Global IT Security Risks: 2012

Kaspersky Lab is a leading developer of secure content and threat management solutions and was recently named a ‘Leader’ in the Gartner Magic Quadrant for Endpoint Protection Platforms. In order to develop security solutions that most closely meet the needs of our customers, Kaspersky Lab conducts regular surveys focusing on the key IT security issues and cyber-threats.

In 2011 Kaspersky Lab, in partnership with B2B International, carried out a survey covering IT professionals working for large and medium-sized businesses. The aim of the survey was to find out what IT specialists thought of corporate security solutions, to ascertain their level of knowledge about current threats, the sort of problems they most often face, their ability to evaluate the risks associated with cyber-threats, etc.

A year later, the two companies conducted a similar survey expanding the geography and the number of respondents. This gave us the opportunity not only to assess the situation in the sphere of corporate security in 2012 but also to compare the results with those obtained the previous year and to note the main trends.

The main findings

According to half of those surveyed, cybercrime in its various forms is the second biggest threat to business. Despite the fact that this view has changed very little since last year, the measures being taken by IT specialists are woefully inadequate - only a little more than half of the respondents believe their company is really secure. The same applies to related areas such as intellectual property theft and industrial espionage.

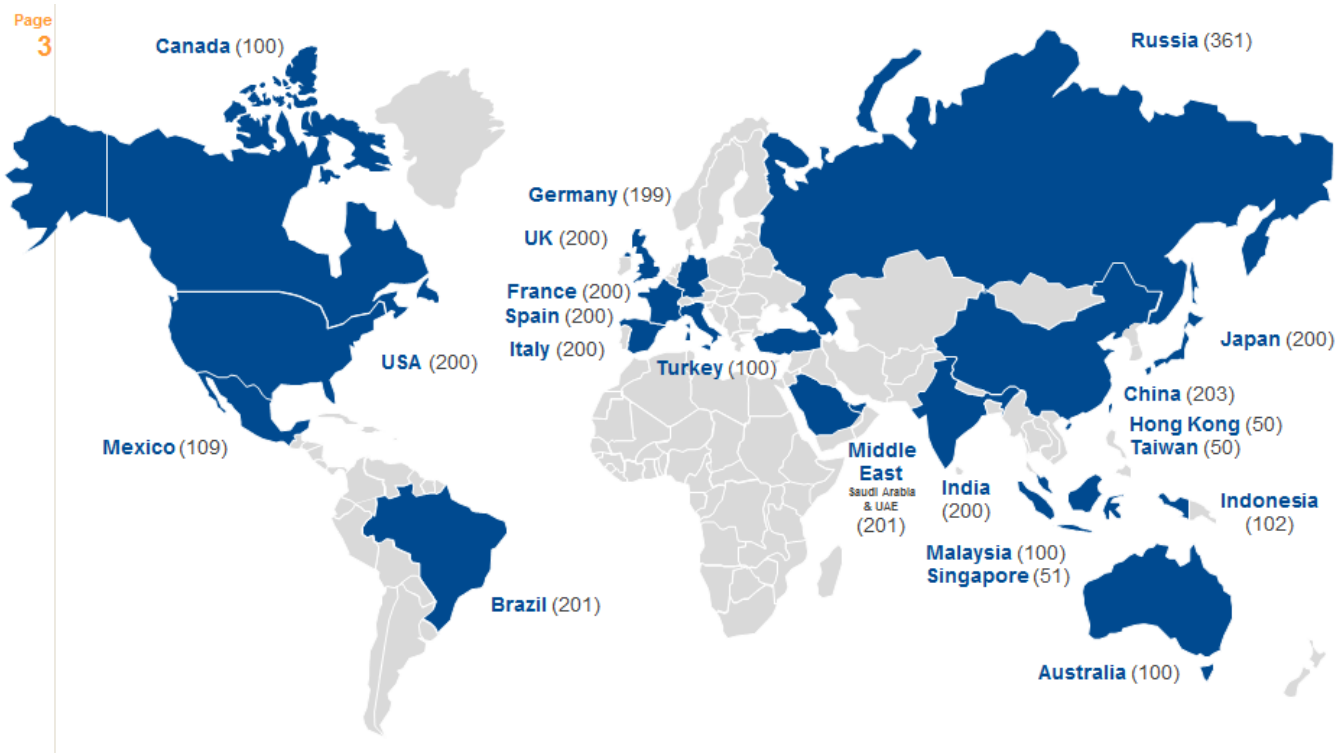
If we take a closer look at the emerging security issues, we see that IT professionals are most often faced with malware, spam and unauthorized attempts to penetrate the system. Internal threats also need to be singled out. The most serious problems in this area are caused by software vulnerabilities as well as problems linked to the use of mobile devices to access the corporate network. The seriousness of this latter issue has increased over the past year, with one-third of respondents describing the lack of control over mobile devices a serious problem. Meanwhile, more than half of those surveyed admitted they had begun to pay more attention to the issue. 10% of respondents said they had experienced critical information leaks due to the loss or theft of a mobile device.

The part of the survey that dealt with security policies for mobile devices showed that one third of companies allow their employees to use them with full access to the corporate network and its resources. By doing so, they are creating a gaping hole in their security. When it comes to corporate security policies for personal devices, the findings are not very encouraging either: only 9% plan to introduce tough restrictions. A significant proportion of the respondents (36%) stated that their companies would approve of using personal devices for work-related tasks.

Targeted attacks pose yet another major threat to company infrastructure. Over the past year several incidents have occurred that have made IT specialists start taking the issue seriously. In particular, 11% of respondents believe that this threat will be their main concern in the future and one third of specialists are sure their companies will be attacked sooner or later.

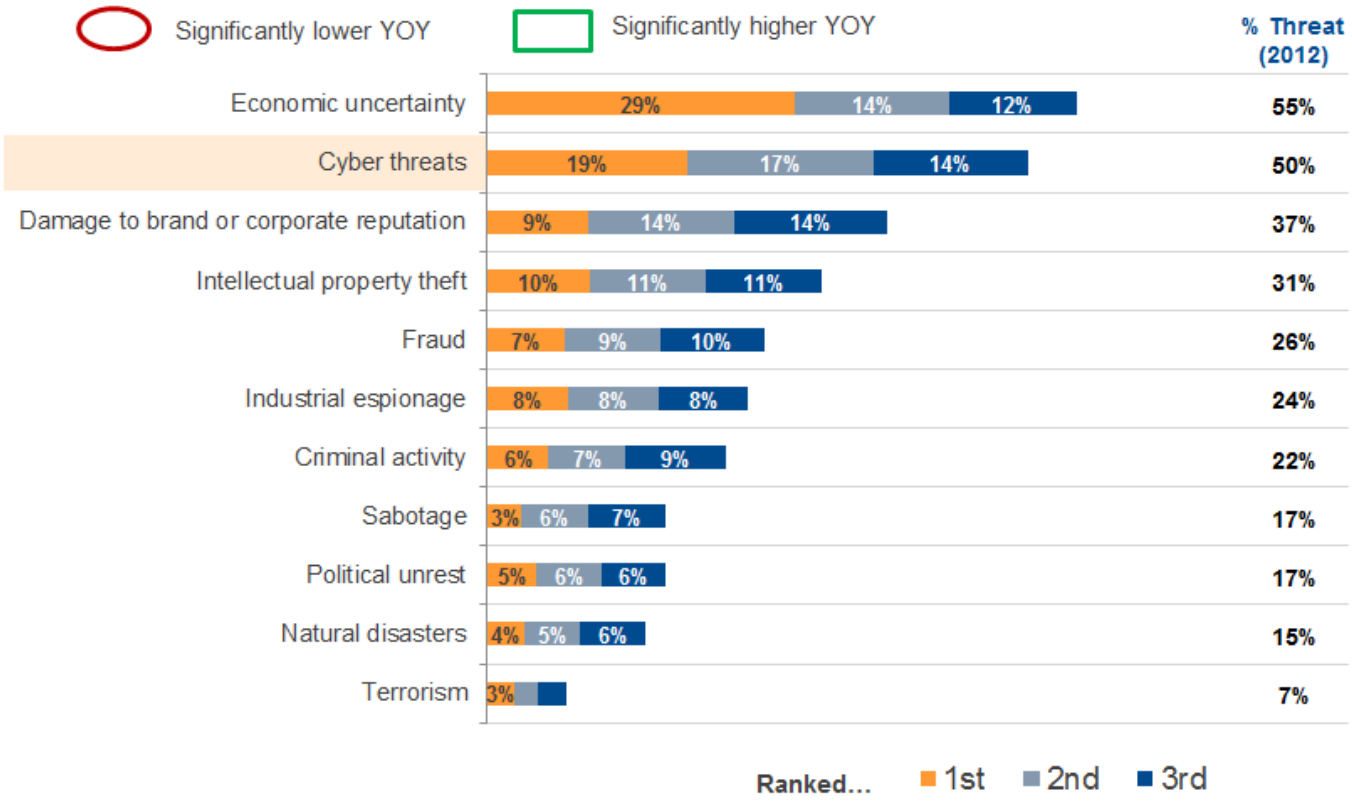
Many IT professionals cited budget constraints and the lack of a clear understanding among senior managers when it came to their department's objectives and goals, not to mention an insufficient number of trained personnel. At the same time 31% of those surveyed admitted that they had never heard about any of the most common cyber-threats, including direct threats to their companies. Thus, it is not just a matter of hiring new employees; existing staff also need to be educated.

Countries Covered



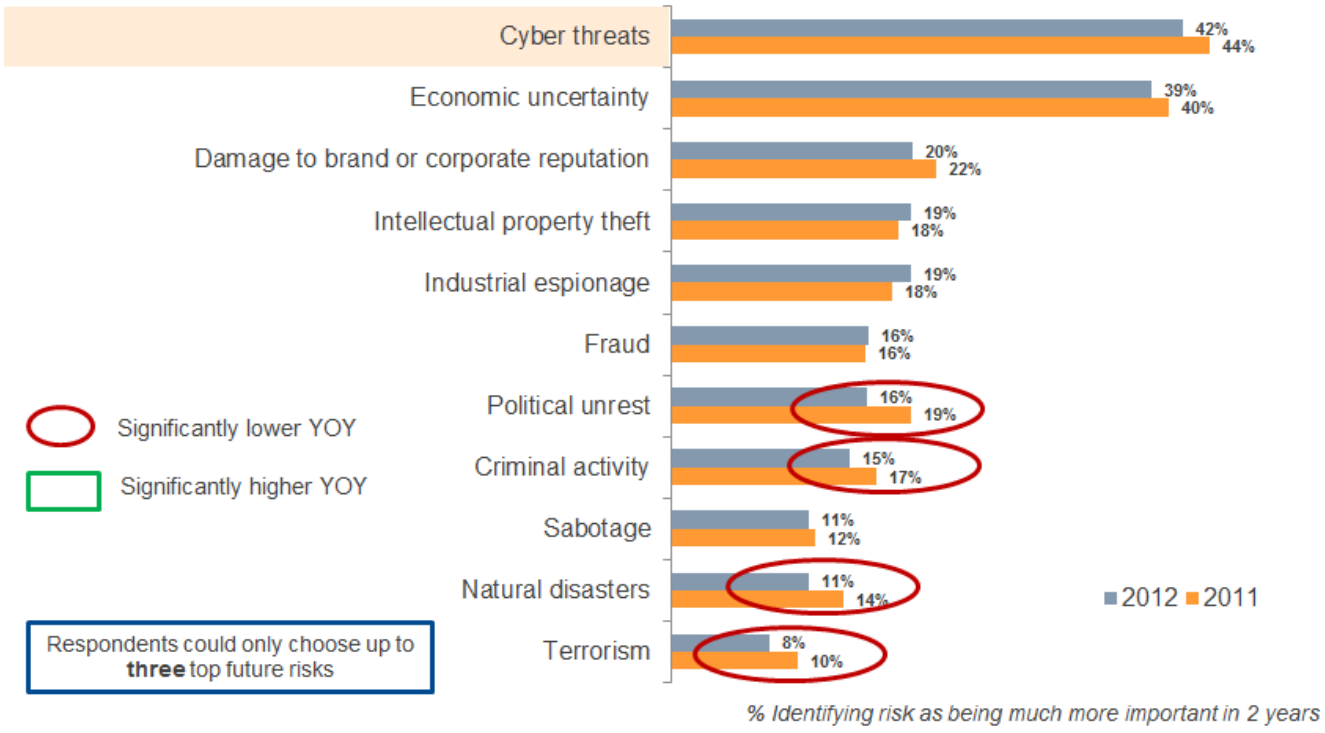
More than 3,300 senior IT professionals from 22 countries took part in the survey. All respondents had an influence on IT security policy, and a good knowledge of both IT security issues and general business matters (finance, HR, etc.). Globally, respondents were drawn from companies of three sizes: Small Business (SB, 10-99 computerized seats), Medium Business (MB, 100-999 seats) and Enterprise Organization (E, 1000+ seats).

Key business threats: cybercriminals, bad economics and damaged reputations



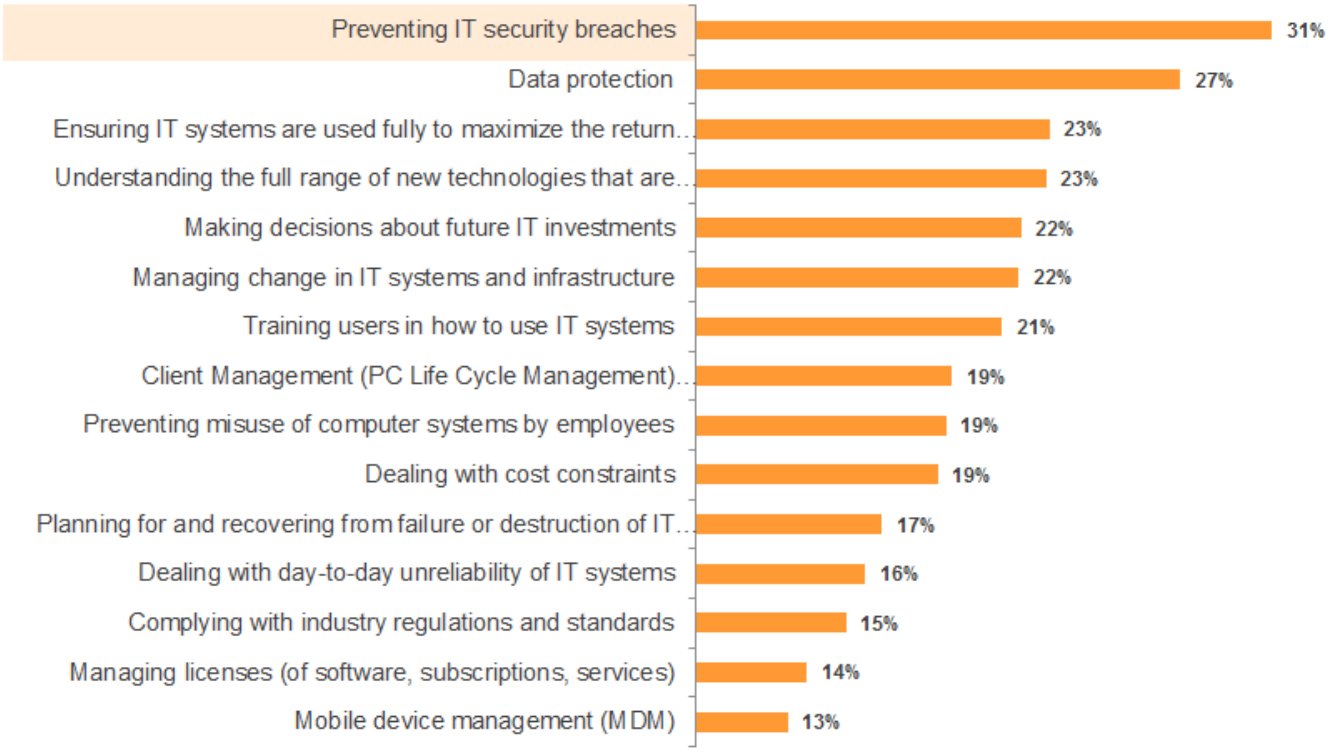
Half of the respondents (50%) ranked cyber-threats as being among the top three most pressing risks for business today and overall, they were seen as the second biggest danger to business. Among the other IT security risks cited were intellectual property theft (31%), computer fraud (26%) and industrial espionage (24%).

Cybercriminal activity seen as the most important future threat as well



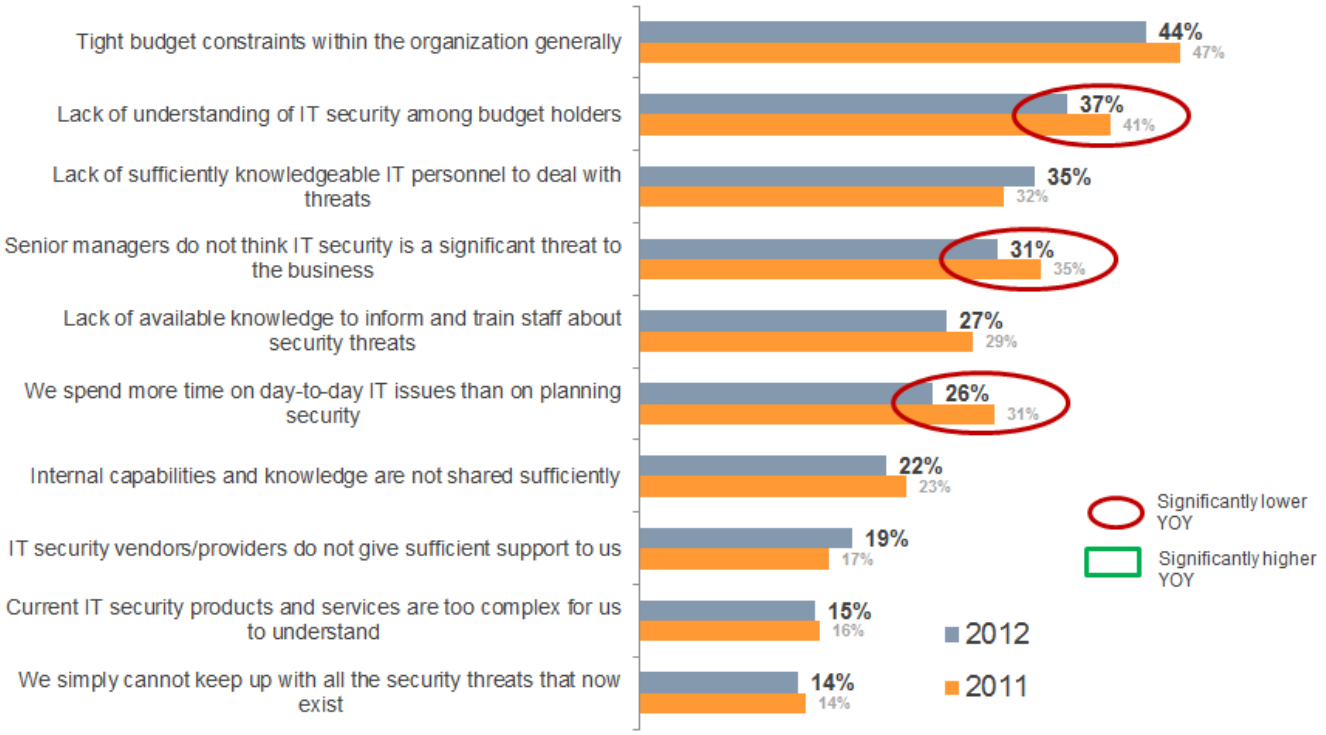
Currently cyber-threats are second in the list of most pressing problems: 42% of respondents believe that in the next two years they will become an even bigger issue. This is more than likely to happen considering the increasing number of malicious programs and the emergence of new types of attack. Half as many of the professionals surveyed believed there would be an increase in other IT risks: intellectual property theft and industrial espionage scored 19% each, while those foreseeing future risks coming from computer fraud amounted to 16% of the respondents.

IT security remains the #1 concern for IT professionals



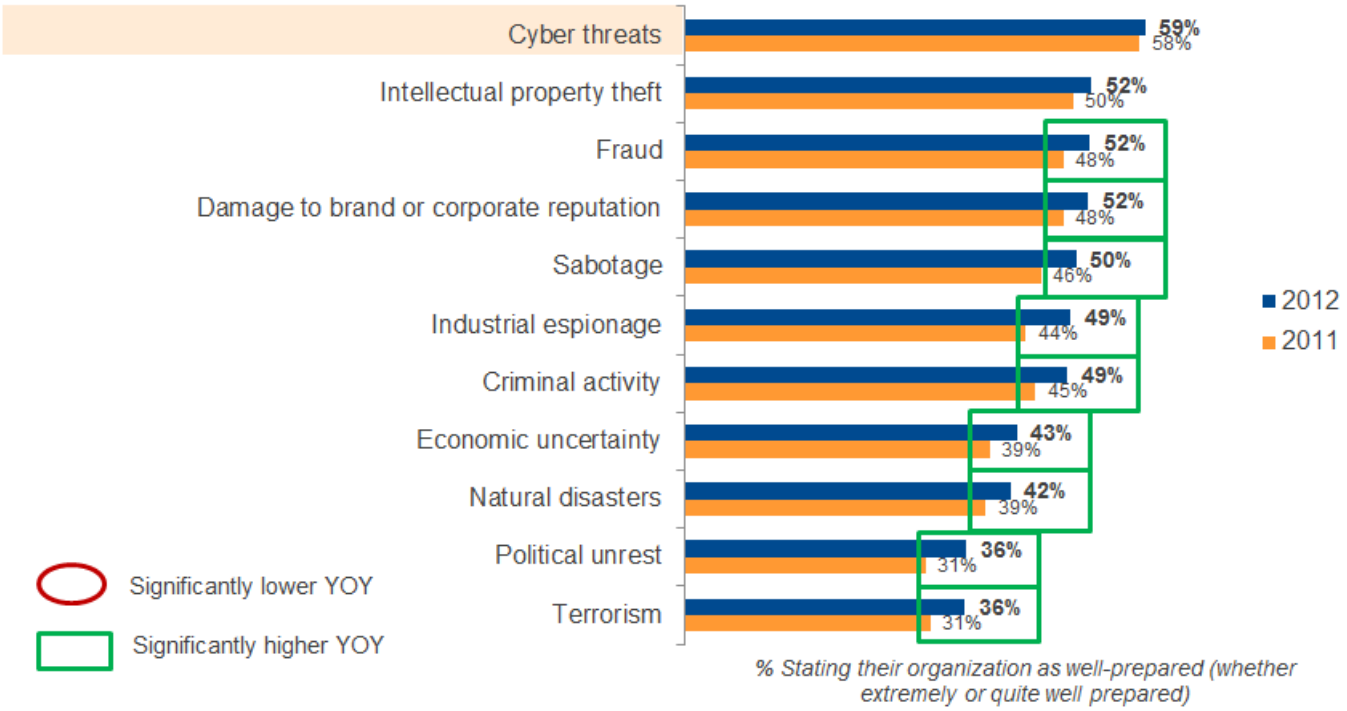
According to the research, preventing IT security breaches is the top concern for IT professionals (31% of respondents). This is followed by data protection (27%) and, oddly enough, ensuring IT systems are used fully to maximize IT infrastructure ROI (23%). Unfortunately, such an important task as control over mobile devices is in last place with 13%. If a company's security policies are not applied to mobile devices, both corporate and personal, it often leads to the loss of sensitive information which could end up in the wrong hands.

Obstacles to tighter security



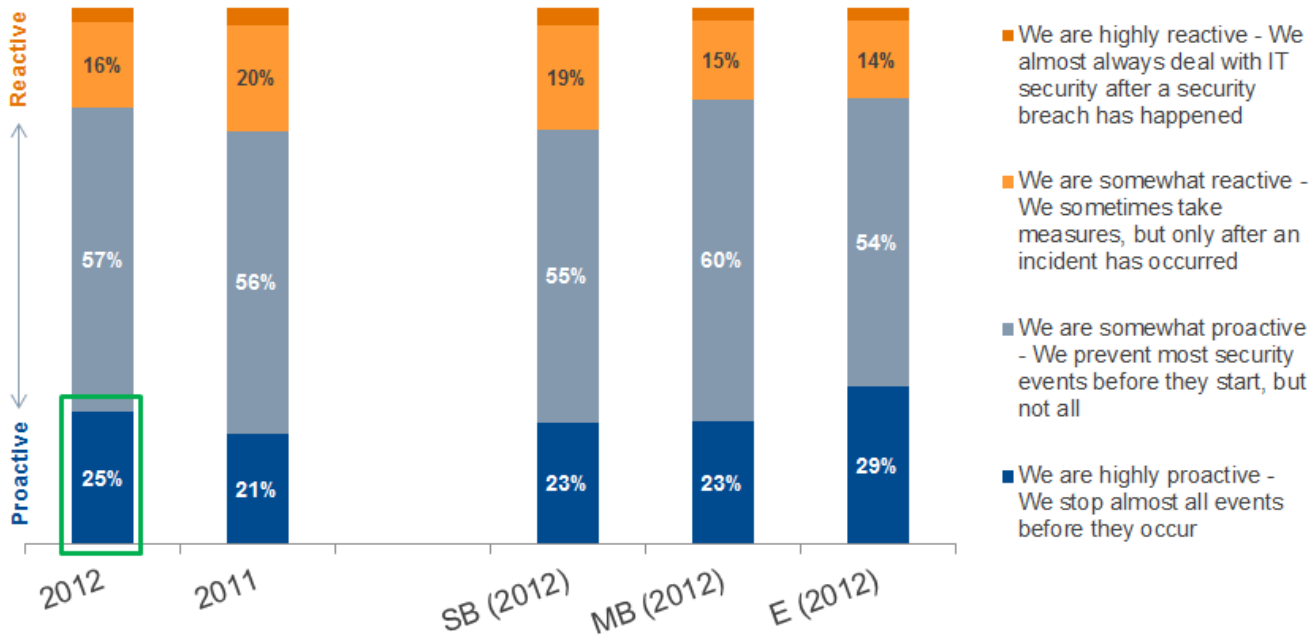
Sometimes IT security specialists face problems within their company or in a specific department that mean they can't perform their duties in full. According to the survey, the main problem is money-related: 44% of respondents indicated budget constraints and 37% cited a significant degree of misunderstanding of IT security issues among those in charge of the purse strings. Insufficient numbers of trained personnel to deal with IT threats is the third most cited problem, and one of the most important in our view. This issue was cited by 35% of those surveyed – an increase of 3% compared to last year's figure. Thus, it turns out that that the main problem for IT professionals is their inability to make their management understand just how important corporate protection against cyber-threats is.

Less than two-thirds of businesses consider themselves ready for cyber-threats



According to the survey results, IT professionals are well aware of the dangers of cybercrime. But are they ready to face them? Unfortunately only 59% of respondents feel that they are more or less prepared for them, which is just 1% more than last year. The situation is very similar with regards to other risks: though the level of preparedness is increasing, 48% are not sure they can combat intellectual property theft or fraud, while 51% believe they are incapable of protecting their company from industrial espionage.

General approach to IT security: more proactive response to emerging threats



The only reliable way to keep a business and its reputation safe is to take preventive measures against system infection or data leakage, i.e. to implement proactive protection. However, for various reasons, this is not always possible. According to the survey, 25% of IT professionals can combat almost all threats, but at the same time 16% prefer to solve problems after they occur. Last year's corresponding figures were 21% and 20% respectively, which allows us to conclude that companies are becoming more serious about the need for preventive measures.

Measures taken to avert security risks: the popularity of encryption

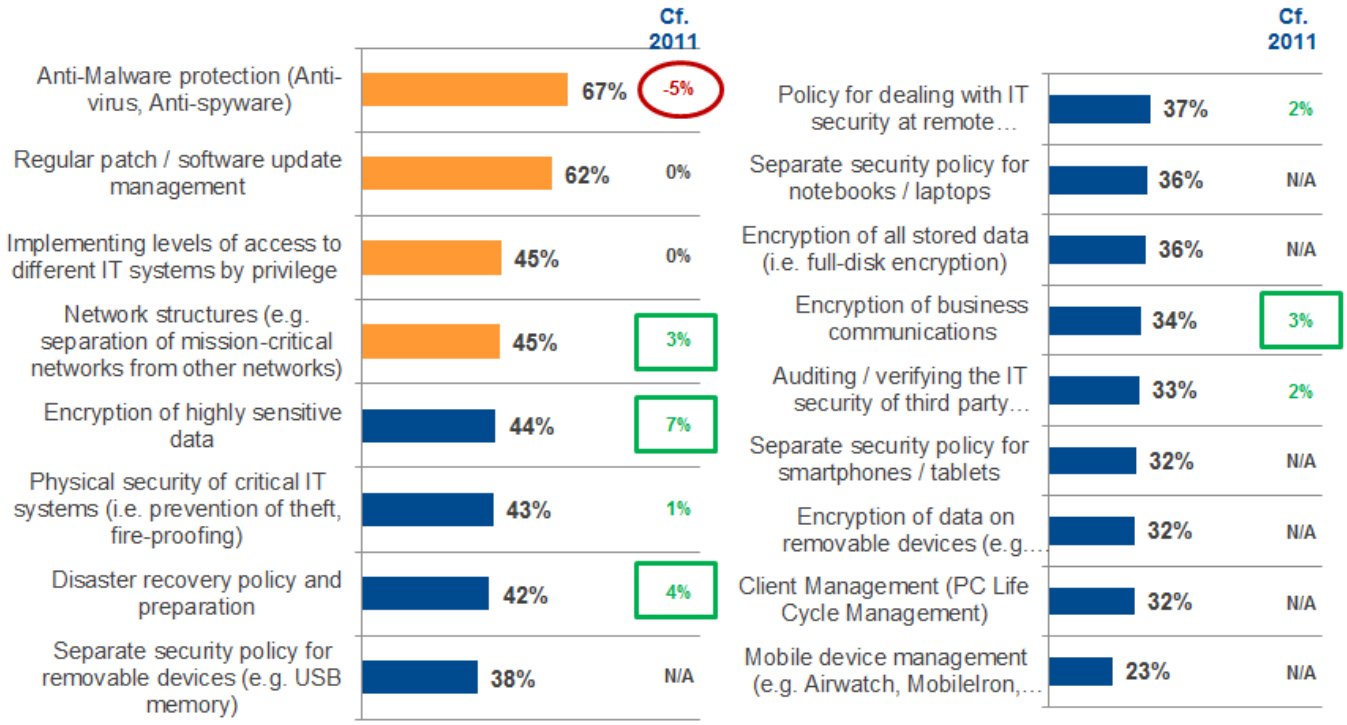
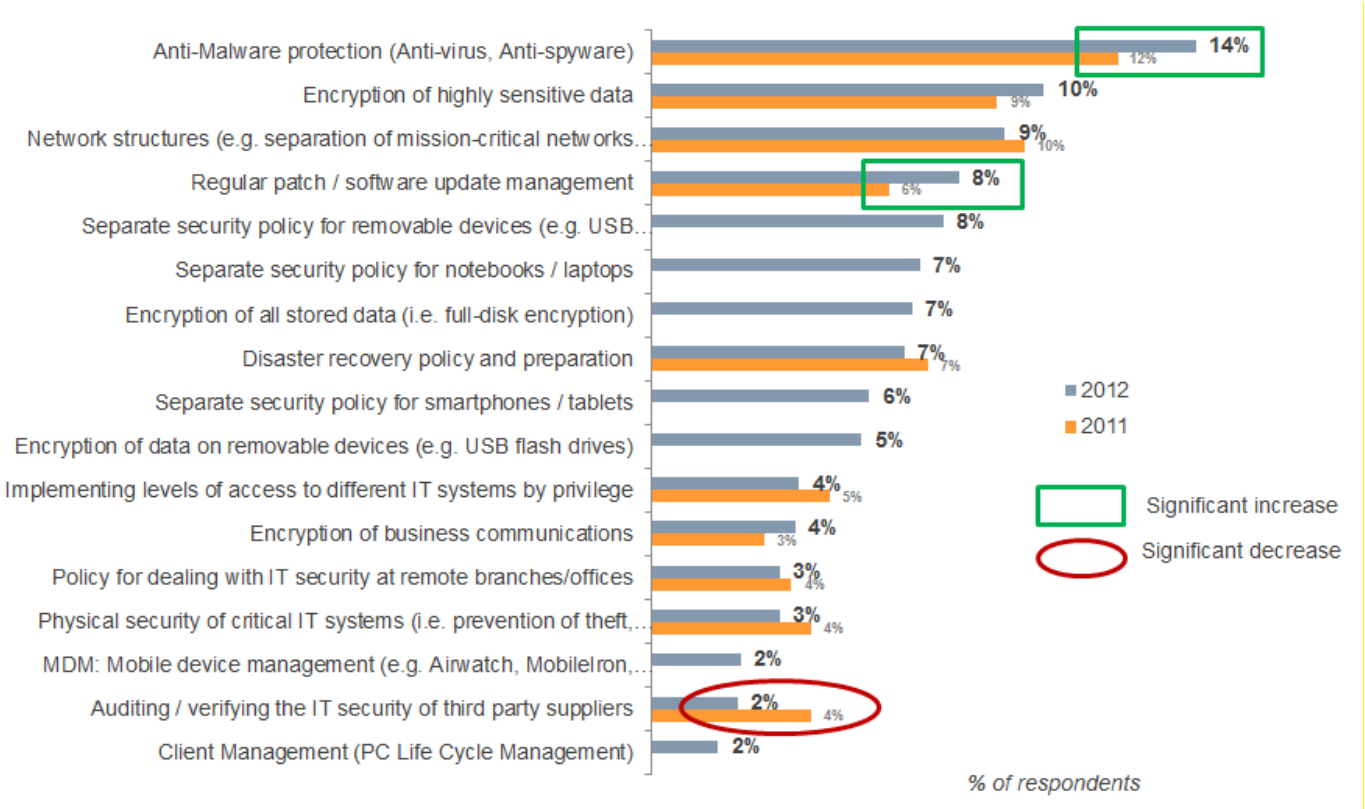


*Chart shows % of organizations that have **fully** implemented different security measures*

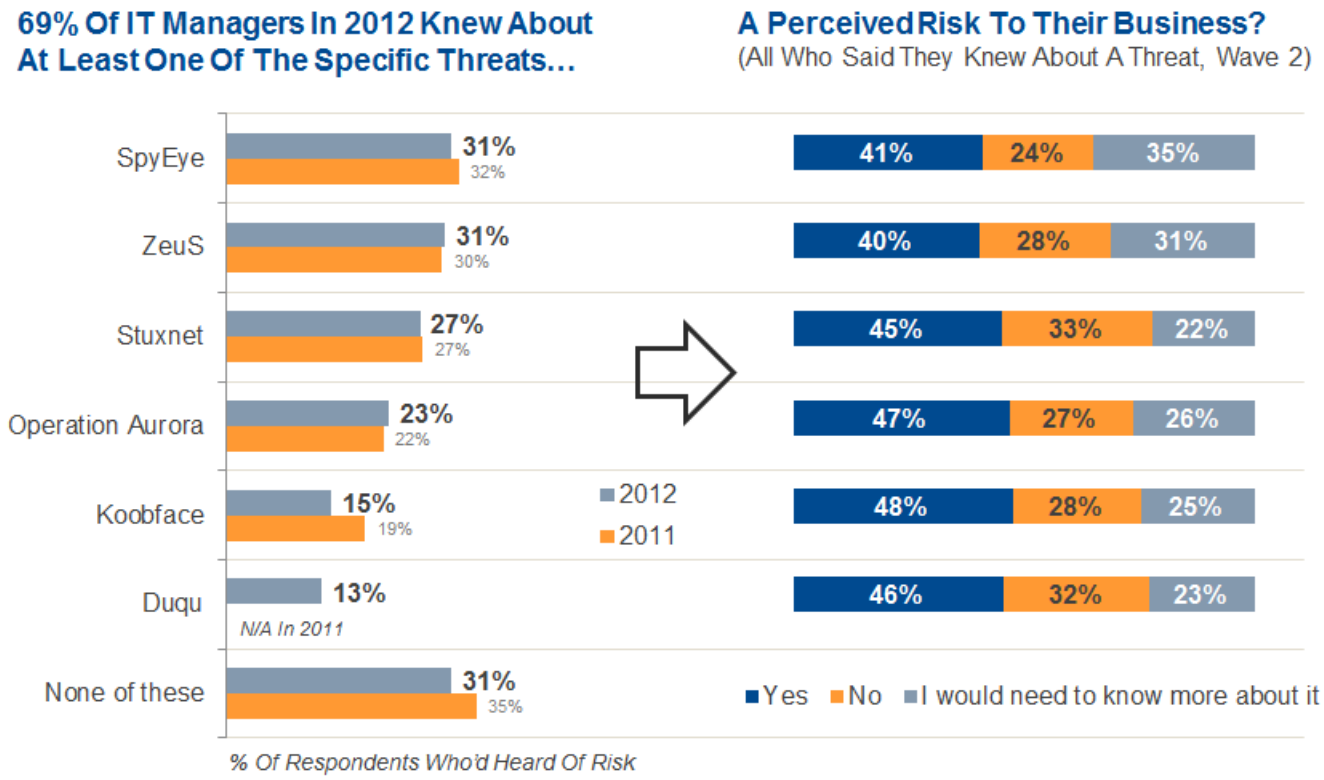
67% of respondents cited anti-malware protection as the main protection against cyber-threats. Regular software updates, i.e. patching vulnerabilities that can be used for infecting the system, is not far behind with 62%. The next most popular measure taken to avert security risks is the introduction of different levels of access rights to the various IT systems according to privilege. The popularity of encryption has grown considerably – 44% of companies have now implemented this technology.

Which one measure would they improve?



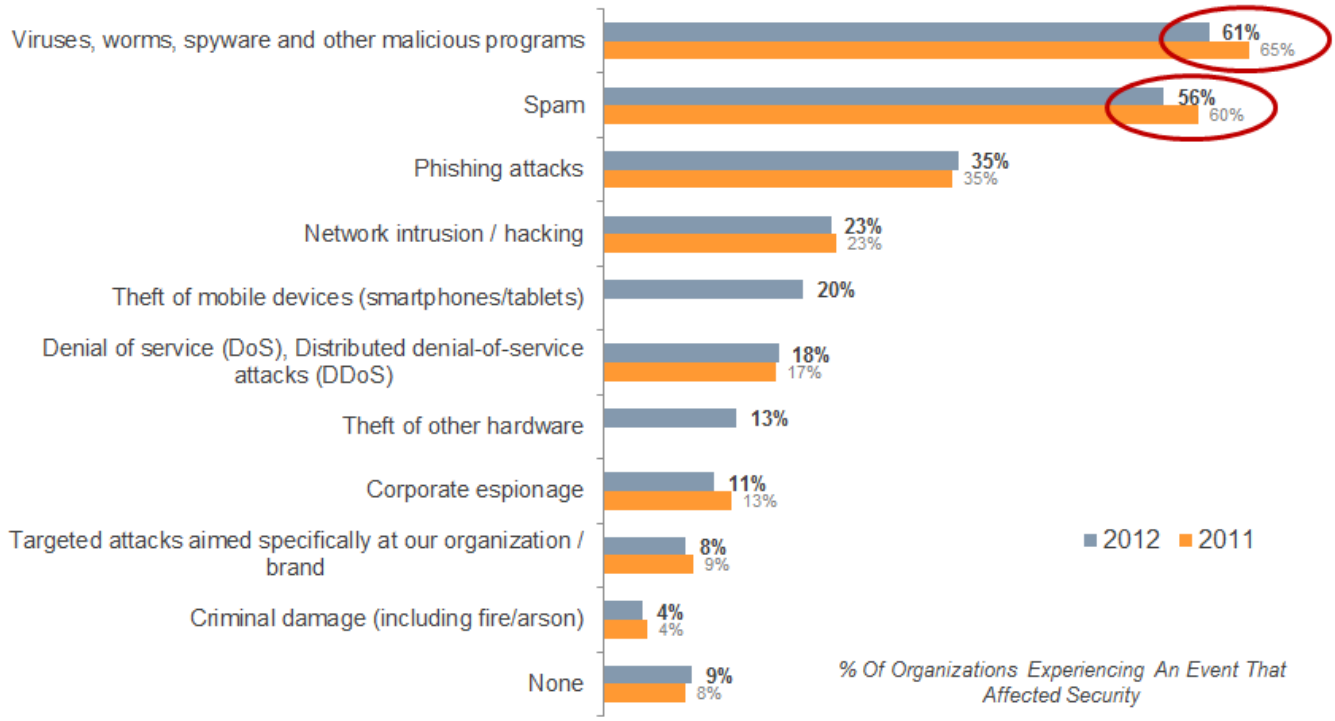
Antivirus protection is still the most popular and frequently used method of protection against external threats. At the same time, IT specialists are aware that a solution that only blocks malicious programs is incapable of providing corporate IT infrastructure with comprehensive security. That is why 14% of business representatives consider it necessary to improve both anti-malware protection and other solutions. In particular, the specialists see the huge potential of encrypting highly sensitive data (10%) as well as improvements to the structure of a company's local network (9%).

Cyber-threat awareness is surprisingly low



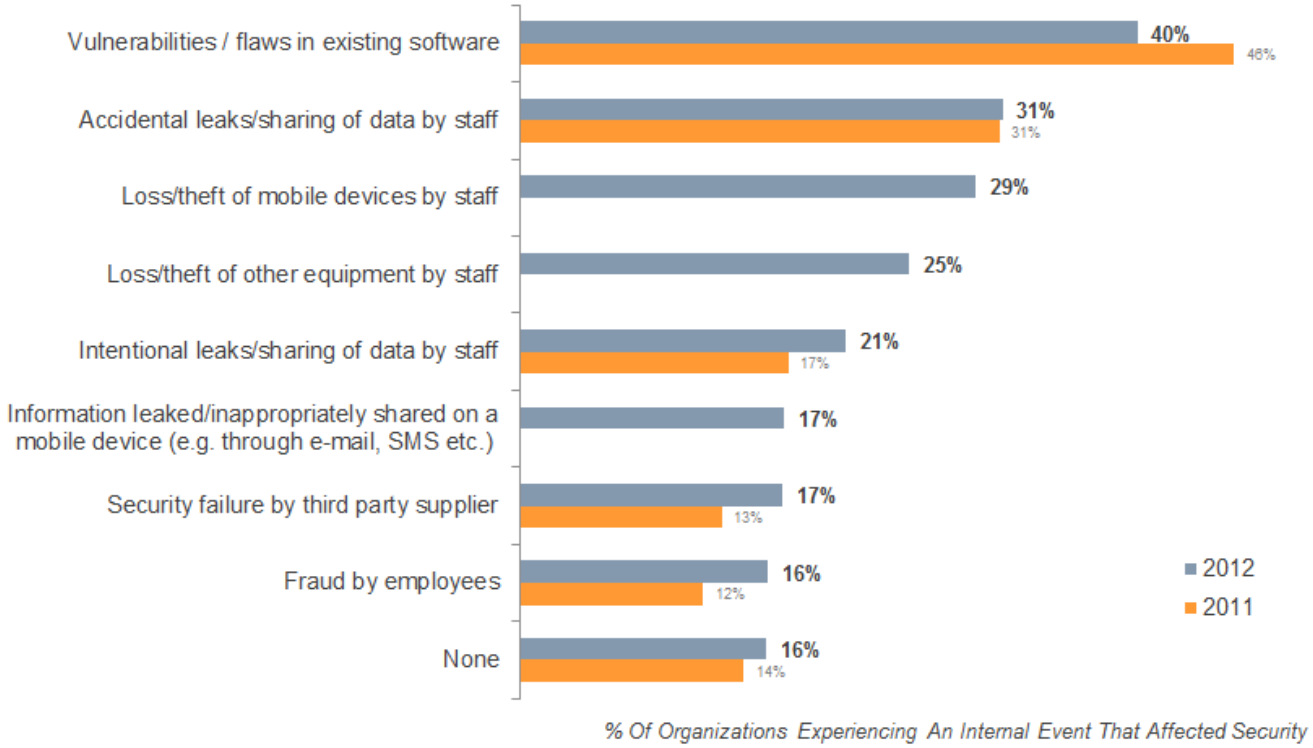
The survey revealed that 31% of IT professionals have not heard of any of the most common cyber-threats including those targeting the corporate sector. It turned out that only 31% of respondents were aware of SpyEye and Zeus, while Duqu went largely unnoticed – only 13% of those surveyed having heard of the computer worm. It should be noted that nearly half of those who have heard about these threats consider them a danger to their business. However, the general cyber-threat awareness of the modern IT professional leaves much to be desired.

External threats encountered: malware, spam and phishing



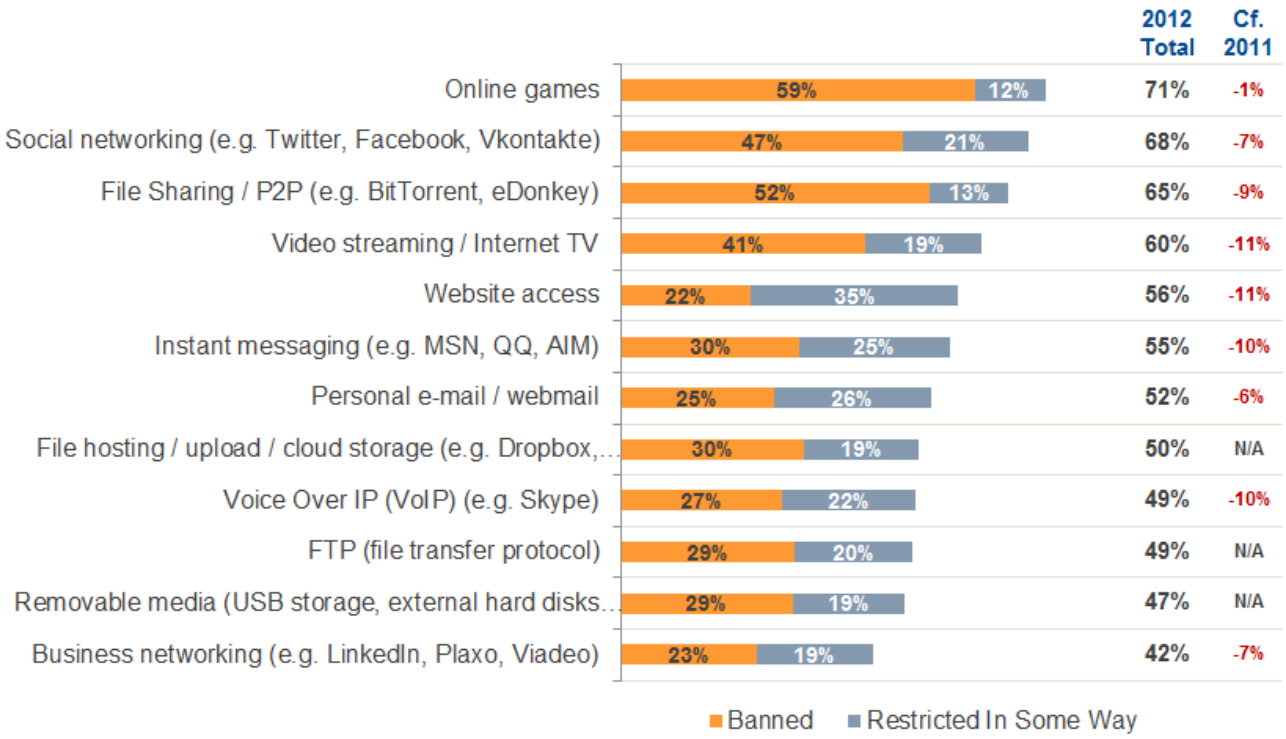
The most common threats faced by IT specialists are malicious programs (61%) and, unsurprisingly, spam (56%). Both points demonstrated a slight decline of 4% though this is insignificant considering the general number of attacks. Phishing is the next most common threat (35%) followed by network intrusions (23%) – the share for both are unchanged from the previous year. Only 8% of respondents said they had encountered targeted attacks, one of the most advanced threats. Interestingly, despite the minimal changes to the percentages recorded for the various threats, the number of data loss incidents increased significantly: 35% compared to 30% in 2011.

Internal threats encountered: vulnerable software causes most concern



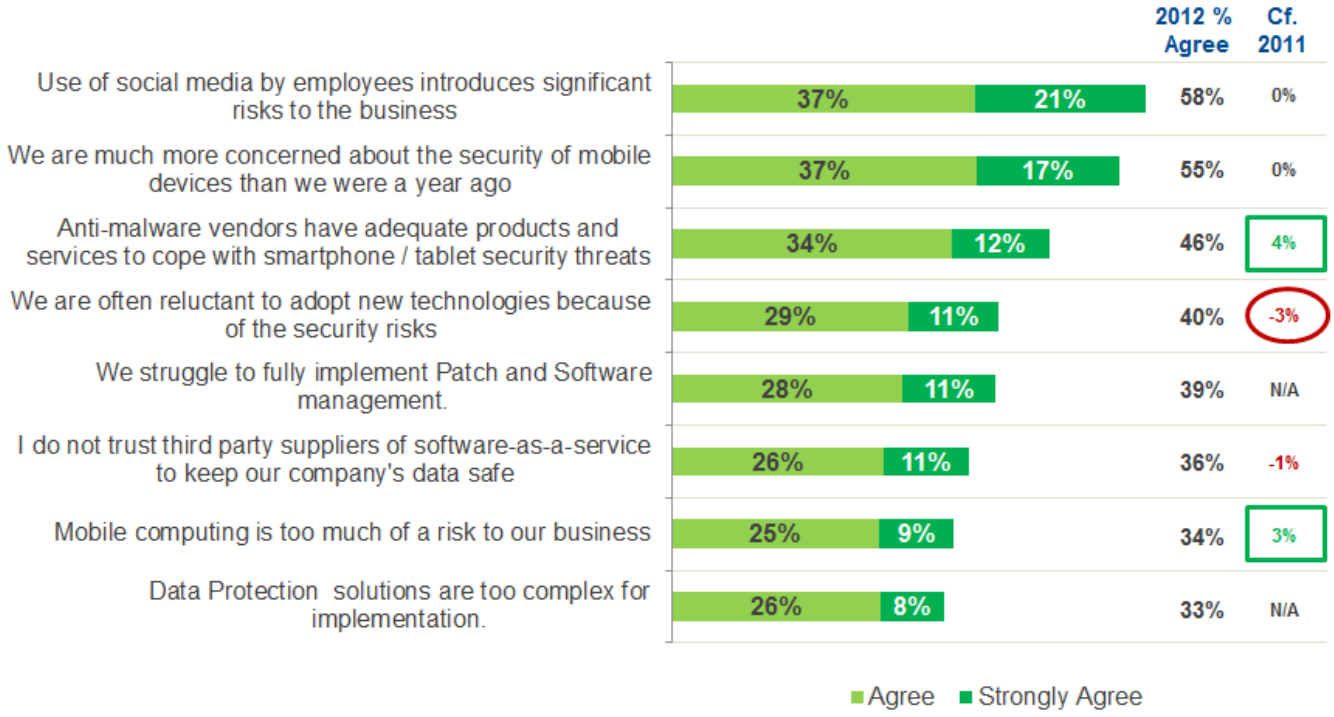
In addition to the external threats originating from cybercriminals, there are internal threats that can be just as dangerous. The most common internal threat faced by IT professionals is that of vulnerabilities in software – cited by 40% of respondents. This comes as no surprises as targeted attacks on companies usually involve the exploitation of vulnerabilities in software. Other internal threats are directly linked to a company's employees: 31% of those surveyed experienced data leaks due to the actions of staff and 29% said their companies had suffered the loss or theft of mobile devices.

Banned or restricted activities: gaming, file sharing and social chitchat



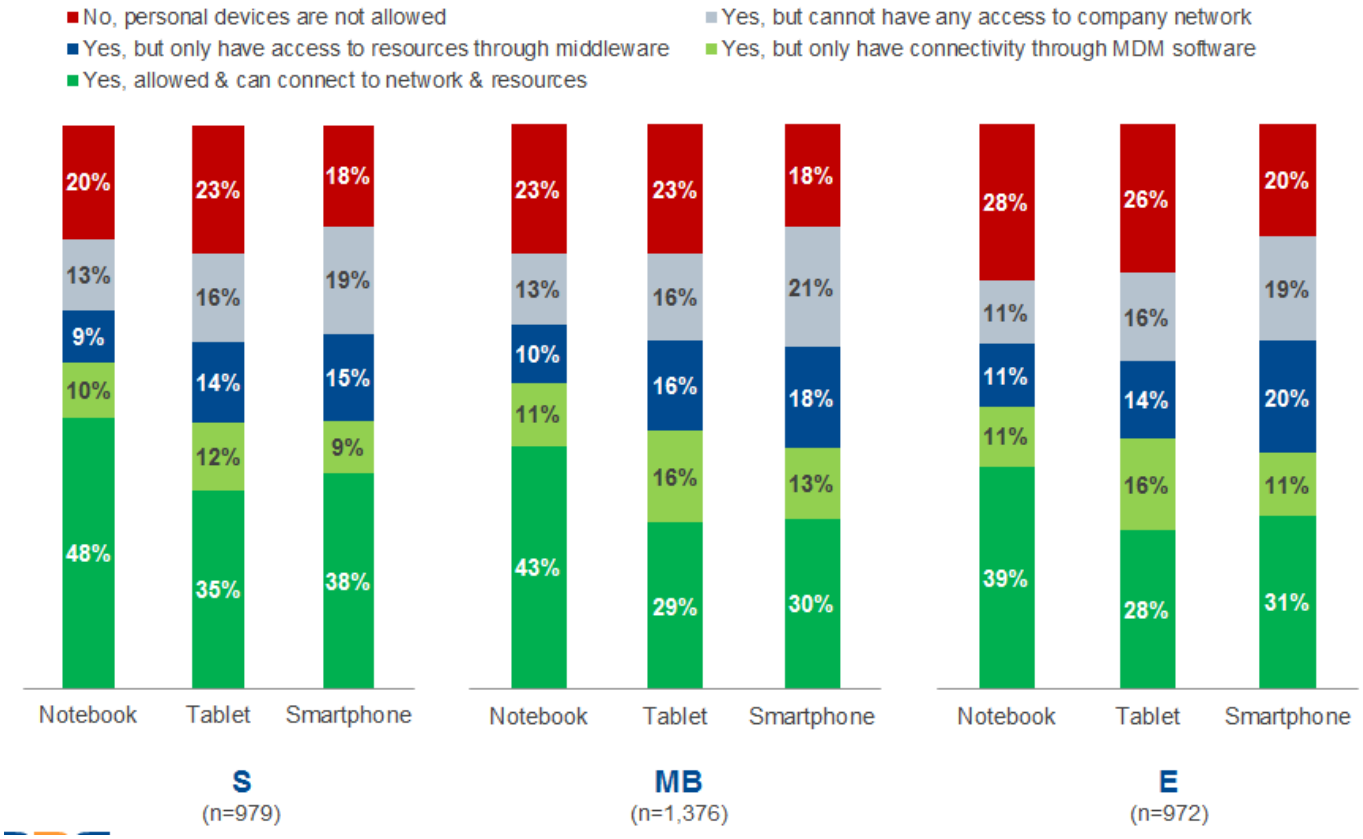
To combat internal and external threats as well as to increase productivity a company's IT department may restrict access to certain resources. First place is occupied by online games, with 71% of companies blocking them in one way or another. 68% of respondents said their companies restrict access to popular social networking sites, although only 42% of those surveyed apply this rule to business-related social networks. 22% of respondents impose a blanket ban on websites altogether, while another 35% enforce certain restrictions. The survey results show that companies are trying to block the two main categories of online resources – time wasters that eat into staff working time (games, online videos etc.) and those that could lead to a data breach (cloud file storage, external media, etc.). Social networking sites fall into both categories: not only can employees spend their work time on such sites, they can also inadvertently disclose sensitive information. The fact that online games are the most frequently banned online resource suggests that companies are more concerned about the staff performance than corporate security. Considering the growing number of targeted attacks and business threats in general, more attention should be paid to breaches of sensitive data.

Mobile devices: a new problem for business



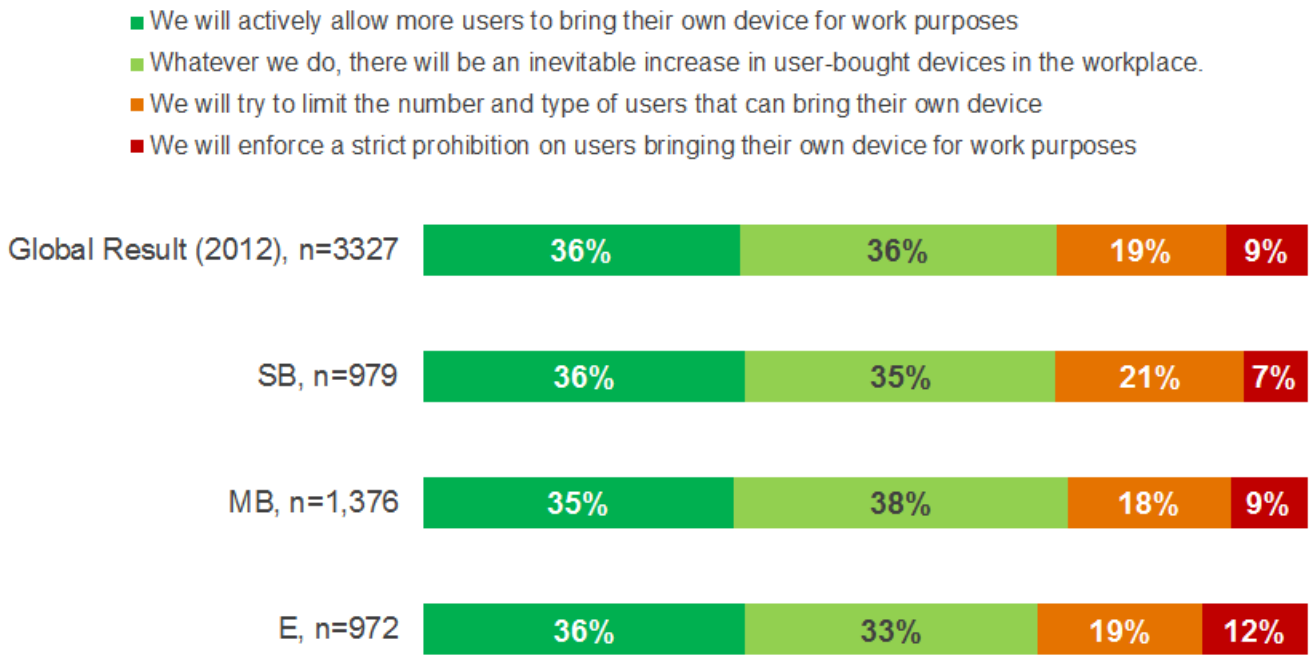
That which just a year ago seemed highly unlikely is today rated by IT professionals as a very real threat. The survey revealed that 34% of respondents consider mobile devices a serious threat to business while 55% admit they are thinking more about the security of corporate smartphones and tablets than they did last year. This is not surprising given that 10% of respondents have already experienced data leaks following the loss or theft of mobile devices.

Personal devices: won't restrict them, but can't manage them yet



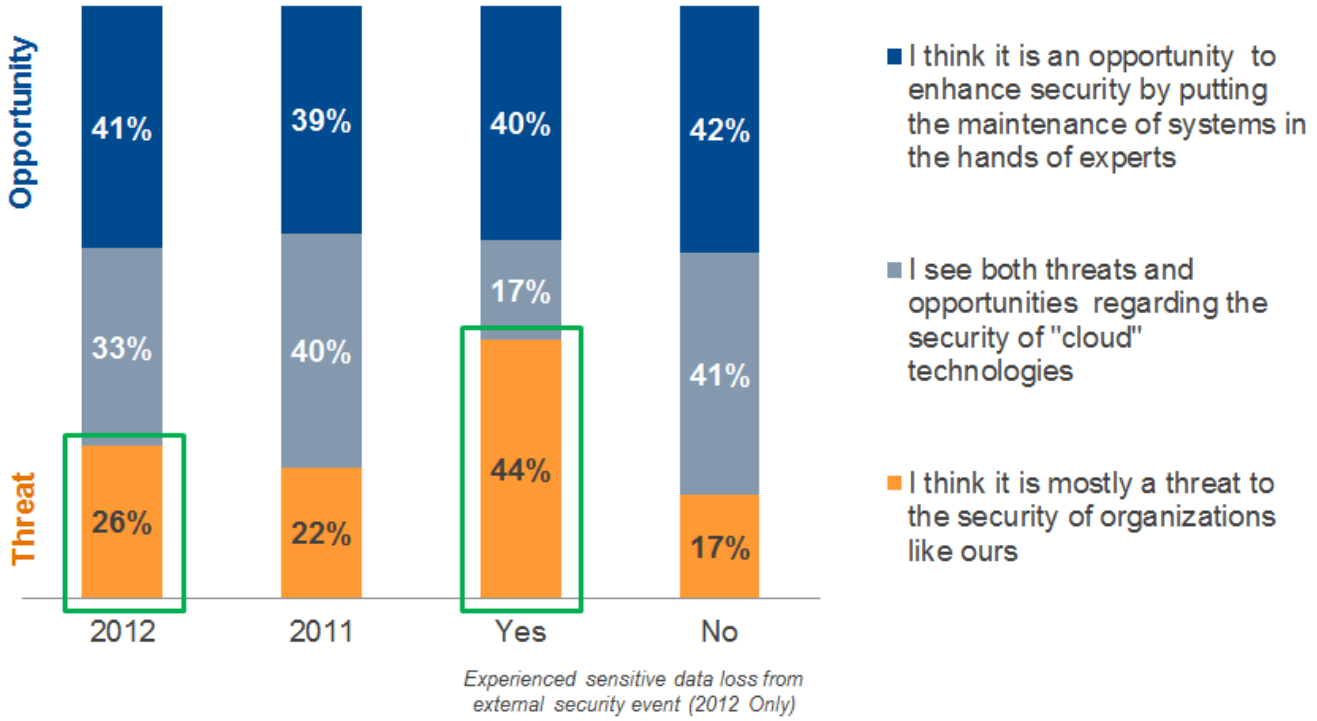
Although more and more IT professionals are inclined to consider personal mobile devices as a security threat, companies show no sign of banning them or otherwise restricting their use. For example, personal smartphones are prohibited in just 19% of companies, while full access to corporate resources is provided by 33% of companies. Small businesses are less likely to introduce restrictions. For instance, the use of personal laptops is allowed in almost half the companies (48%) in this category, whereas in big enterprises the figure is 39%. The deployment level of dedicated tools to ensure the security of mobile devices (Mobile Device Management) is still extremely low both in small and large companies.

BYOD: imminent future



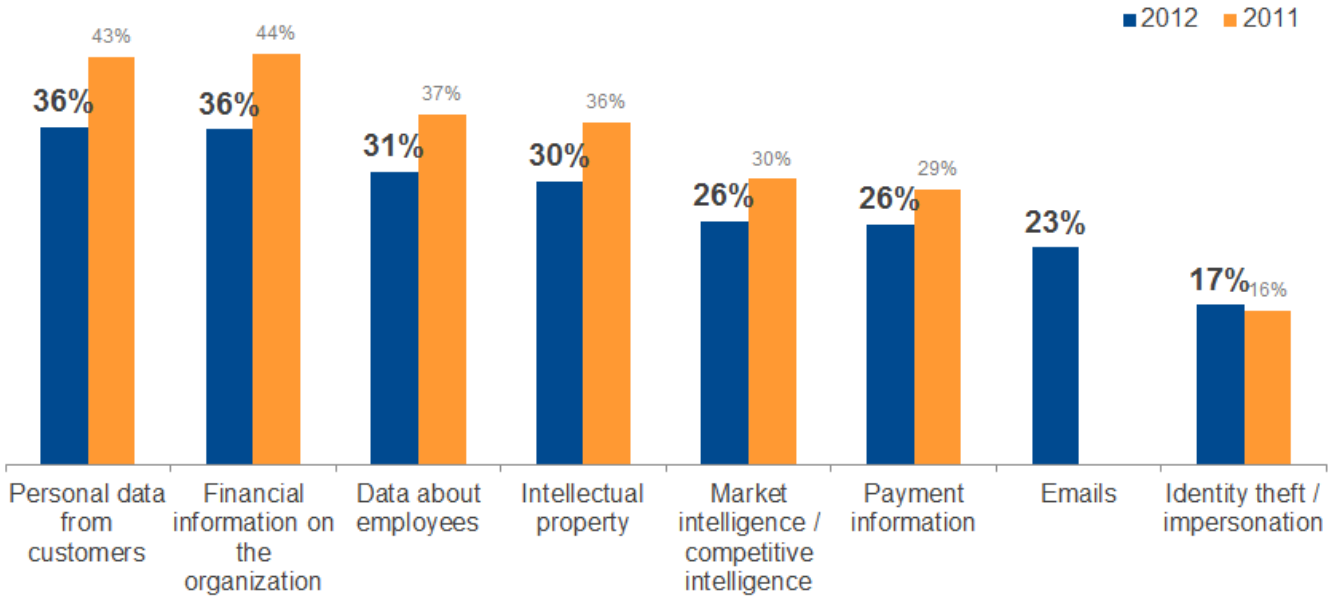
Most companies have a positive attitude to the 'bring your own device' concept where employees use their personal devices for work, or at least view this IT infrastructure development as inevitable. Only 9% of respondents are planning to ban the use of personal devices, while 19% intend to restrict the number of tablet or smartphone users who have access to the corporate network. At the same time 36% said they were even going to encourage their employees to use personal devices for work. This approach could benefit a company but only if common safety rules for personal devices are enforced and an effective solution is implemented to control and protect all devices, regardless of whether they belong to the employee or the company.

Cautiousness towards cloud is in the rise



The popularity of cloud systems and services is growing among both home users and businesses. 41% of respondents see cloud services as an opportunity to strengthen the security of a company's corporate network by transferring part of the infrastructure such as a mail server to third-party experts. However, it should be noted that using the cloud can pose a security risk, especially when it comes to confidential data – something that 26% of IT specialists agree with. Over the past year companies have been able to better understand and evaluate both the benefits and risks of cloud technologies. Meanwhile, the number of IT professionals who consider the cloud a threat to their business has increased by 4%.

Confidential data loss



The loss of confidential data can result in serious problems for a company and its reputation. However, the situation in the field of data protection is anything but straightforward. The type of data breaches cited most by IT professionals surveyed were highly sensitive personal data from customers and financial data. The use of dedicated solutions to protect data could reduce the risk of data breaches, but one-third of the respondents think the implementation of such systems is too complicated.

Conclusion and recommendations

Protecting against cyber-threats is one of the most important tasks facing both small and large businesses. Viruses and Trojans, spam, software vulnerabilities, and careless handling of confidential information are just some of the problems faced by IT professionals on a regular basis. In the future they expect an increase in the intensity of targeted attacks. Yet another growing problem is that of employees accessing the corporate IT infrastructure with their personal mobile devices.

Increasing the level of computer literacy among staff is an essential element of security, while top management must be fully aware of the potential consequences of cyber-threats and understand that reliable protection of the corporate network is necessary to ensure the effective development of a company's IT infrastructure. Currently only half of the experts surveyed feel their company is ready to face today's and there's little to suggest that this situation is set to change. Based on the results of the survey, Kaspersky Lab suggests the following set of recommendations to protect your business against digital threats:

- **Data encryption**

Confidential data leaks are one of the biggest challenges facing all companies. We strongly recommend the partial or complete encryption of data as an additional layer of security. Even if a device ends up in the wrong hands or a malware attack is successful, a cybercriminal that gains access to files that have been encrypted will not be able to see their contents.

- **Paying particular attention to personal devices**

Many employees at both large and small companies use personal devices, usually mobile, to connect to the corporate network and work with confidential information. Sometimes these devices are not sufficiently protected which can lead to data loss. For employees the use of personal devices for handling corporate data is so natural that they don't even think about the dangers. That's why the company needs to implement a security policy that covers the use of both personal and corporate mobile devices for work-related tasks.

- **Be prepared for targeted attacks**

Although targeted attacks are not as common a threat as worms and Trojans, in the future the number of attacks targeting the infrastructure of specific companies will grow. One-third of those surveyed believe that their company will eventually be attacked with highly unpredictable consequences. We recommend putting measures into place now for combating targeted attacks, and in particular paying more attention to proactive protection methods designed to prevent threats rather than dealing with the consequences.

- **Educating staff**

The survey showed that a significant number of key specialists don't know anything about the cyber-threats they are expected to combat. This is compounded by a low level of computer literacy among employees which can lead to a company's IT infrastructure being infected or confidential information being leaked. That is why teaching company personnel all the basics of IT security is no less important than installing the latest security software.