Global IT Security Risks

June 17, 2011

Kaspersky Lab leverages the leading expertise in IT security risks, malware and vulnerabilities to protect its customers in the best possible way. To ensure the most effective protection for businesses it is important for us to understand what IT managers think about security, how they deal with various problems, and what the main concerns are. In order to achieve better knowledge, we actively communicate with our clients and partners and align our strategy taking this feedback into account. This helps us a lot in developing the best security solutions for companies of all sizes and industries. To further study business needs, we initiated global research, covering various aspects of IT security.

The research was performed in partnership with B2B International, one of the leading global research agencies. More than 1300 IT professionals in 11 countries participated in the survey . All of them influence IT policies and take part in evaluating security risks. The survey covers businesses of all sizes, starting from small (10-99 people) to medium (100-999) and large (1000+). A wide range of topics relating to IT security was covered, including wider business risks, actions taken to protect the business, and incidents that have occurred.

Contents

Main findings

IT security is the biggest concern

IT strategy is one of the main concerns for businesses, ranked higher even than financial, marketing and human resources strategy. Almost half of all organizations see cyber-threats as one of the top-three developing risks. Wider business threats may also be a result of an IT security breach. These include damage to brands, espionage, and intellectual property theft. Meanwhile, businesses of all sizes have to deal with an ever-growing number of Internet-enabled devices, with the majority of “endpoints” connected to the Internet, especially in large corporations. Three quarters of all companies globally expect an increase in the number of devices in the next 12 months.

A significant number of businesses have already become victims to cyber crime, including targeted attacks, events of corporate espionage and loss of sensitive intellectual property. This in turn leads to the conclusion that cyber threats have become much more important for business, which was confirmed by 46% of the organizations.

59% of companies report to be at least well-equipped against cyber threats. However, small businesses indicate a lower level of confidence. Almost half of the organizations have experienced an increase in the number of cyber-attacks against them in the last 12 months. Businesses are worried that cyber-attacks may involve organized criminal gangs and are concerned about government interference. As a result, prevention of IT security breaches was the #1 concern in all regions among IT staff.

Top external threat: malware

In the last 12 months 91% of companies have experienced at least one IT security event from an external source. The most common threat comes in the form of viruses, spyware and other malicious programs. 31% of malware attacks resulted in some form of data loss, with 10% of companies reporting loss of sensitive business data. The second most frequent accident is network intrusion; 44% of companies surveyed experienced a security issue related to vulnerabilities in existing software. 18% of the organizations also reported intentional leaks or data being shared by staff. Loss of sensitive data occurred in almost half of these cases.

Security breaches most frequently result in the loss of financial data, followed by personal customer information, intellectual property, and employee information. Levels of sensitive data loss are much higher in developing markets. For example, 12% of companies experienced a loss of payment information, but in emerging markets 19% of organizations reported such an incident. While malware has proved to be the most effective weapon of the cyber-criminal, each of the Top-5 security threats are also related to IT security - surpassing “traditional” crime such as theft of hardware.

Cautiousness towards new media

Given the fact that knowledge about IT security threats among end users is lacking, companies restrict their activities in some way. Thus, 57% of organizations agreed that use of social media by employees introduces significant risks. 53% of companies have banned these kinds of services for end users, and a further 19% restricted access in some way. Social networking is the second most restricted activity, with the most restricted being file sharing; then comes video streaming, instant messaging, personal e-mail, and VoIP. Restrictions are most frequently applied in larger corporations. File sharing and social networking are also regarded by IT staff as the most potentially dangerous end user activities.

Growth of mobile workforce is the next challenge

The security of mobile devices is a new issue for businesses. 55% of the companies reported that they are much more concerned about this subject than they were a year ago. In fact, around a third of the workforce has been “mobile” for some time already. However, only 36% of companies have a fully implemented policy to deal with security off-site. Just 30% have separate policies for mobile devices, and even less require mobile data encryption. Companies that have taken the mentioned measures evaluate them as least effective. It is no surprise that a third of businesses think that mobile computing is too risky to adopt. There is no doubt that the number of mobile personnel will grow, so mobile devices should be guarded by the same security policies and solutions as traditional PCs.

Reluctance in adopting new technologies

Emerging new technologies such as cloud-based services are evaluated as a possible new source of security risks. 42% of companies are occasionally reluctant to adopt new technologies because of the risks involved. Software-as-a-Service, being part of the new “cloud” trend, is considered to be an opportunity in terms of security by 38% of the companies. Organizations see this as a possible way to effectively “outsource” security issues to the service vendor. Still, some think that cloud computing is mostly a threat. Others are not sure, seeing both opportunities and threats. The number of companies that do not trust third-party suppliers of SaaS with data safety is still high (38%). Implementing SaaS solutions does not mean cancelling in-house security. There is no difference for cyber-criminals where to steal data from - be it on local or cloud infrastructure. Criminal techniques are mainly the same in both cases.

Anti-malware protection is a must

Protection from malware is the most commonly implemented measure among organizations across the world. It is placed among four core measures, taken by two-thirds of all companies.

- Anti-malware protection
- Client firewalls
- Data backup
- Patch/update management

Still, only 70% of companies have implemented anti-malware protection fully across the business; 3% have no protection at all. The level of anti-malware implementation varies from country to country. In emerging markets 65% of companies have adopted it, while the UK and US show 92% and 82% levels of implementation, respectively. Another key feature of anti-malware protection is that companies of all sizes tend to implement it. It is also seen as the most effective measure along with data backup. Given the number of malware-related incidents, protecting business from this threat is absolutely necessary.

Proactive and reactive approaches to security threats

Just a little over half of companies evaluated themselves as highly organized and systematic in dealing with IT security threats. 33% possess the opposite, fatalistic attitude, arguing that many IT security events are unforeseeable and difficult to prevent. 28% indicated a somewhat complacent attitude. For them IT security breaches are things that “happen to others”, not themselves. The reactive approach is more popular: where companies invest in IT security only after an incident takes place. IT management in businesses using Kaspersky Lab products is more inclined to look for the newest solutions and technologies. But overall, this kind of attitude is not the norm. Using the latest technologies in IT security is important, and company-wide protection has to be implemented before sensitive data is compromised.

More IT security investments as part of the solution

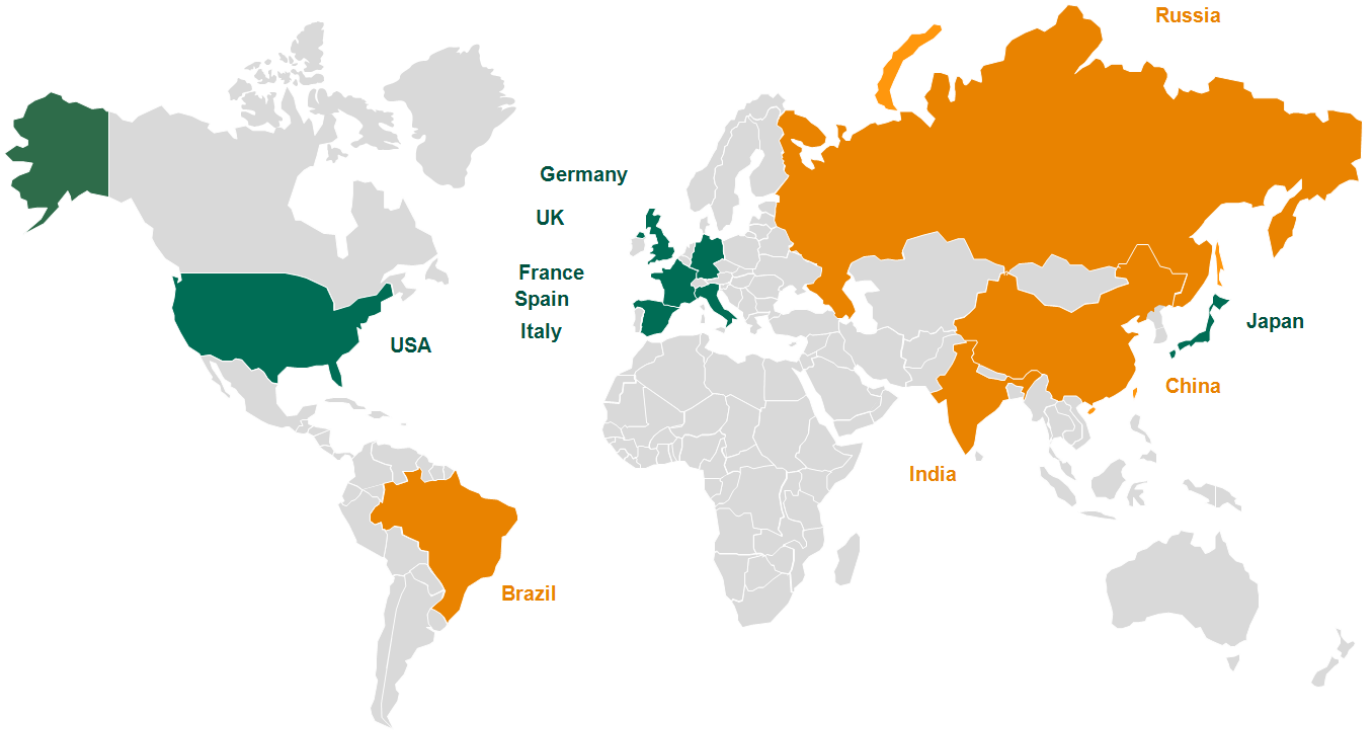
Currently, the average sum of investments in IT security is reported to be €5,500 for small businesses, €58,000 for medium companies and €2.3 million for large corporations. Still, most organizations think that an increase in investment of 25% or more could be required. 45% think that current investment rates are inadequate. More than two thirds reported insufficient resources in terms of staff, systems or knowledge. 48% cited budget constraints as a barrier, and this number is significantly higher in developing countries.

Generally, most of the companies think that extra investment in IT security is money well-spent (69%). But still there is a significant degree of misunderstanding of IT security among those who are in charge of budgets. 34% of company representatives think that senior management does not see IT security as a major problem. Likewise, there are signs of difficulties in explaining the importance of IT security to end users. Only 42% of respondents agreed that most employees are concerned about IT security. The same number of company representatives think that end users are knowledgeable about IT security threats.

The survey showed up a great level of concern about IT security among IT managers in all types of businesses. Below you can find the detailed results of Kaspersky Lab’s research and our recommendations.

In depth overview

Survey details



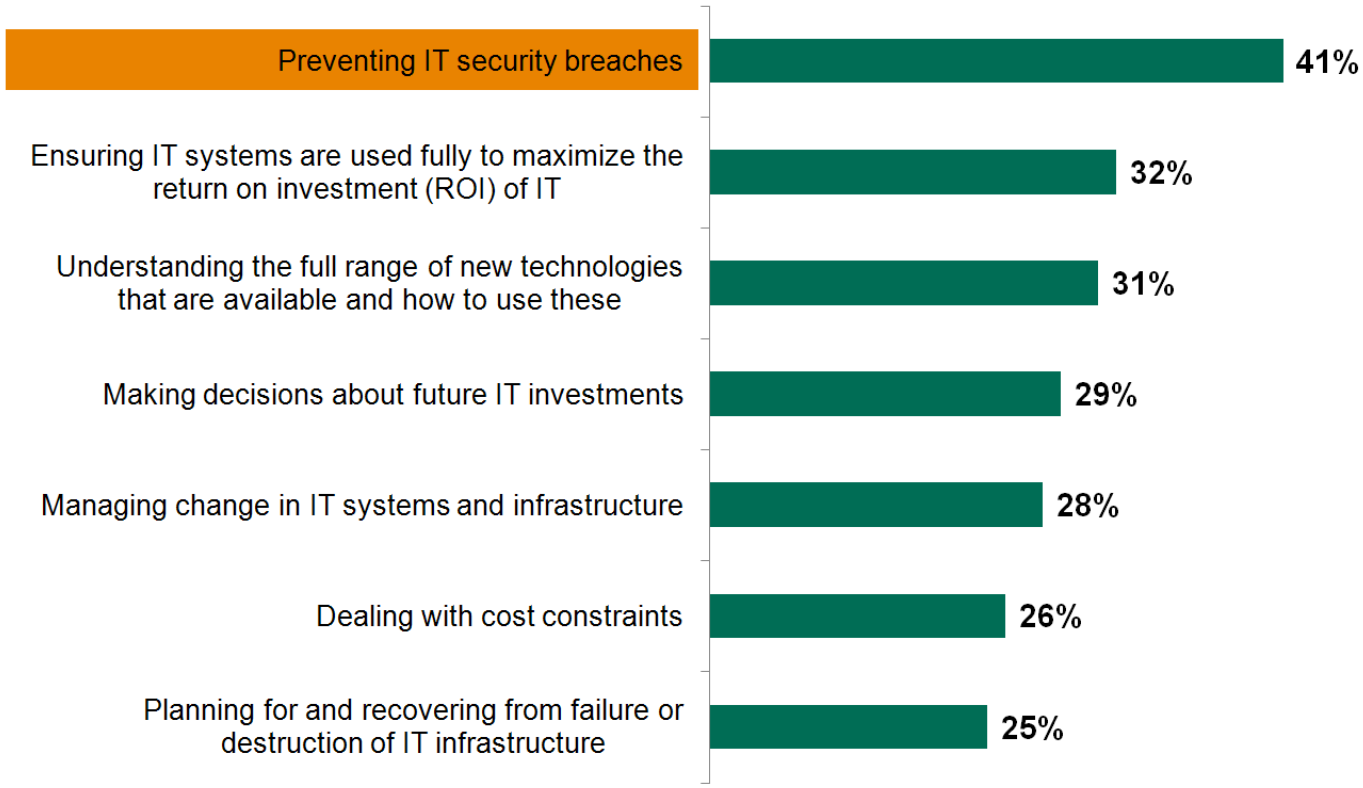
Developing Markets: Brazil, China, India and Russia **(sample=500)**
Developed Markets: Germany, UK, France, Spain, Italy, USA and Japan **(sample=800)**

More than 1300 senior IT professionals from 11 countries took part in the survey. All respondents had an influence on IT security policy, and a good knowledge of both IT security issues of general business matters (finance, HR, etc.) Geographically, the survey was conducted in 11 countries, including both those with developing and mature economies.

IT is a top-four strategic concern

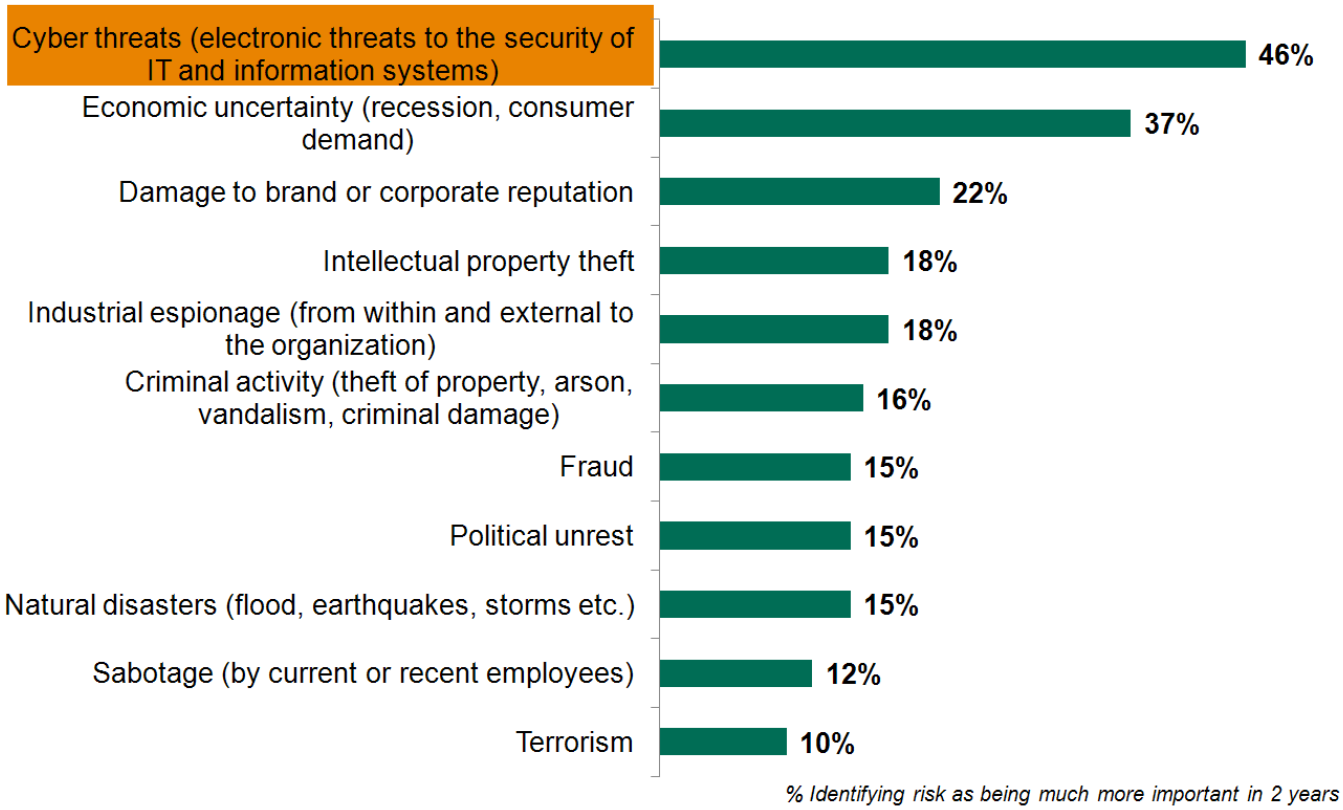
IT strategy was evaluated as one of the most important strategic concerns for businesses, along with operational strategy, development of new products and services and financial strategy.

Main concerns of IT staff



Preventing IT security breaches is the top concern for IT professionals. Understanding new technologies and finding possible ways to implement them is also in the top-three.

Future risks



Almost half of the companies see cyber threats as one of the top-three emerging risks.

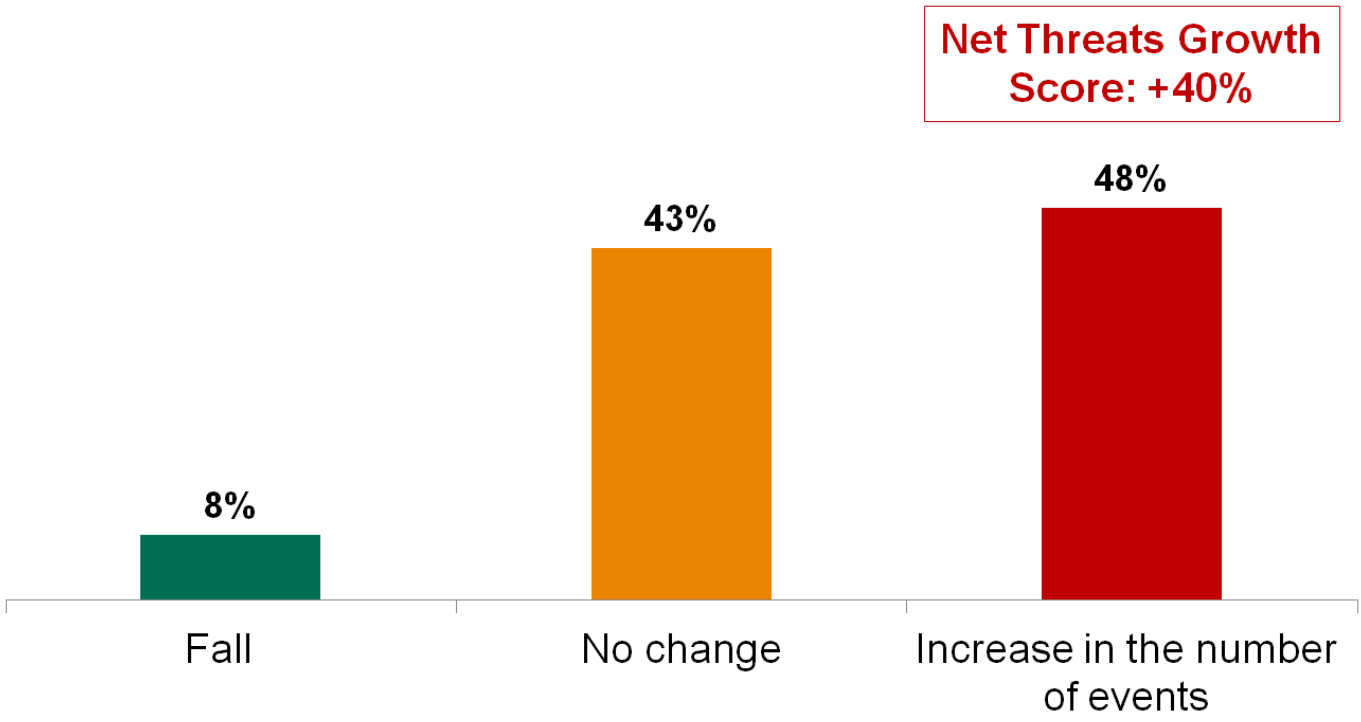
Region-specific IT concerns

Issue	Total	Developing	Developed	Asia	Western Europe
Preventing IT security breaches	1	1	1	1	1
Ensuring IT systems are used fully to maximize the return on investment (ROI) of IT	2	3	3	3	3
Understanding the full range of new technologies that are available and how to use these	3	2	6	4	3
Making decisions about future IT investments	4	4	5	2	5
Managing change in IT systems and infrastructure	5	8	2	10	2
Dealing with cost constraints	6	10	4	5	8
Training users in how to use IT systems	7	5	8	8	5
Planning for and recovering from failure or destruction of IT infrastructure	7	7	7	8	5
Preventing misuse of computer systems by employees	9	6	9	7	9
Dealing with day-to-day unreliability of IT systems	10	8	10	6	10
Complying with industry regulations and standards	11	11	11	11	11

Table shows ranking of concerns of the IT function – Rank 1 indicates the issue selected by most respondents within a group

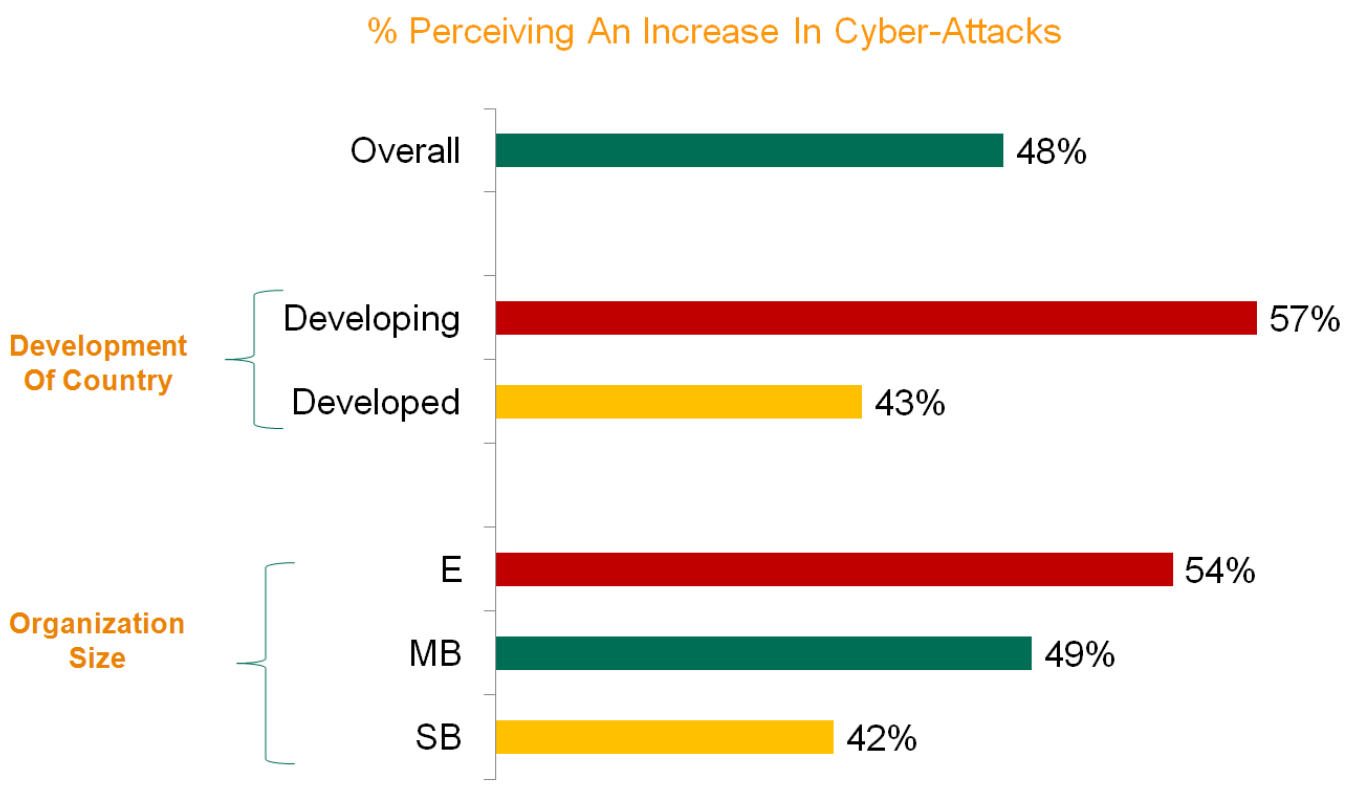
Prevention of IT security breaches was named a main concern in all countries, regardless of the market situation. For other issues there are significant differences between emerging and mature markets. For example, cost constraints are much more important in developed countries. At the same time companies in emerging markets pay more attention to IT-specific education of end users.

Significant increase in the number of cyber-attacks



Almost half of surveyed professionals reported an increase in the number of IT security accidents during the last 12 months. On the contrary, only 8% saw a decrease.

Most danger for developing countries and large corporations



While 48% of businesses reported an increase in number of cyber-attacks, figures for developing countries and large corporations are much higher.

Average annual investment in IT security

Small Businesses
(10-99 Seats)

$8,055

$93/employee

Medium Businesses
(100-999 Seats)

$83,200

$167/employee

Enterprise Businesses
(1000+ Seats)

$3,263,476

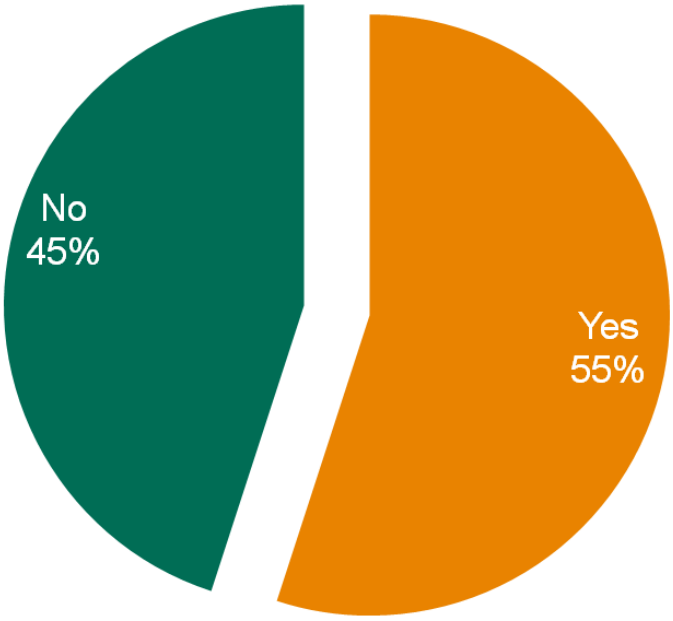
$388/employee

The rate of investment on IT security per employee is the highest for large enterprises. The difference between small and medium businesses is less noticeable.

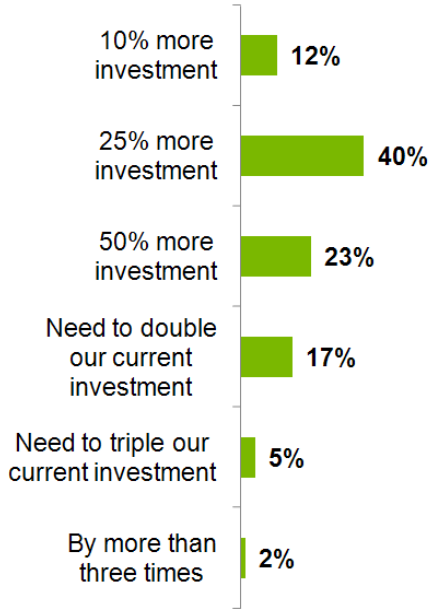
KASPERSKY

More investments required

Adequate Investment In IT Security?

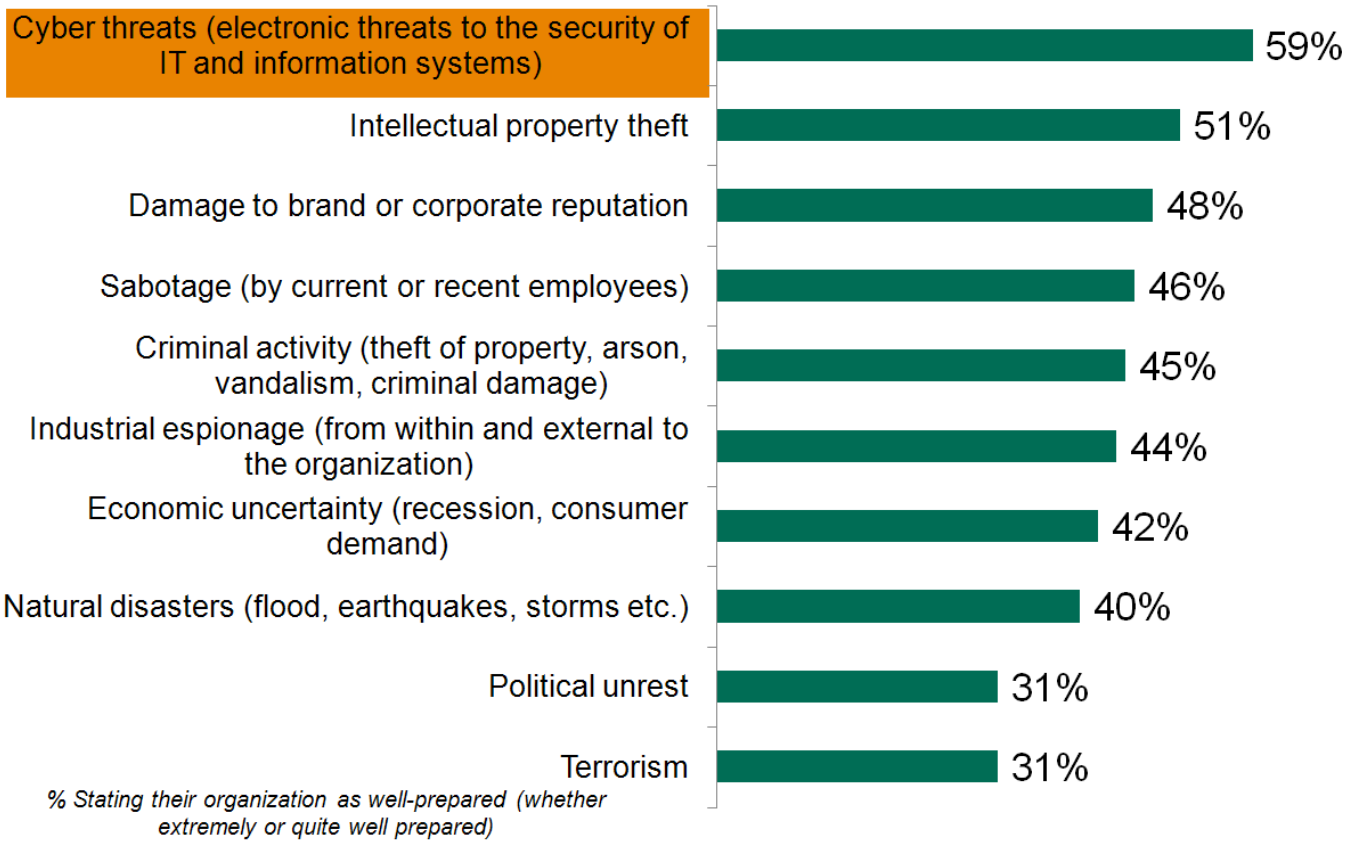


Additional Investment Required…
(Among those who feel current investment is inadequate)



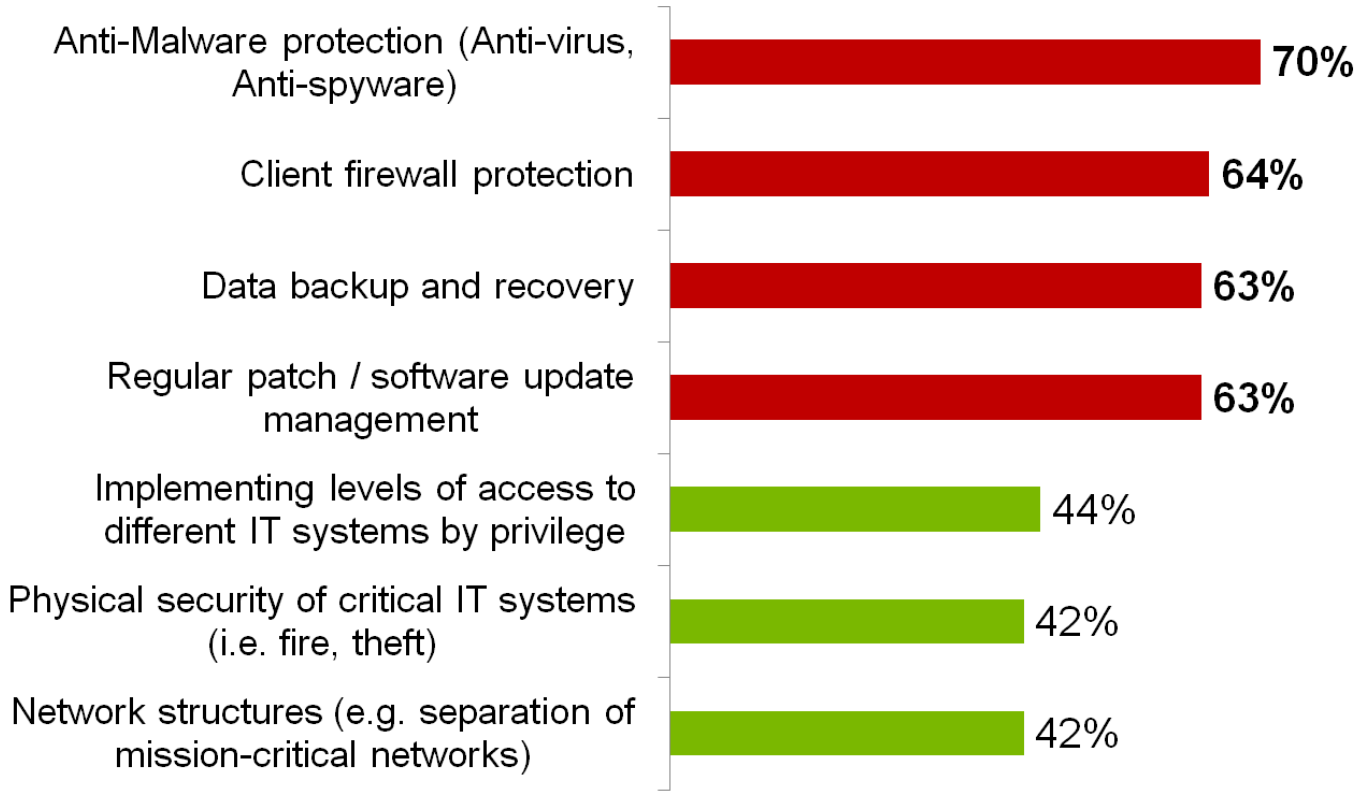
45% of the companies do not feel that the current rate of investment in IT security is sufficient. 40% of respondents feel that a 25% increase in funding is necessary.

Preparedness for different business risks



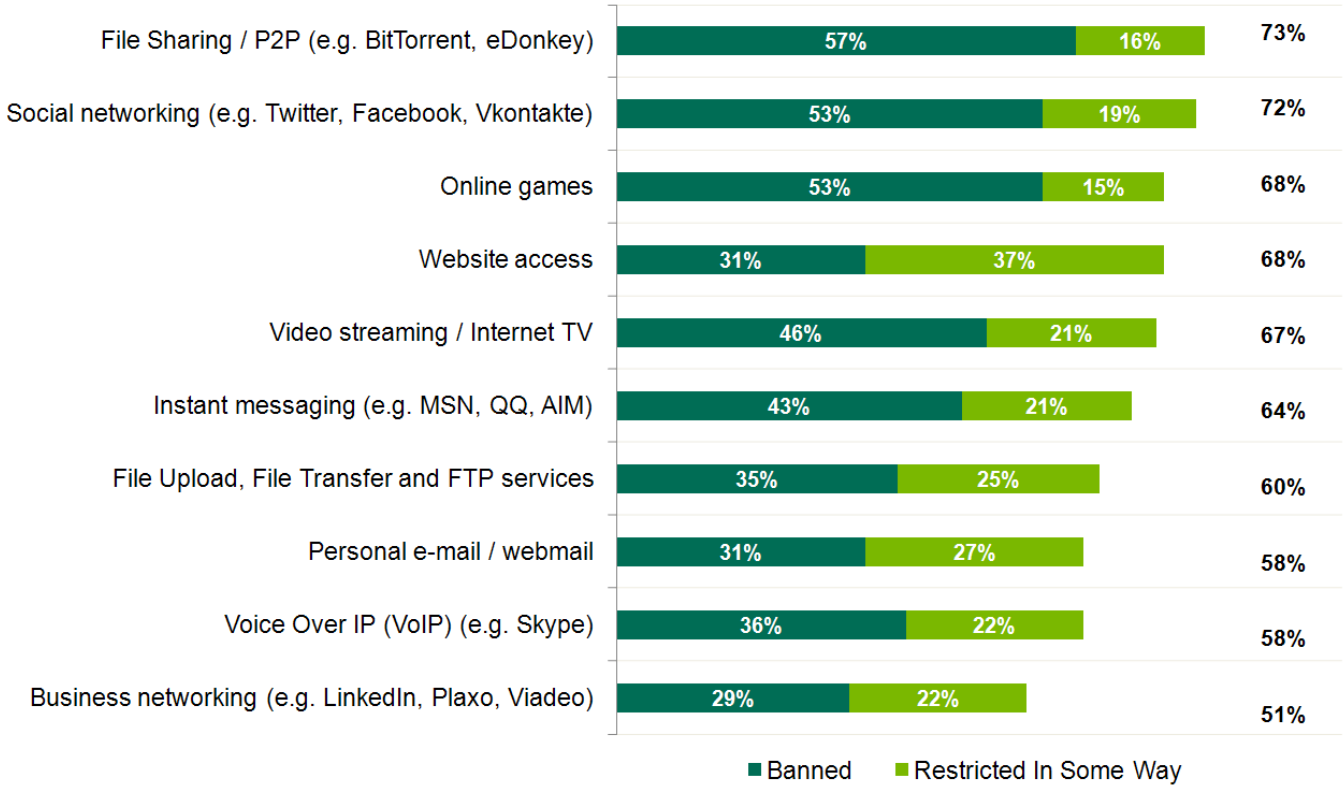
Despite the fact that cyber threats are one of the top concerns for businesses, only 59% of companies feel that they are well-prepared for them.

Top seven measures taken to avert security risks



Anti-malware protection is the most fully implemented security measure. Still, protection from malware has not been implemented completely by 30% of companies, and 3% have no protection at all. Firewall protection, data backup and regular software updates are also implemented quite commonly.

Banned and restricted user activities



Companies are very cautious about new media; most of them ban or restrict access to social networking websites in some way. While file sharing remains the most restricted activity, social networks surpass even online gaming, instant messaging and personal e-mail communication.

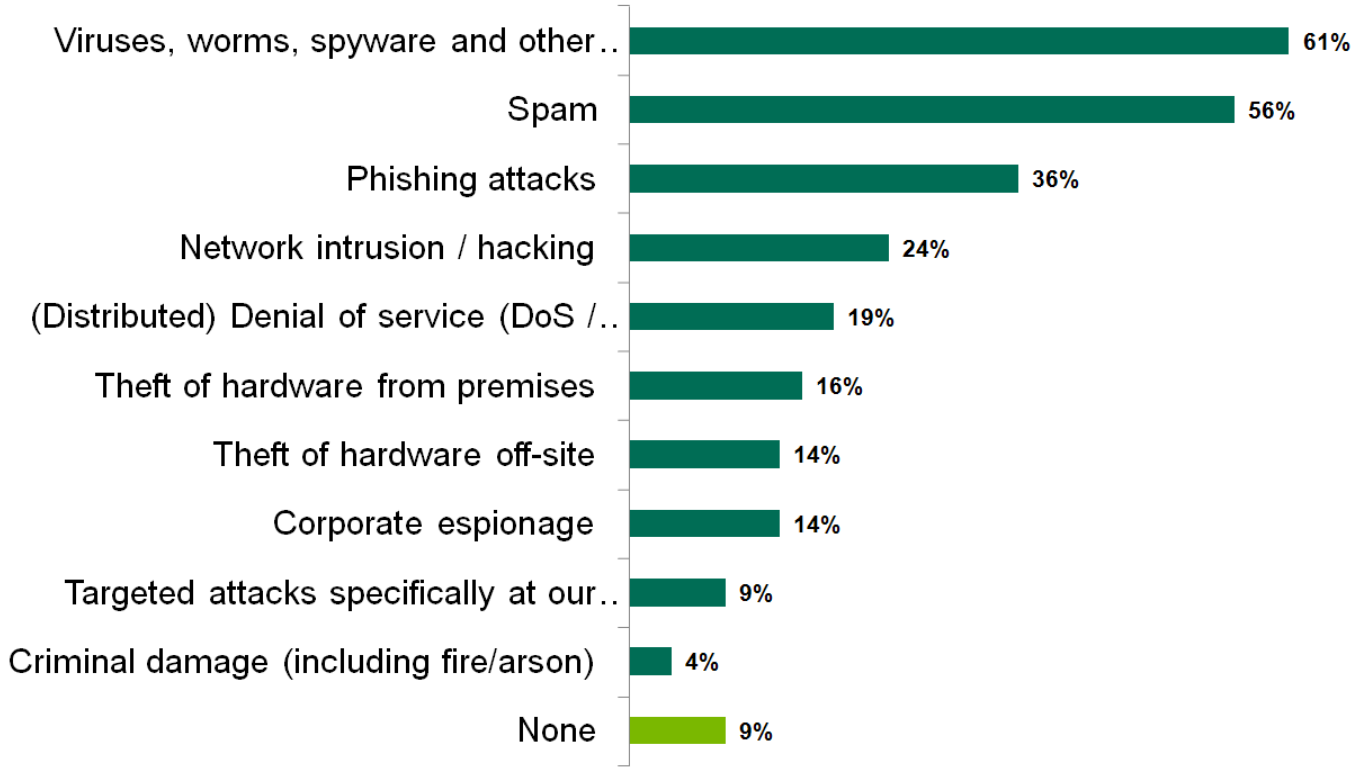
Restrictions by country and economic type

Activity / Application	Overall	Develop-ing	Develop-ed	United States	Russia	China	Brazil
File Sharing / P2P	**55%**	46%	61%	62%	50%	44%	50%
Social networking	**35%**	36%	35%	44%	52%	26%	41%
File Upload, File Transfer, FTP	**34%**	33%	34%	33%	44%	28%	38%
Website access	**32%**	30%	33%	35%	42%	29%	19%
Personal e-mail / webmail	**31%**	29%	32%	36%	22%	28%	32%
Instant messaging	**23%**	32%	18%	20%	19%	36%	35%
Online games	**21%**	21%	21%	19%	16%	21%	32%
Video streaming / Internet TV	**13%**	18%	10%	8%	12%	21%	14%
Business networking	**11%**	15%	9%	5%	4%	24%	7%
Voice Over IP (VoIP)	**10%**	14%	8%	5%	9%	17%	9%

Table shows the % of organizations identifying an application / activity as one of the greatest threats.

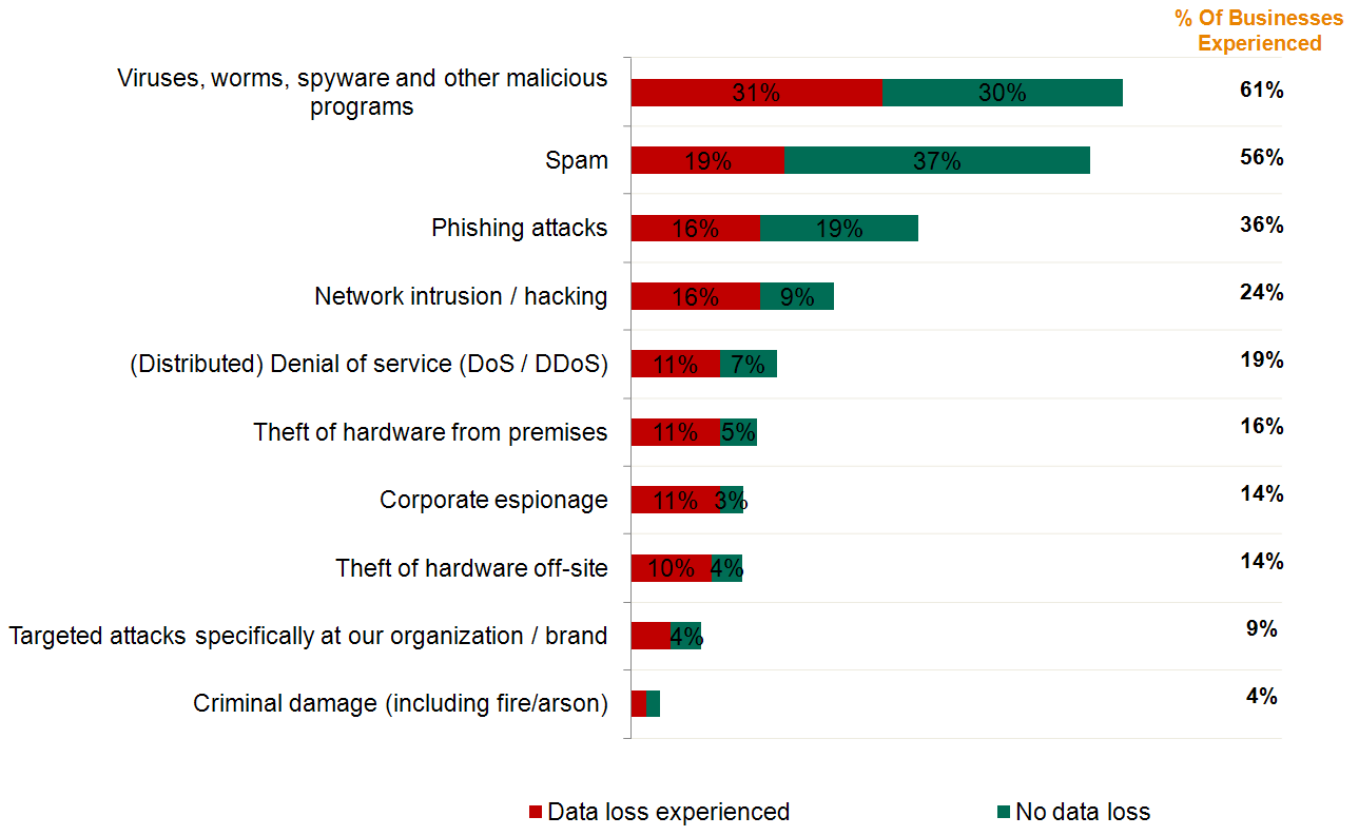
Social networking is seen as the second biggest threat globally, especially in the US, Russia and Brazil. Companies in developed countries pay less attention to restricting instant messaging, although it too may become a security threat.

Types of external threats experienced



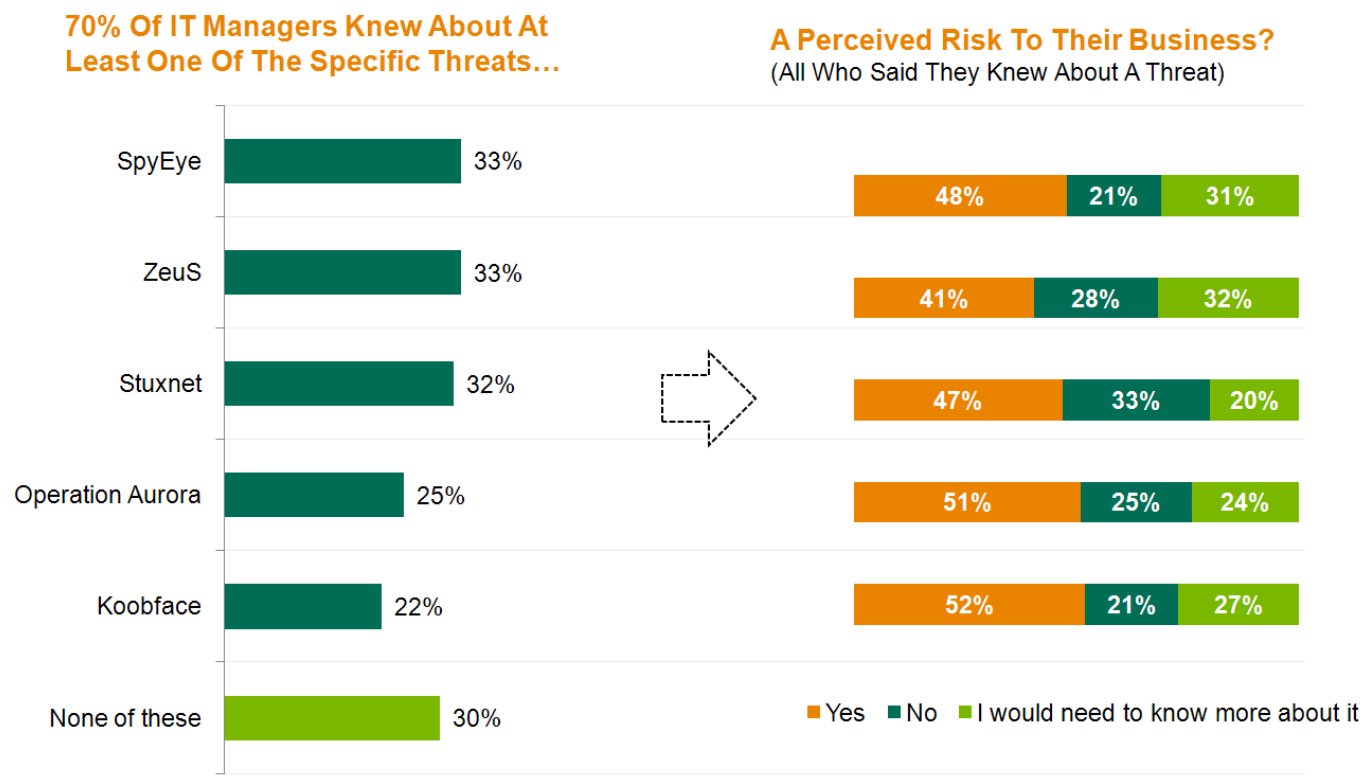
Malware is the most frequent reason behind security incidents, surpassing spam and phishing attacks. The top-five threats are all related to cyber security.

Data loss experienced



The highest number incidents of data loss is also connected to malware, and in 31% of cases the security breach leads to sensitive data loss.

Knowledge of specific external threats



Among the most identified threats are SpyEye, ZeuS and Stuxnet. However, only around half of respondents think that each of these threats puts their company in danger.

Conclusion and recommendations

Among businesses of all sizes around the world there is a solid level of awareness about IT security threats and the respective risks. Cyber threats are ranked as the most growing concern, confirmed by almost half of respondents. At the same time every second company evaluates its IT security budget as insufficient, with a 25% increase in funding seen as necessary. Anti-malware protection, being an essential part of business security, is implemented only in 70% of organizations. This has led to a situation where the majority of companies experienced an IT security breach in the last 12 months, and almost a third lost business information.

Strong IT security across all business departments covering all endpoints is necessary to avoid major damage to a company. The number of cyber-threats, including targeted attacks, may lead not only to sensitive data loss –a company's brand image can also be damaged, which is a top threat for the majority of businesses. At least half of the companies feel there is more work to be done. This includes increasing the number of IT security staff, raising the level of investment and implementing the newest solutions and technologies to protect a company's business.

Recommendations of Kaspersky Lab

- **Choose a security solution that fits your business**

Investment in IT security is important, but the actual budget always depends on the size of your company. Choose a product that addresses all security issues and at the same time perfectly fits your business in terms of the number of endpoints, servers, etc. It is also necessary to be prepared for company growth. Thus, the right security product has to offer a good deal of scalability.

- **Invest in employee education**

Overall, IT security really depends on how much end users know about cyber threats. They do not have to be experts, but it would be wise to spend the time and budget to make them learn more. Remember that the most damaging targeted attacks could never be performed without unintentional "help" from an employee. In other words, when staff think before opening a suspicious e-mail attachment, you save a great deal of money.

- **Ensure effective anti-malware protection for all endpoints, including mobile devices**

Since the highest number of incidents are related to malware, effective protection has to be enforced for all endpoints. Although the majority of companies already use some kind of anti-malware solution, protection of all business branches with all potentially vulnerable endpoints is not common. This recommendation also applies to mobile devices, which are increasingly becoming points of vulnerability. The most effective solution is to expand a company's security policies and introduce centralized control and malware protection for employees' smartphones. Protection of sensitive data in case of device loss or theft is also recommended.

- **Set up a centralized management system for all endpoint devices**

The number of endpoints is growing rapidly, so it is necessary to have a centralized management system to control all corporate devices. Small companies usually do not implement such a system, and at the same time they are the most vulnerable to cyber threats. It is recommended to use specialized small business solutions to protect and manage company endpoints in case of small companies.

- **Protect end user communication instead of restricting it**

It might be possible to protect the corporate network from threats by further restricting end user activity. But it is more effective to protect communication of staff from links to infected and phishing websites. This kind of protection should cover the most frequently used means of communication, including e-mail and instant messaging.