaged property, the value depreciation of the damaged property, the cost of repairing the damage and lost monetary funds.

13. If the guilty parties are found, the Guard company shall demand payment from them.

14. If stolen goods and property are returned to the Client, a representative of the Guard company shall be present.

The value of the returned property shall be subtracted from the requirement for compensation presented by the Client, and the paid amount shall be returned to the Guard company. If part of the returned property is damaged, a record shall be compiled in the presence of representatives of both parties and an assessment expert. In such a case the Guard company shall compensate the Client for loss in value.

15. The Guard company shall be freed of liability only in such a case where it can prove its innocence. The Guard company shall not be liable for:

- a) property damage caused by natural catastrophe;
 - b) theft or robbery of cash left in the guarded site if the Client has left more money than specified in the security regulations and if said money was not in a stationary safe or vault;
 - c) personal things left by the Client's employees;
 - d) damage caused by a criminal inside if he/she got in before the site was closed and exited before the guard period began;
 - e) goods stolen from display windows of stores or other businesses if there was no list of them in the window;
 - f) theft of gem, gold, platinum and palladium jewellery and gold, platinum and silver watches left outside of stationary safes and vaults;
 - g) theft and robbery of goods or other movable property if an investigation shows that the Client had not turned the burglar alarm on, had not relinquished the site to the Guard company and had not informed the Guard company of a faulty alarm system ;
 - h) theft of goods and other movable property if the Client has neglected development of technical protection according to the requirements of the mutual document and this has made the theft possible.
- The Guard company also is not liable for damage caused by loss of monetary funds and movable property caused by an outside intruder in cases specified by sections b), e), f), g), h).

16. The Client shall present a demand for compensation for damage, which the Guard company shall handle as agreed.

V. Additional terms

17. The Guard company is obligated to turn the alarm system on after working hours at the following sites

And should they be faulty, to report this to the Client in the following cases

18. The Guard company may assume responsibility for fire safety at the cost of the Client if the site does not have its own fire department.

The fire safety terms are as follows:

19. The Guard company shall handle guarding of special transports in the following cases: _____.

Compensation for taking care of these tasks and related Guard company's expenses shall be paid as follows:

20. In exceptional cases (work done by the Client, which compromise the integrity of fences and grates) the parties agree that the Guard company shall place supplementary monitoring points for a maximum of 10 days.

21.

(special terms and requirements that concern the guarded site's technical protection and sufficiency of alarm equipment at important sites and liability for neglecting to meet these requirements).

VI. Period of agreement

22. This agreement is made for the period _____ and it shall become effective beginning with the date of its signing.

If neither party requires cancellation of this agreement one month before its termination, it shall continue with the same terms and agreement period.

Notice may be served of termination of this guarding agreement before the end of the agreement period by agreement of both parties. If a party intends to refuse guarding of separate sites, said party shall inform the other party 15 days in advance.

23. All disputes regarding this agreement shall be solved using legal methods.

This agreement was compiled as two identical copies, one for the Guard company and one for the Client.

24. Parties' juristic addresses and bank data:

Guard company:

(company name, street address and post office)

Bank account no. _____ bank.

Client:

(company name, street address and post office)

Bank account no. _____
_____ bank.

Signatures:

In behalf of the Guard company:

In behalf of the Client:

Stamp

Stamp

This Business Security and Russia booklet provides an overall picture of the areas of security that need to be taken into consideration in business operation connected to Russia. This booklet, produced in the Doing Business Safely in Russia project, particularly emphasises the Russian aspects of business security. Background checks of potential business partners, working with security companies, familiarity with the operating culture of the authorities and ensuring economic security are prerequisites for sustainable business operation in Russia. This booklet also covers information security, the threat of serious crime, environmental safety, fire safety and rescue operation, travel safety and safe living in light of the challenges presented by the Russian operating environment. The author extensively analyses business security and offers practical guidelines for anticipating and managing security risks.

ISSN: 1239-7741

ISBN: 978-952-5153-67-5 (vol.)

ISBN: 978-952-5153-68-2 (pdf)

