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.

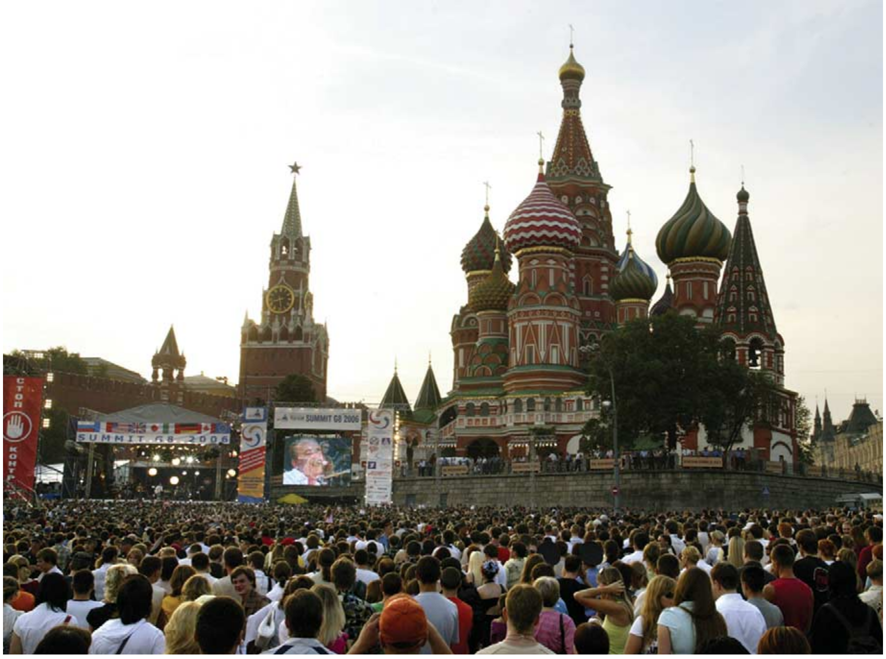
Big businesses now buy at least 60% of the infosecurity solutions in Russia. In fact, as a rule of thumb, the quality of its data security systems is directly proportional to the size of the organization. For example, the Revenue Service and the Bank of Russia have the best data security systems available. 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