Alexander Gudko
sibirov@ya.ru

Russia emerges into the shadows

Once a dark and closed securotocracy, Russia hopes to build a fleet, light, modern economy. Moscow-based Alexander Gudko surveys.

Russia's information security market is about 12 years old. It started in the early 1990s when information security experts employed by various government agencies began offering their services commercially. The initial market focused on anti-virus software, but emerging information security threats drove growth.

One of the first major systems to require a large-scale integrated approach to information security was the government's automated elections system. This was meant to automate the support processes to prepare and conduct nationwide elections and referendums.

Russia's information security market continues to grow. In 2005, it was estimated at $200-300 million. Until recently, many industry experts saw the domestic information security market as very fragmented. Scores of small companies address the infosecurity needs of small and medium business but have to share no more than 60% of the market value; a few dozen market players that focus exclusively on major corporate customers or government agencies hold the remaining 40-45%.

However, consolidation has already begun. In terms of product range and the availability of major international brands, the Russian market is hardly different from any other national market. Accordingly, any company setting up in Russia needs to compete either on price or innovation, and for the past five years, totally new solutions have been in short supply everywhere.

> "The outsourced infosecurity market has been growing faster than both the domestic IT market and most of the data security markets in the West"

Sales by domestic suppliers and integrators are tiny compared to the sales generated by major international players. However, the outsourced infosecurity market has been growing faster than both the domestic IT market and most of the national data security facilities markets in Western Europe and North America. The main customers are major corporations or nationwide financial institutions. These customers can afford the extra costs related to the systems' installation and staff training.

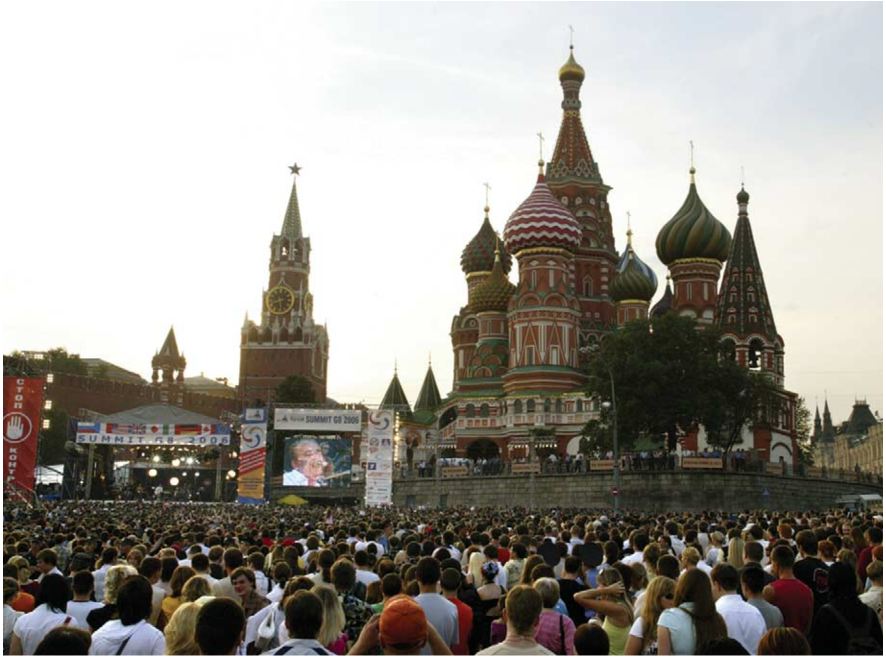
Big businesses now buy at least 60% of the infosecurity solutions in Russia. In fact, as a rule of thumb, the quality of its data security systems is directly proportional to the size of the organization. For example, the Revenue Service and the Bank of Russia have the best data security systems available. But until recently many other government organizations had no option but the cheapest basic solutions.

However, a series of events in 2005 changed the government's approach.

Save our bases!

In 2005, it seemed anybody willing to pay a modest fee to a street vendor could buy a CD containing confidential information relating to various aspects of Russian citizens' private life. In fact, in 2005 the number of leaks of vital confidential information from several government agencies doubled compared with 2004. Despite police efforts, the sources have never been identified.

The incidents were reported widely. The media believes that these databases were sold by agency insiders. The constant leaks have undermined the credibility of many ministries and agencies. Experts say



Concert held to support Russia's enforcement of intellectual property rights on the eve of G8 summit in St. Petersburg. (AP Photo/Mikhail Metzel).

some of the databases on sale contain hundreds of gigabytes of information. They are so big that for practical purposes they could not be sold via email or the internet, but had to be delivered to the buyers on portable hard drives. This suggests that the problem lies in a security triple whammy of poor pay, inadequate motivation schemes and inadequate infosecurity measures.

The scandal shifted public attention from hacker threats and virus hazards, which traditionally receive inflated coverage by the media, to insider leaks.

Mikhail Saveliev, a marketing expert at Informzaschita says: "Over the past year, market demand for protection from internal threats has grown significantly. (Up to then) the main trend was a growing demand for after sales services, auditing and consulting services. This probably stems from the fact the companies are paying more attention to the efficiency of data protection systems, maintaining their functionality at the highest level possible."

Government support analysts agree that the government has stepped up its support for the domestic IT sector. This support is partly explained by the increasing threat to national security. Year after year, the number of attacks that target both private and public sector information support systems has grown.

"The number of leaks of vital confidential information from several government agencies doubled"

Organizations are fighting back with more money and better administrative support. The government has set up a project to network computer incident response centers, the federal Electronic Russia programme, and the recently adopted Concept for the use of information technology by government organizations until 2010. All these state-funded projects are designed, among other things, to create the domestic information security industry.

What's spam?

In contrast to the US and Europe, spam has not yet become an issue in Russia. In Russia, there's no clear legal definition of spam or of direct marketing. This hampers legal action against spammers and makes it hard to recover the costs of processing unsolicited mail. "The lack of clear legal definitions facilitates unfair competition in general, while companies involved in spam filtering can be legally charged with 'intrusion on people's privacy'", says Kaspersky Lab's director of managed security services, Andrey Nikishin.

Despite this handicap ,the Special Technical Operations Bureau (STOB), a division of the Russian Ministry of the Interior plays a key role in fighting cybercrime. "STOB units, also called K units, are now stationed in each region of the Russian Federation and cooperate closely with each other," says STOB director Boris Miroshnikov. "As a result, to respond to a complaint filed with any regional K units, we can quickly deploy experts from any other K units in the country and, when necessary, the bureau's international connections. Apart from combating computer crime, K units help other departments in the Ministry of Interior to investigate crimes related in any way with information technology."

Legal framework

The legislative base that relates to information technology continues to improve. An article that deals with computer crime was added to the Russian Penal Code in 1997. While legislators then saw many threats only vaguely, they provided law enforcement officials with flexible tools to fight cybercrime.

STOB director Boris Miroshnikov

As the bureau gains experience, it recommends improvements to the legislative base and related bylaws, offers better enforcement practice, and a methodology of its own. It aims to develop a common conceptual structure with its partners, investigators, lawyers, judicial and prosecution bodies. More work to make the legal framework respond to current threats quickly will certainly help crime prevention.

Big networked businesses differ in their approach to infosecurity compared to smaller local businesses. The later normally finance their data security facilities in accordance with the so-called 'leftover principle'.

Carpet culture

One reason Russian companies are reluctant to install integrated information security systems stems from the prevailing culture. In developed countries, all serious incidents relating to information security and preservation of information resources have to be disclosed to the public; in Russia, problems are normally swept under the carpet. In addition, for many companies the cost of fixing the consequences of an information leak are much lower than the cost of a full-blown infosecurity installation.

Accordingly, following an incident, the affected companies install data security systems or simply do nothing; they comfort themselves with the idea that 'bombs dropped from an airplane never hit the same crater'.

And they shut up

"It's no use trying to scare consumers with abstract threats, the problem is ignored largely because of the Russian mentality, says Kaspersky Lab's Nikishin. "For example, in the West, life insurance is a normal thing, while in Russia the number of people who obtain a life insurance policy is negligible. People believe that premature death can never happen to them. This indestructible optimism is also very common among Russian businessmen."

Surveys indicate that almost half of all users decide to buy an anti-virus software only to clean their computer of the viruses already present, not to safeguard against them.

A typical question from a business owner to security system suppliers is "What financial benefit am I going to get from the data security systems you are offering?" Clearly it stems from the lack of understanding of the role of a security system.

To buttress arguments for installing a data security system in a financial institution, some suppliers now show the management a printout of credit card numbers or other important files that their specialists accessed after cracking the organization's computer system, often from a back-office computer.

> "This indestructible optimism is also very common among Russian businessmen"

"The suppliers have to overcome a specific mentality of managers in charge of corporate security, who are typically ex-cops or security service operatives," adds Mikhail Saveliev. "Traditionally they focus on incident investigation rather than on their prevention. Hence they may downplay requests to install surveillance equipment and monitoring software to control the company's applications and staff operations. Besides, the status quo policy enables security managers to present reports that reflect better on their performance."

Spell it out

While the concept of secure electronic document management is popular in Russia, customers' awareness is low. "When the customers come to suppliers, they have no idea what they really want us to do. We have to ask them if they want to protect the procedure itself or to set up interoperation regulations for company employees, or ensure the protection of documents during their sending or perhaps we should rather control the documents once they are received by the addressee," says Mikhail Saveliev.

"The customers tend to order integrated solutions piece by piece, as their understanding of the system's functionality grows. This raises the total cost of the system installation."

Security of funding remains an issue, especially when the client installs secure electronic document management systems in government agencies. System integrators need to ensure there will be enough money for a few years ahead. But this rigid budget scheme means it is harder to take advantage of new, better products and to upgrade quickly.

Pirates of the Crimea

"The main problem of the Russian information security market is typical for all the emerging markets, namely the high level of piracy," says Kaspersky Lab's Nikishin. "I'm sure that if the currently competing Russian anti-virus software companies consolidate their efforts against pirates, the level of piracy could drop by 10%. This would result in additional revenues for everyone that would significantly outweigh the benefits of any competitive strategies".

According to Kaspersky Lab, pirated software, including personal antivirus software, is about 90% of the installed base.

Andrey Nikishin, Kaspersky Lab

Red tape

Until recently, data security standards were based on the regulatory documents adopted in the 1980s. Today, the requirements by the Federal Technical and Exportation Control Service (formerly the State Technical Committee) include the domestic standard, GoST 15408-2002 (the so-called Common criteria). This standard is a Russian translation of ISO 15408.

In contrast with the older version, the new standard is adequate to address modern threat models. On the one hand, the market environment greatly benefited from the introduction of the Common criteria because every business can now build a security system of its own. On the other hand, this standard applies only to the protection of non-classified information. Until 2007, suppliers can choose for themselves which criteria (the new or the old ones) to use to certify their product.

> "The lack of clear legal definitions facilitates unfair competition, while spam filtering companies can be charged with invasion of privacy"

Furthermore, this creates the problem of deadlines. If the product doesn't require debugging, the old version of the regulatory documents requires it to be certified within three months. Certifying the same product under the Common criteria takes much longer.

Russia has yet to sign the agreement on mutual recognition of certification audits, but the market expects it to. It is too early to say that the new standard is well established in Russia, but product certification in accordance with this standard has already begun.

Speaking about the adoption of such international standards as the Sarbanes-Oxley Act or Basel II, their use in Russia is hampered by a low level of business organization in general. Work is underway to adopt ISO 17799, and certification to this standard will provide competitive advantages to both client companies and suppliers who now plan to enter foreign markets or establish ties with foreign partners.

Great Gate

Non-resident data security system suppliers who want to start up in Russia will have to abide by government algorithms and standards of cryptographic protection.

The Russian government has serious influence on the information security market. Regulatory bodies enforce meticulously the rule that all government bodies have to use only government-certified data security systems. Accordingly, in those consumer segments where the choice of data security systems requires state certification, the share of products from domestic suppliers is nearing 100%.

This doesn't mean that Western products cannot be successfully certified and licensed in Russia. To address this, foreign suppliers usually establish partnerships with Russian colleagues. An example of one such successful cooperation is a joint project between Cybertrust and Informzaschita to integrate Russian cryptographic algorithms into the UniCERT international system. This PKI solution was certified by the Federal Security Service at the end of 2004. After obtaining this crucial certification, the Russian Finance Ministry bought the system for use in Russia's largest public key system, which has one million certificates.

In another case, C-Terra CSP became the first Russian company to combine the Cisco VPN technology with CSP VPN Gate. Today, the gates realize the encryption-decryption algorithm specified by GoST. Elsewhere, the combined efforts of Microsoft and Russian company CryptoPro resulted in the certification of MS Windows XP in accordance with the Russian information security requirements. These are only a few examples that show that the combined efforts of professionals can overcome many obstacles on the way to ensuring information security.

Professional training

Today, infosecurity experts are in great demand. A number of military academies used to provide this kind of training. However, it was focused more on computers rather than on infosecurity as such.

"There's no established caste of Russian infosecurity professionals as yet," says Mikhail Saveliev. "Many military academies are trying to provide this kind of training but their disadvantage lies in the lack of really professional lecturers with extensive practical experience. Frequently, these guys are ex-federal security service and law enforcement officers."

> "Regulatory bodies enforce meticulously the rule that all government bodies have to use only government-certified data security systems"

Nikishin says, "When training information security experts, Russian universities are trying to cooperate with the leading Russian suppliers of information security systems to share their expertise. This plays an important role in the absence of experience engineers".

For example, Kaspersky Lab experts lecture in Moscow State University and other Russian universities, devise specialized training programmes and run job placement programmes in the lab. Government funding is also increasing. ●

About the author

Alexander Gudko is a business expert based in Moscow. Tel: +8 910 473 0113; email: sibirov@ya.ru; Website: www.marketlight.ru.