



# Global Corporate IT Security Risks: 2013

May 2013

For Kaspersky Lab, the world's largest private developer of advanced security solutions for home users and corporate IT infrastructures, meeting the needs of its customers is a top priority. In order to keep track of these needs and keep concentrating on developing technologies and solutions for which there is real demand, Kaspersky Lab conducts regular surveys focusing on the key IT security issues and cyberthreats which worry businesses.

In 2011, Kaspersky Lab, in partnership with research company B2B International, carried out its first global survey of IT professionals from small, medium-sized and large companies around the world. The survey aimed to find out what representatives of these companies thought of corporate security solutions, to ascertain their level of knowledge about cyberthreats, what cybersecurity related problems they most often face, how they address these problems and what they expect in the future.

In 2013, Kaspersky Lab and B2B International conducted the third of these surveys. The results provided below reflect the opinions of companies on key issues related to the security of the corporate IT infrastructure. They also reflect the changes that have taken place since the previous two studies. Comparing current and historical data helps to identify and analyze existing trends in this area, ultimately creating a complete and, we believe, objective picture of the threat landscape, as well as future problems and trends affecting corporate IT security.

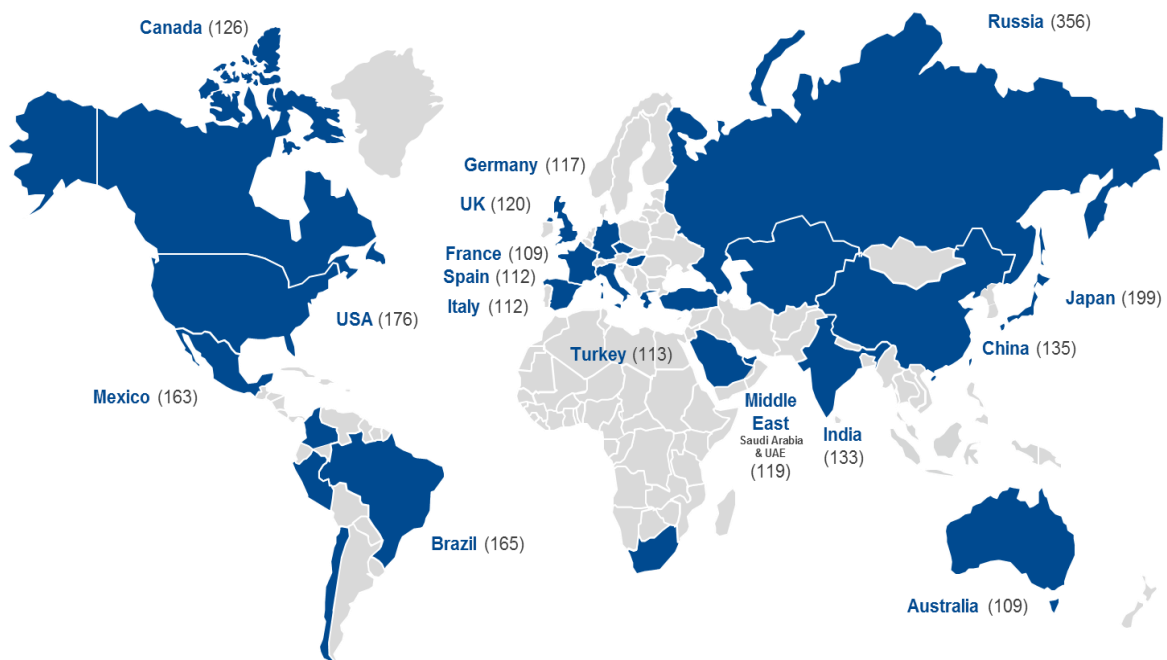
## The main findings

---

According to the survey results, one of the major problems facing businesses is the creation of a clear IT infrastructure development strategy with an information security strategy at its heart. Companies are increasingly determined to secure their IT infrastructure in the light of increasing numbers of incidents – and significant financial losses associated with them. The main findings of the survey are:

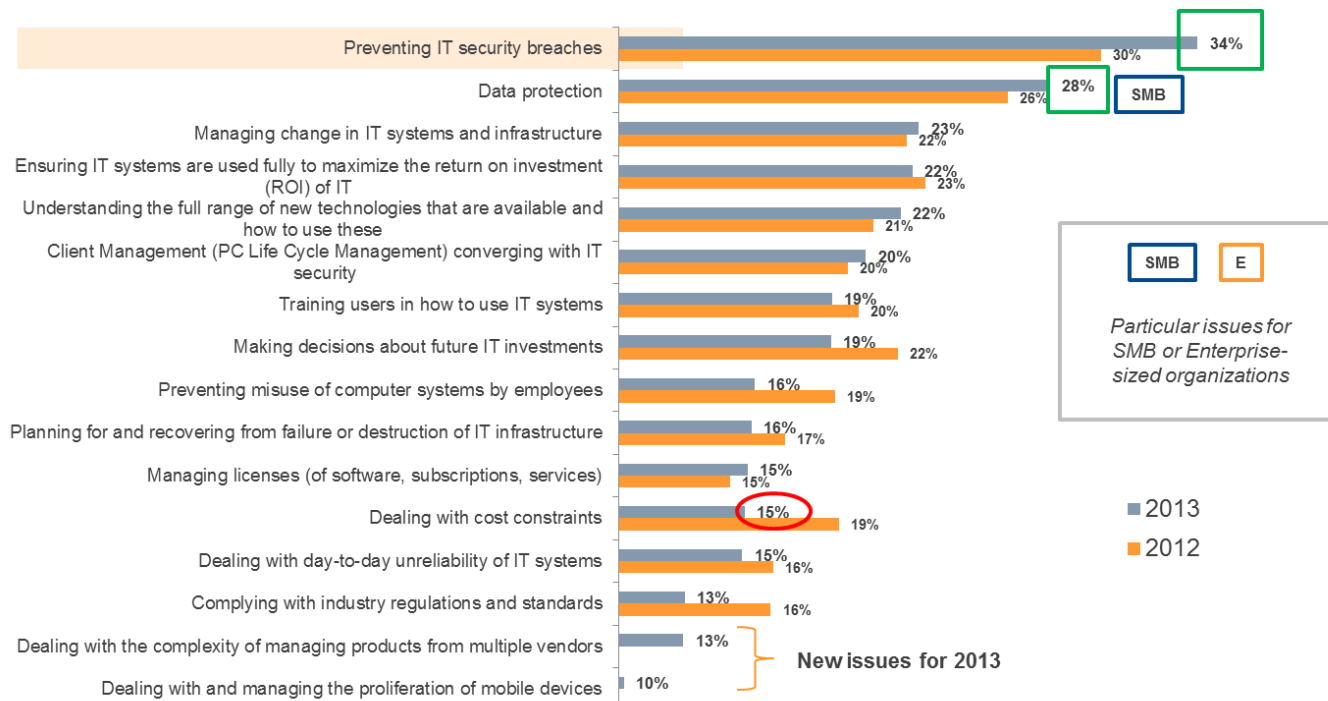
- ▶ Maintaining information security is the main issue faced by a company's IT management.
- ▶ In the past 12 months, 91% of the companies surveyed had at least one external IT security incident and 85% reported internal incidents.
- ▶ A serious incident can cost a large company an average of \$649,000; for small and medium-sized companies the bill averages at about \$50,000.
- ▶ A successful targeted attack on a large company can cost it \$2.4 million in direct financial losses and additional costs.
- ▶ For a medium-sized or small company, a targeted attack can mean about \$92,000 in damages – almost twice as much as an average attack.
- ▶ A significant proportion of incidents resulting in the loss of valuable data were internal, caused by issues such as unclosed vulnerabilities in software used by the company, intentional or negligent actions of employees or the loss or theft of mobile devices.
- ▶ Personal mobile devices used for work-related purposes remain one of the main hazards for businesses: 65% of those surveyed saw a threat in the Bring Your Own Device policy.
- ▶ Information leaks committed using mobile devices – intentionally or accidentally – constitute the main internal threat that companies are concerned about for the future.

## Countries Covered



The B2B International survey is based on 2,895 interviews with IT professionals working in companies from 24 countries across the globe. All respondents had an influence on their companies' IT policies and a good knowledge of both IT security risks and the operation of non-IT divisions of their companies. Most of the companies that took part in the survey can be divided into two large groups. The first comprises medium-sized businesses with 100 to 1500 workplaces equipped with workstations which have Internet access, plus a small number of small companies with 10 to 99 computerized workplaces. The second large group of respondents comprises representatives of large companies with 1500 or more computerized workplaces.

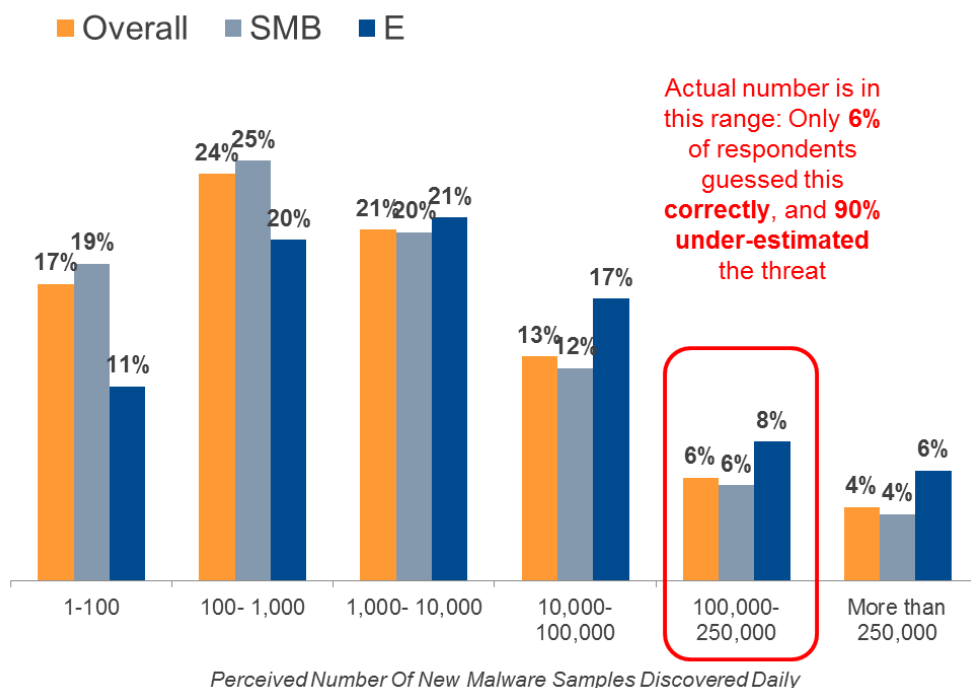
## The IT Function Concerns



As in 2012, preventing IT security incidents and protecting data were the two main priorities cited by IT professionals when discussing components of the corporate IT strategy. Over a third (34%) of respondents ranked protection from incidents as the top priority – a 3% increase on the previous year. Another notable change since 2012 is an increase in concerns expressed by IT professionals about the management of their companies' IT systems and infrastructure. This issue has moved up from sixth to third position on the list of IT management priorities. The fact that it ranks next to IT security is no accident: companies are increasingly aware that unpatched, vulnerable software is systematically used on corporate computers and a large number of unaccounted-for mobile devices are used to process information that is directly related to the company's business. This can result in incidents involving important data being leaked.

Overall, the need to develop a considered IT strategy which includes, among other elements, IT security measures, is one of the top five issues requiring the attention of top managers. About a third of all respondents (31%) emphasized the importance of developing an IT strategy, making this a higher priority than the need to develop a marketing strategy or a staff recruitment and development strategy.

## Perception of daily malware discovery rates: 6% accuracy

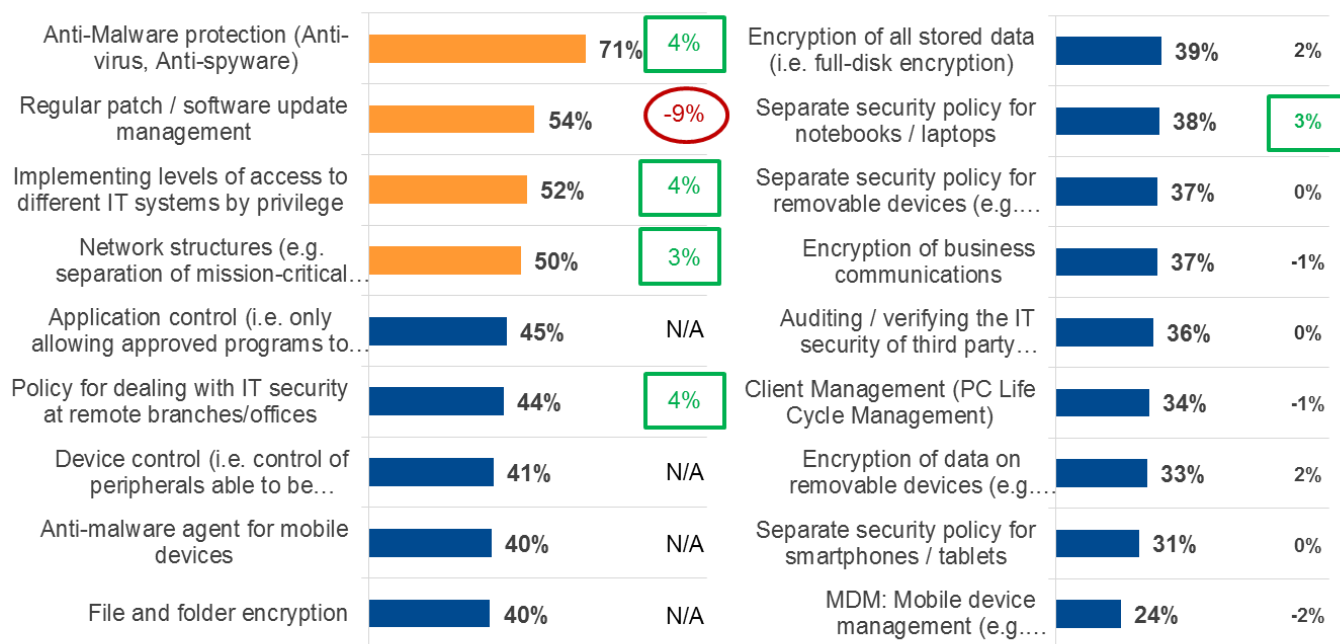


Business Size	Estimated Mean No. Discoveries /Day (Thousands)
Overall	35
SMB	32
E	49

As the survey has demonstrated, the overwhelming majority of companies underestimate the scope of new cyberthreats appearing daily. According to Kaspersky Lab, about 200,000 new malware samples appear every day. Only 6% of the respondents provided estimates that were close to this figure, while about 90% gave significantly lower estimates and 4% significantly higher.

Although this figure alone cannot provide an objective measure of the extent to which businesses are prepared to protect themselves from IT security incidents, accurately assessing the level of threat can seriously affect decisions made by companies in choosing the tools for securing their IT infrastructure.

## Steps taken to minimize risk



N/A issues are new for 2013

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

○ Significantly lower YOY    □ Significantly higher YOY

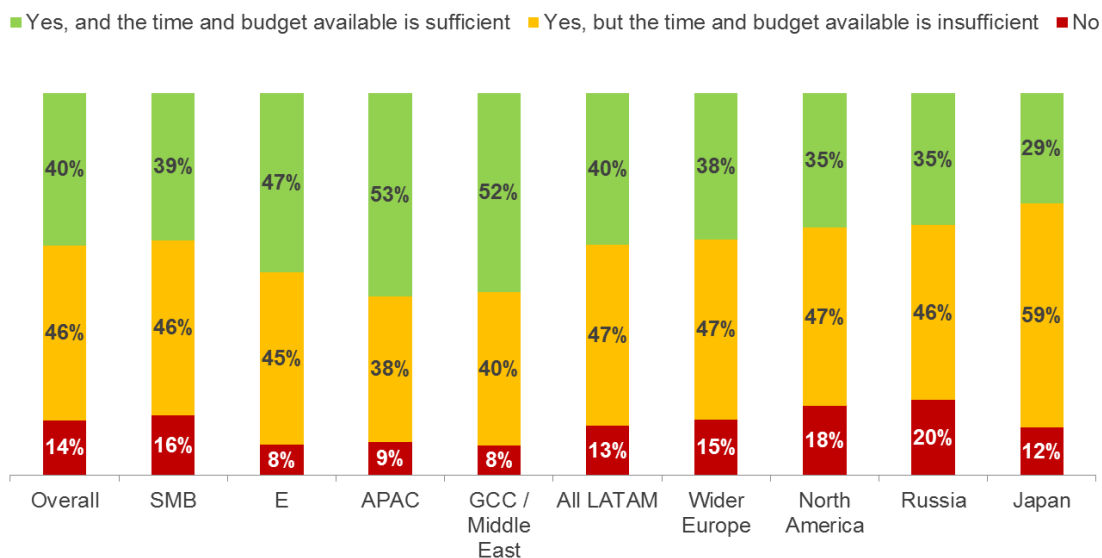
Anti-malware solutions are the most common way of securing a corporate IT infrastructure. About 71% of respondents reported that their organizations had fully deployed such systems. It is also common for companies to use tools to manage regular software updates (54%), but the proportion of such companies was 9% lower than in the previous year. Managing access rights to different parts of the IT infrastructure is another common practice, used by about 52% of the companies surveyed. About 50% of the respondents said they isolated critical parts of their IT infrastructure.

The survey also demonstrated that companies were implementing additional security measures which were either used rarely or not used at all in the previous year. Such measures included: application control (45% of companies), device control (41%), antivirus solutions for mobile devices (40%) and file-and-folder encryption (40%). The number of companies which use full-disk encryption (39%) and removable media encryption (33%) has grown by 2%. At the same time, 2% fewer companies than in 2012 used solutions for centralized management of mobile devices (Mobile Device Management) – according to the survey, the proportion of such companies was 24%.

## IT security policies

### Budget And Time Allocated To Development Of IT Security Policies

In Common With Observations About Mobile Security Policies, 3 In 5 IT Decision Makers Felt That Time And Budget Given To Developing IT Security Policies In General Is Insufficient.



Developing and implementing IT security policies is another way to provide additional protection for the company. These policies existed in 86% of the companies surveyed. However, 46% reported that they had had insufficient time and resources to develop and implement these policies.

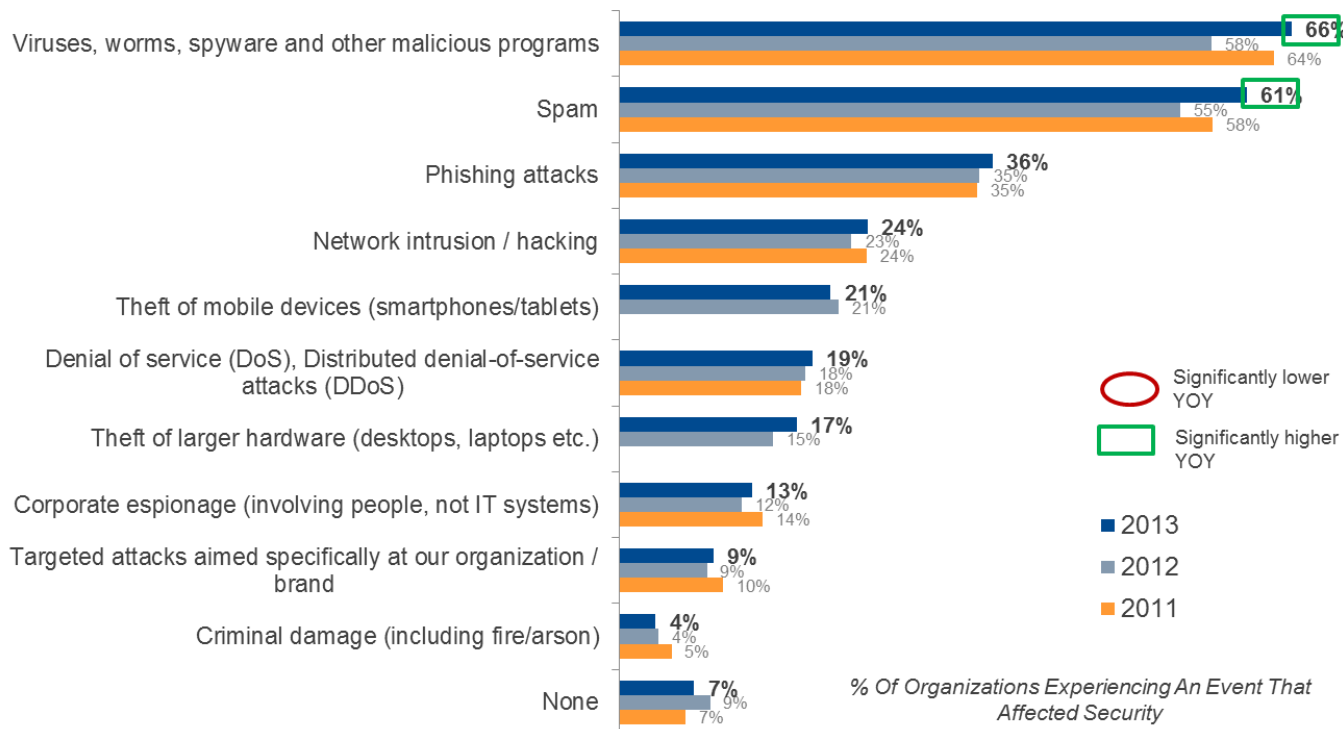
In addition to the lack of time and money, companies also reported problems with enforcement and staff attitudes towards policies. Just over half of all respondents – 52% – said that employees of their companies took IT security policies seriously and complied with them. At the same time, about 32% of the survey participants did not agree that the staff of their companies were willing to comply with the policies in place and 38% of respondents indicated that employees did not understand why specific IT security policies had been implemented in their companies.

Measures aimed at maintaining and monitoring compliance with corporate security policy most commonly include education: 60% of the respondents reported that they regularly circulated bulletins providing the latest information on threats and reminding staff of the importance of IT security policies. In addition, about 58% offered targeted training programs. Sanctions against employees who violate security policies are less widespread: their use was confirmed by 46% of respondents. Importantly, this remains unchanged even for companies that have experienced IT security related incidents.

Despite the measures taken by companies to secure themselves against cyberthreats, a large percentage of respondents reported that their organizations had been attacked.

## IT security threats experienced

### External threats

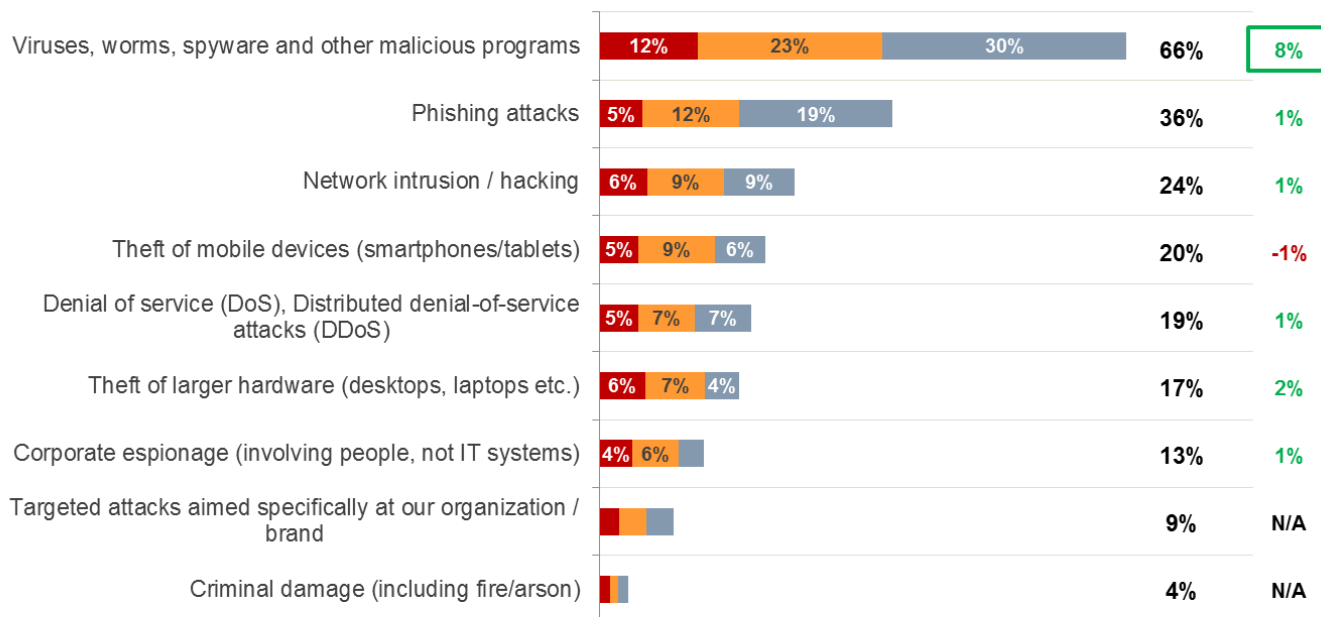


Q37. From the list below, which of the following **external** information security threats have you experienced within your organization's network in the last 12 months?

About 91% of the organizations surveyed reported that their IT infrastructure had been the object of at least one external attack in the past 12 months. Malware, spam, phishing, network intrusion and the theft of mobile devices were the five main threats faced by companies. The proportion of respondents who reported that their companies had experienced malware attacks has grown significantly from 58% to 66%. The number of victims of spam attack grew by 6 percentage points to 61%. Phishing attacks were experienced by 36% of the companies surveyed, attacks on the network infrastructure by 24%, and mobile device theft by 21%. The proportion of companies which reported theft of mobile devices did not change YOY, remaining high. As in 2012, one company in five faced this type of threat.



## External threats: data loss experienced

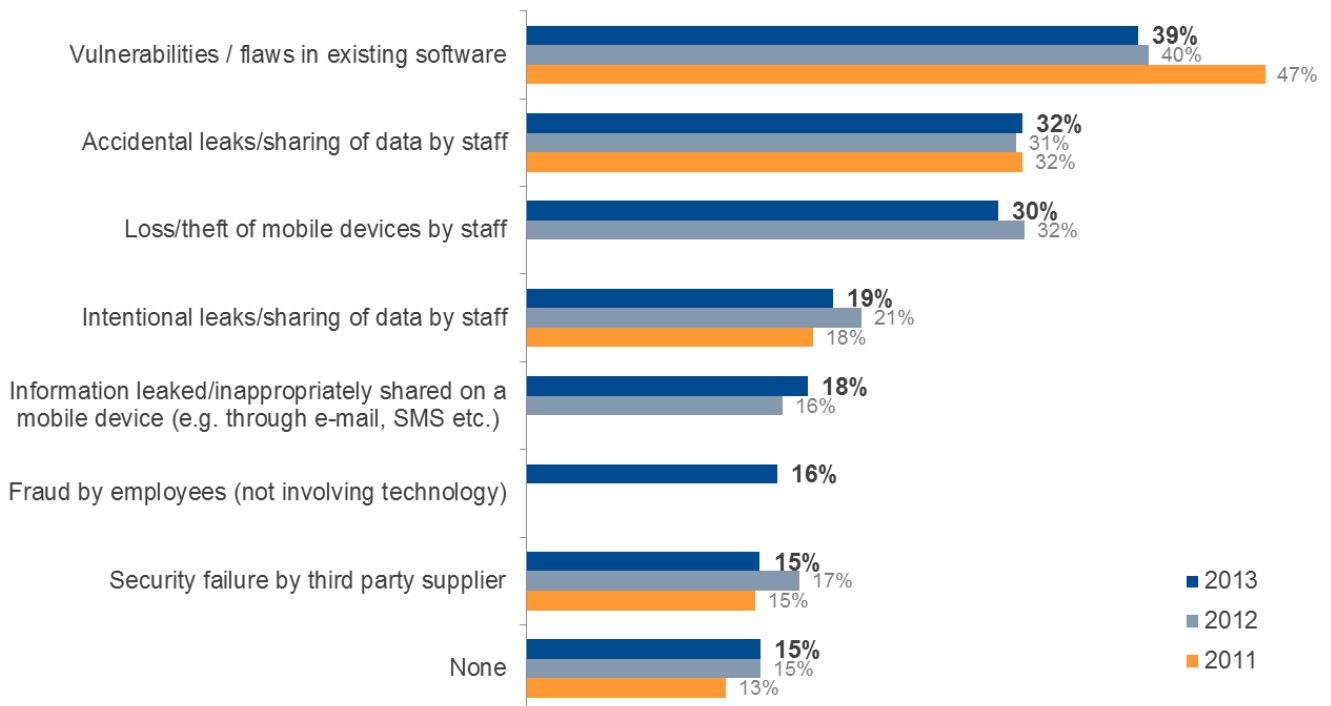


**Did data loss result?** ■ Yes - Of sensitive business data ■ Yes - Of non-sensitive business data ■ No

One of the key parameters determining the extent of the damage caused by an attack is whether the incident led to internal data being leaked. According to the survey, an average of 35% of companies experienced data leaks as a result of external attacks. In 25% of cases this involved leaks of important data, the disclosure of which could damage the business interests of the affected companies. Malware attacks caused the greatest damage: they resulted in leaks of valuable sensitive information in 12% of cases. These were followed, with 5-6%, by phishing attacks, network intrusion/hacking and theft of mobile devices. Remarkably, according to the survey results even targeted corporate espionage which does not affect IT systems causes less damage, percentagewise (4%), than cyberthreats.

## IT security threats experienced

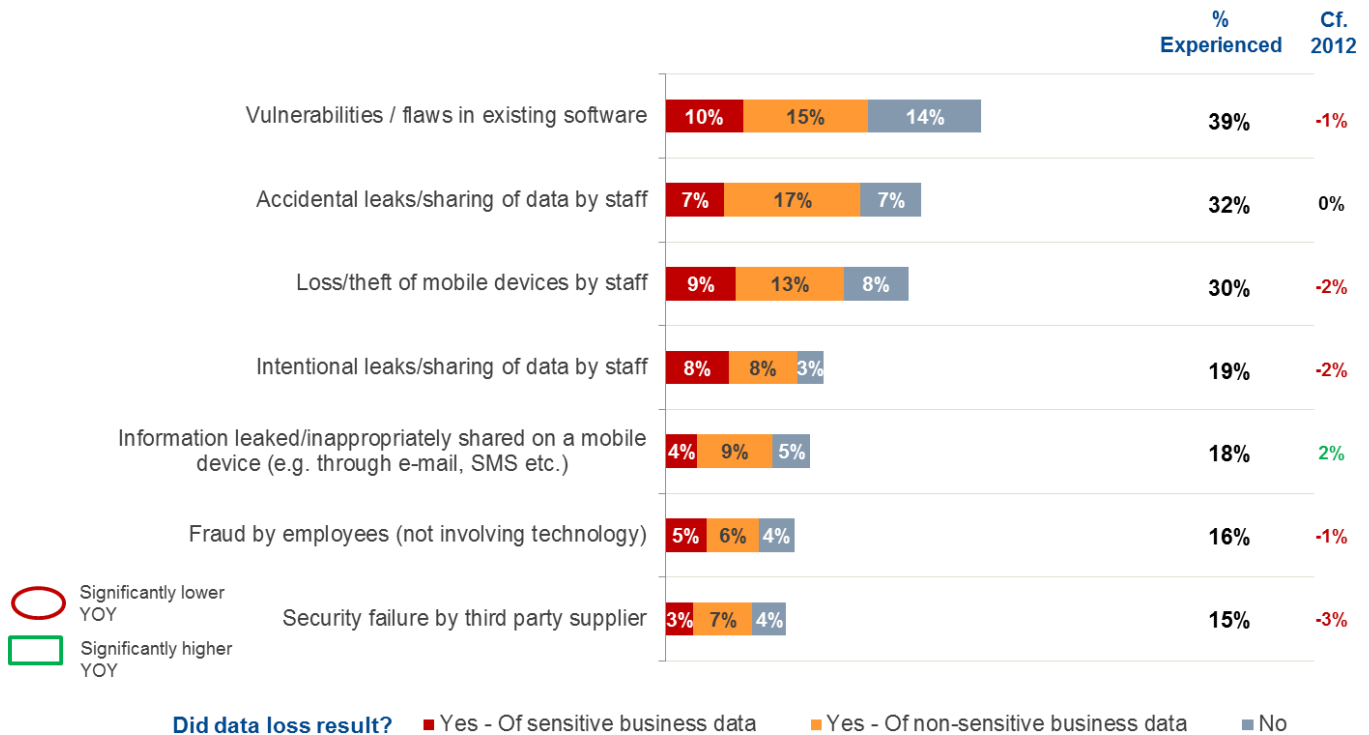
### Internal threats



Among the internal threats faced by companies in the past 12 months, vulnerabilities in the software used by the companies surveyed ranked highest. Although the proportion of such incidents has gone down significantly since 2011 – from 47% to 39% – it still remains high. Accidental data leaks by employees constitute the second most common internal threat. Incidents of this kind were reported by 32% of respondents. Slightly fewer companies – 30% – reported incidents following the loss or theft of mobile devices through the fault of employees. Leaks resulting from the misuse of mobile devices (involving mobile email clients or SMS) were reported by 19% of companies.

Remarkably, four out of the five most common internal security incidents reported by companies involved actions by employees using mobile devices.

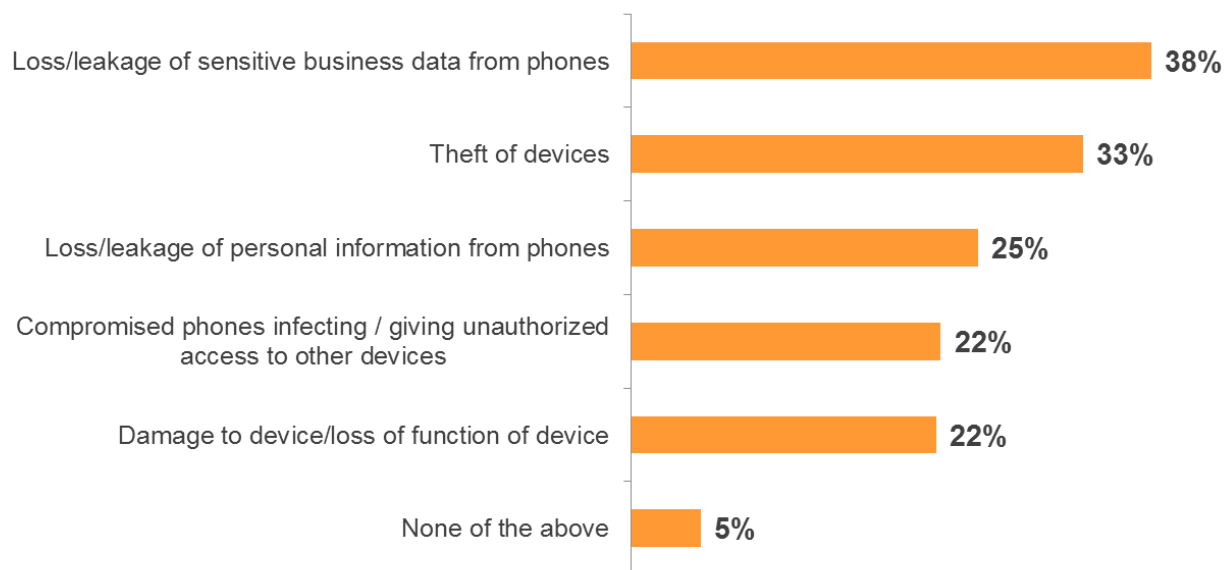
## Internal threats: data loss experienced



On average, 24% of companies had leaks of business data due to internal security incidents. In 6.5% of cases, valuable data was leaked. Leaks of important business data were most often due to unclosed vulnerabilities in the software used by companies – 10% of respondents reported such incidents.

Loss or theft of mobile devices was the second most dangerous type of internal incident. In 9% of cases these incidents resulted in the loss of confidential internal company data. Overall, internal incidents involving employee actions and the use of mobile devices were the second most harmful for companies, after software vulnerabilities.

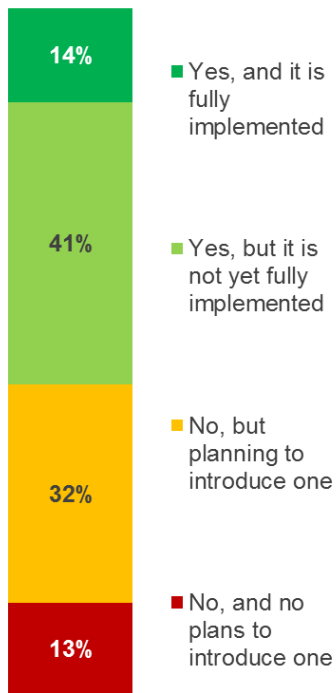
## Mobile phones: one big threat



Incidents involving the misuse of mobile devices, particularly mobile phones, were among the most dangerous threats – both external and internal. The Bring Your Own Device trend, which means that company employees are increasingly using smartphones and tablets at work, has evolved significantly. However, this affects security to such an extent that mobile devices now form a separate class of threats with its own subcategories. Thus, 95% of respondents reported that at least one mobile device-related security incident had been recorded in their company in the past 12 months. In 38% of cases mobile devices were involved in leaks of important corporate data. About 33% of cases were linked to the theft of mobile phones, which can also lead to data leaks. In 25% of incidents, employees' personal data was leaked; in 22% of cases a compromised smartphone provided access to other corporate devices. Mobile threats are forcing companies to implement additional security policies for mobile devices. However, this is not yet happening in all organizations.

## IT security policies for mobile devices

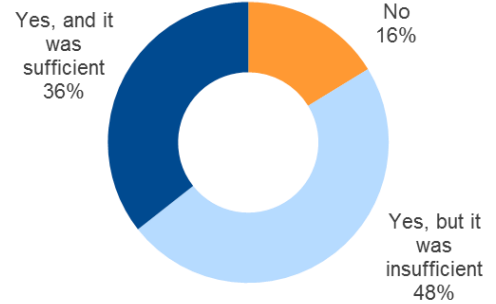
### IT Security For Mobile Devices:



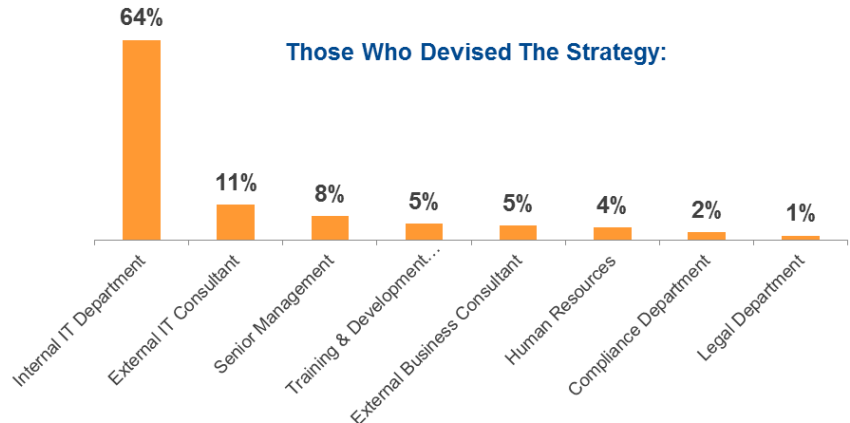
Those somewhat or fully implemented:



### Was There An Increase In Budget?



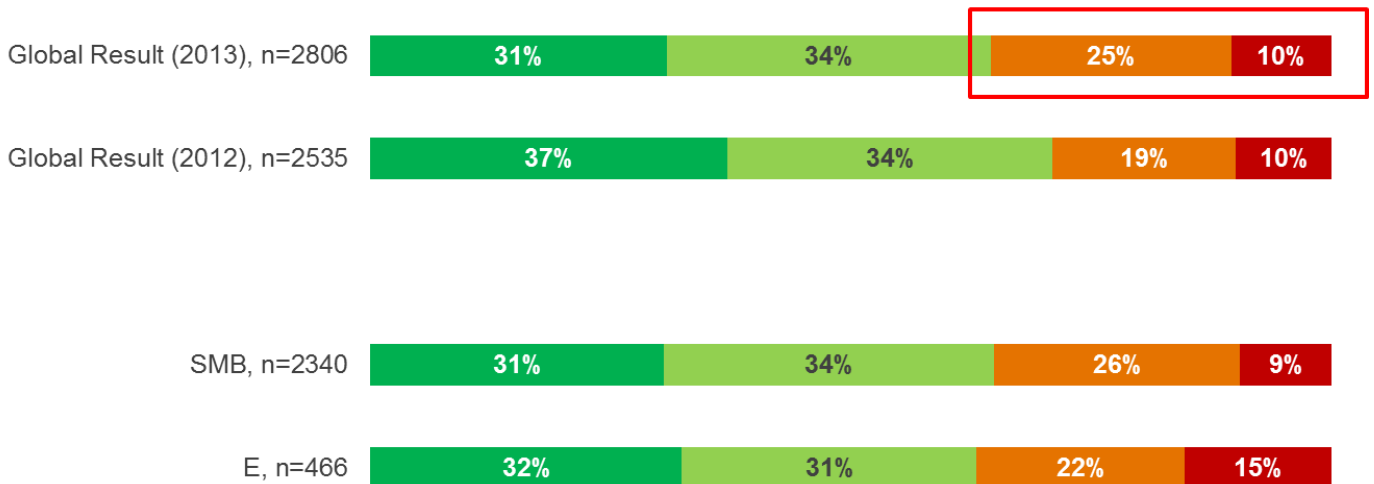
### Those Who Devised The Strategy:



Implementing IT security policies for mobile devices (such as internal corporate directives regulating the use of such devices) could significantly reduce the risks posed by smartphones and tablets in a corporate IT environment. On the whole, most of the companies which took part in the survey demonstrated that they realize this: 55% of respondents stated that IT security policies were implemented and applied in their companies to a greater or lesser degree. Another 32% of respondents reported they did not have such policies in place, but were planning to implement them in the future. At the same time, almost half (48%) of those who said they had security policies for mobile devices added that the budget increases provided in order to implement such policies had not been sufficient and another 16% stated that no extra budget had been available at all.

## BYOD policy into the future

- We will actively allow more users to bring their own device for work purposes
- Whatever we do, there will be an inevitable increase in user-bought devices in the workplace.
- We will try to limit the number and type of users that can bring their own device
- We will enforce a strict prohibition on users bringing their own device for work purposes



Most survey participants recognized the so-called Bring Your Own Device trend, which involves corporate employees using their personal mobile devices (smartphones and tablets) in their work, as an inevitable phenomenon. Only 10% of respondents stated that they would step up measures to ban personal devices in the workplace. At the same time, 31% did not plan to restrict the use of personal devices by the staff. Over a third of respondents (34%) had simply resigned themselves to the trend, noting that prohibition would have little impact on the number of personal devices used by their companies' employees.

At the same time, most respondents – 65% – identified BYOD as a threat for their business. The level of concern was particularly high in Japan, where 93% of respondents expressed apprehension. Representatives of Russian companies were the least concerned about the issue, although those concerned still made up more than half of the respondents (57%).

## Most serious data loss incidents: external + internal + mobile



The overall ranking of threats which caused leaks of important data is revealing: malware attacks, as well as a range of internal incidents caused by inappropriate staff behavior and improper use of mobile devices were the main sources of damage suffered by companies as a result of security breaches of their IT infrastructure. This financial damage can be evaluated.

## Consequences & costs of IT security breaches: from \$50k to \$649k per incident on average

In 2013, B2B International and Kaspersky Lab added a new section to the Global Corporate IT Security Risks survey, asking respondents to assess the financial damage suffered by their companies due to IT security incidents. The result was that, by the most conservative estimates, the average damage suffered by large companies from a single serious incident was **\$649,000**. For small and medium-sized companies, the average damage was **\$50,000**.

A small handful of smaller companies reported **lost business** in the region of 5% of their annual revenue.

It is worth noting that financial costs varied significantly depending on attack type. For example, for a large company a successful DDoS attack could cause **\$527,000** in damages. That figure rose to **\$2.4 million** for a successful targeted attack.


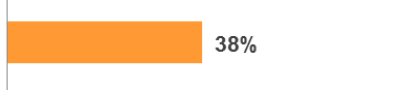
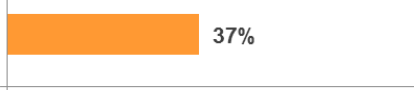
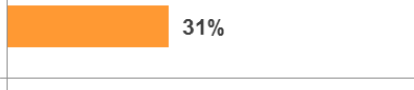
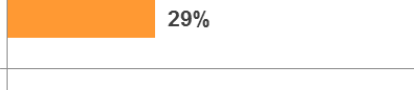
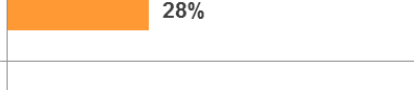

### *Important disclaimer: How estimates were performed*

- ▶ Companies which reported in the survey that they had experienced data leaks (regardless of whether the data leaked was valuable or not) were then asked to assess the damage caused by these incidents;
- ▶ When calculating the final amount, only those leaks which had taken place in the past 12 months were included;
- ▶ Companies were asked questions about additional costs related to mitigating the consequences of an incident and preventing such incidents in the future, as well as other procedures arising from the data leak;
- ▶ Companies which were prepared to discuss damage from cyberattacks were asked to evaluate their own financial damage from such incidents.
- ▶ Using data received from these companies, researchers from B2B International assessed the overall financial damage that IT security incidents could cause, as well as damage by attack type, company size, region in which a company operates and a number of other parameters.



## How the costs add up...

### Additional professional services

		No Additional Cost	A Small Additional Cost	A Large Additional Cost	Long Term/ On-going Cost
IT Security Consultants	 66%	15%	43%	28%	12%
Risk Management Consultants	 38%	11%	41%	32%	14%
Lawyers/Solicitors	 37%	17%	42%	29%	10%
Auditors/Accountants	 31%	20%	44%	25%	9%
Physical Security Consultants	 29%	16%	40%	29%	13%
Management Consultants	 28%	19%	39%	25%	13%
PR/Corporate Image Consultants	 20%	16%	35%	33%	14%

About 87% of incidents involving leaks of valuable corporate data made it necessary for companies to use additional professional services, including IT consultants, risk management experts, lawyers, physical security consultants and public-relations specialists. In 47% of cases, companies described additional costs related to these specialist services as significant.

On average, the overall cost of using additional services amounted to \$13,000 for small and medium-sized companies and \$109,000 for large corporations. At the same time, in a small number of individual cases, small and medium-sized companies had to spend up to \$350,000 and large corporations up to \$7.5 million.

## Damage to business function & reputation

Impact among those reporting each event...

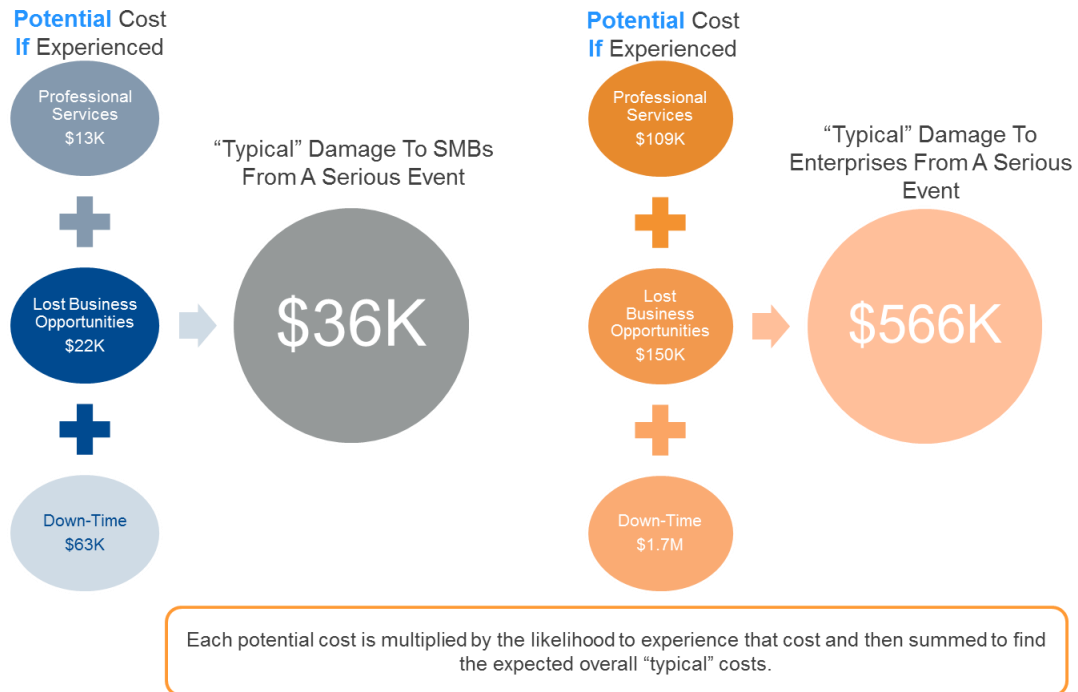
		Very Short Term	Short Term	Significant	Extended
Temporary Loss Of Access To Business Critical Information	51%	19%	42%	31%	7%
Temporary Loss Of Ability To Trade	29%	18%	42%	30%	9%
		Minor & Short Term	Minor But Lasting	Serious But Short Term	Serious & Lasting
Loss Of Contracts / Business Opportunities	29%	24%	29%	35%	11%
Loss Of Credibility / Damage To Company Reputation	27%	25%	30%	33%	12%
Increased Insurance Premiums	21%	23%	44%	25%	7%
Damage To Credit Rating	17%	22%	36%	34%	8%

In 60% of cases, data leaks caused significant disruption to business operations; 53% of incidents resulted in significant damage to the affected company's reputation. In almost a third (29%) of all cases, an incident resulted in the loss of important business contacts and missed business opportunities.

Opportunities missed by businesses were evaluated in terms of financial damage, which, on average, amounted to \$22,000 for small and medium-sized companies and about \$150,000 for large corporations.

Although IT security incidents by no means always resulted in the loss of ability to operate (only a quarter of large companies surveyed reported such difficulties), the damage from such consequences can be substantial – up to \$63,000 for medium-sized and small businesses and up to \$1.7 million for large corporations.

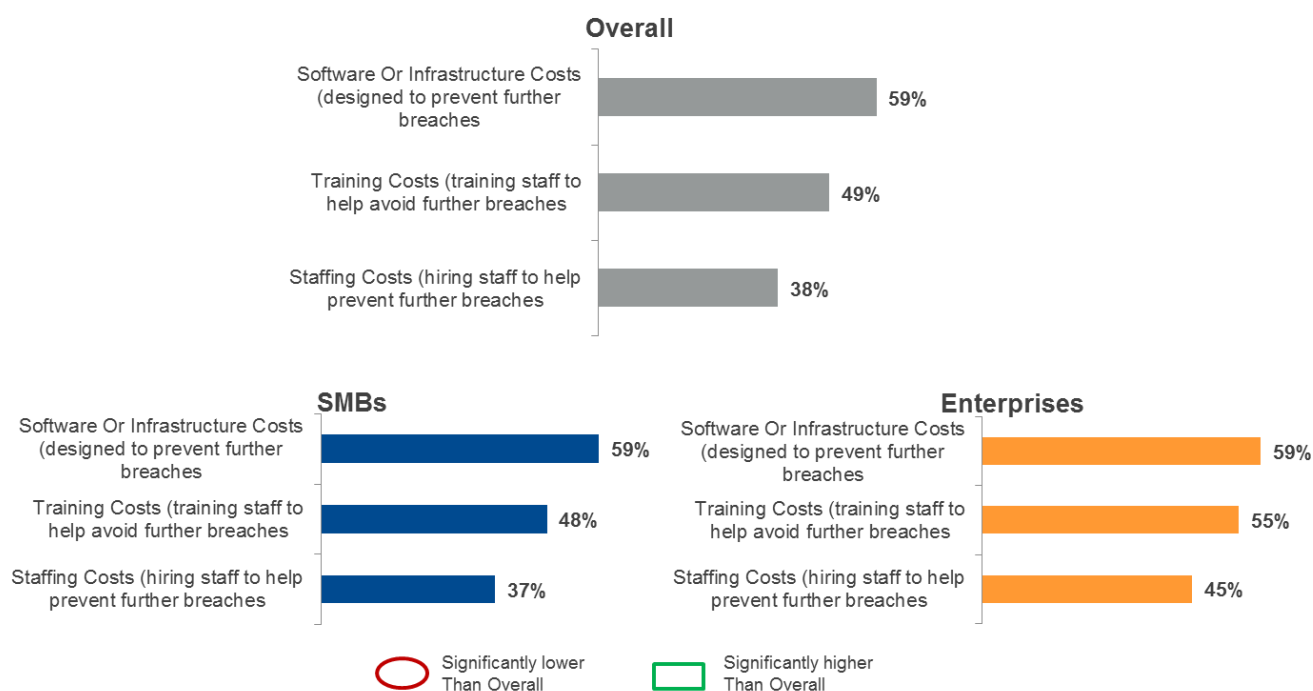
## Estimated financial damage resulting from any serious data loss incident



The average 'typical' damage suffered as a result of a cybersecurity incident was \$36,000 for medium-sized and small companies and \$566,000 for large organizations. It should be noted that the above calculations took into account the probability of different consequences of an incident taking place; they also included smaller additional costs. At the same time, these estimates did not account for relatively rare consequences of incidents – such as a company being forced to offer a minimal service in the wake of an attack.

The above numbers are some way short of the final costs. In addition to expenses directly related to an incident, companies had to spend money on a number of reactive measures, including attempts to minimize the chances of similar incidents happening in the future.

## Actions taken to prevent further breaches

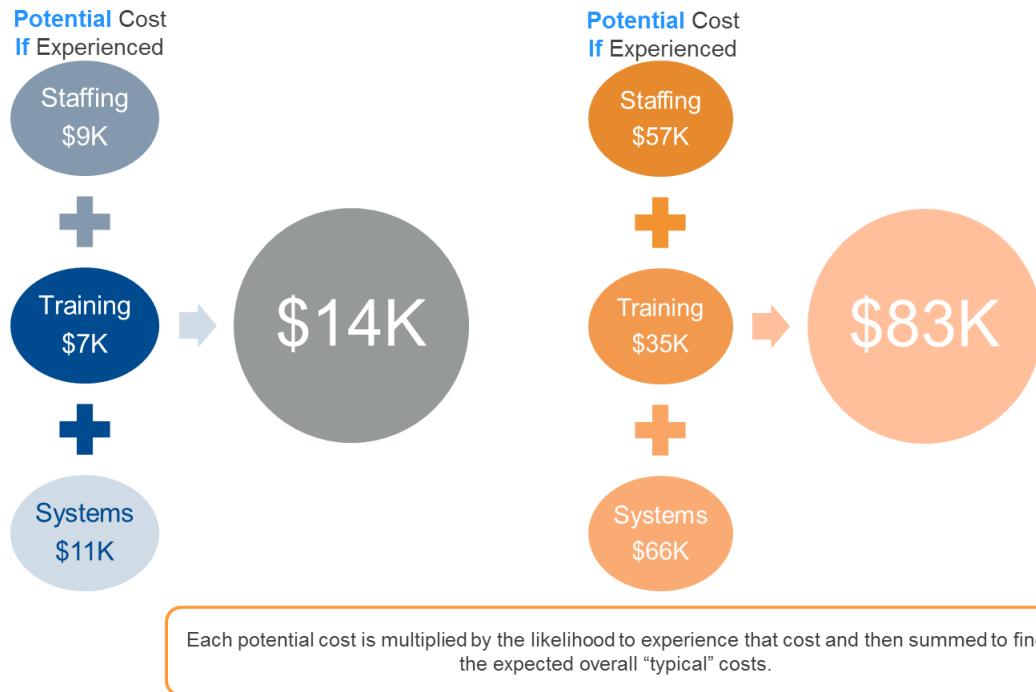


The most common measure aimed at preventing future IT-security incidents was deploying additional software and hardware solutions to protect the IT infrastructure – on average, 59% of companies turned to these measures. Additionally, large corporations invested considerable amounts of money into hiring new staff to maintain IT security and into training existing employees in methods of incident prevention.

On average, recruiting additional staff to maintain IT security cost small and medium-sized organizations \$9,000 and large corporations \$57,000. Training set large companies back about \$35,000, and for small and medium-sized companies the cost was about \$7,000.

Large companies spent about \$66,000 on improvements to the hardware and software parts of their IT infrastructure; small and medium-sized businesses spent about \$11,000.

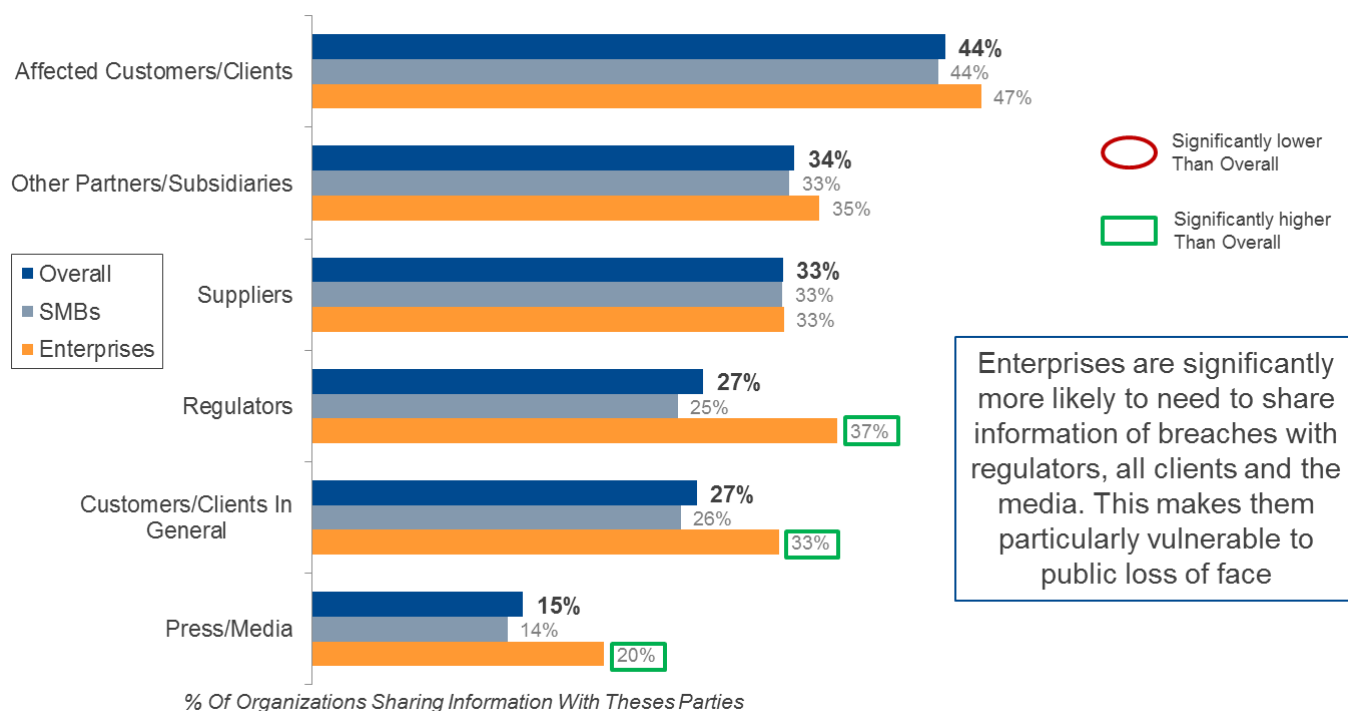
## Estimated reactive spend on breach prevention



As in the case of evaluating direct damage from an incident, estimates of overall reactive costs did not include expenses that were not typical of the majority of companies. For example, if the underlying cause of an incident was employee negligence, it is quite possible that there was no need to upgrade equipment or software. However, regardless of the nature of specific incidents, companies will find it hard to avoid investing in staff recruitment and training, since most successful attacks were the result of oversight or lack of expertise on the part of employees. These were the expenses that made up the estimate of average 'reactive' expenses aimed at preventing incidents in the future. For small and medium-sized businesses, this figure amounted to \$14,000, for large companies it was \$83,000.

Notably, cybersecurity incidents not only inflict financial damage, but could also deal a serious blow to a company's reputation.

## Spread of knowledge of security breach



A leak of sensitive data often means that the affected company must publicly disclose information about the incident. About 73% of respondents stated that they had to distribute information about an incident because a third party had demanded that they do so. A disclosure was most often (in 47% of cases) demanded by customers of large corporations who might be affected by the leak. In the event of an incident, a large corporation would probably have to report it to the regulator, its customers and the press, which would obviously be detrimental to its business reputation.

## Average impact of data security breaches by region

Estimated Average For SMBs	Overall	North America	Wider Europe	Russia	APAC	All LATAM
<b>Base</b>	<b>1,368</b>	<b>108</b>	<b>459</b>	<b>184</b>	<b>216</b>	<b>61</b>
Total Expected Damages	36K	59K	38K	14K	74K	35K
Total Reactive Spend	14K	23K	17K	7K	22K	10K
Overall Financial Impact	50K	82K	55K	21K	96K	45K

Estimated Average For Enterprises	Overall	North America	Wider Europe	Russia	APAC	All LATAM
<b>Base</b>	<b>271</b>	<b>45</b>	<b>67</b>	<b>26</b>	<b>61</b>	<b>21</b>
Total Expected Damages	566k	721K	569K	695K	558K	761K
Total Reactive Spend	83K	97K	58K	57K	164K	52K
Overall Financial Impact	649K	818K	627K	752K	722K	813K



Significantly lower



Significantly higher

The amount of financial damage suffered by a company as a result of a cybersecurity incident varied significantly depending on the region in which the company operates. For large corporations the most 'expensive' regions in this respect were North America and Latin America, where costs could reach \$818,000 and \$813,000 respectively. The situation was different for medium-sized and small companies: companies from the Asia-Pacific region lost the most money – \$96,000 – in an average incident.

## Average impact of data security breaches by type

Estimated Average For SMBs	Overall	Targeted Attacks	Network Intrusion	Fraud/Deliberate Leaking	Phishing	Exploits	DoS/DDoS
<b>Base</b>	<b>1,368</b>	<b>22</b>	<b>98</b>	<b>151</b>	<b>71</b>	<b>150</b>	<b>54</b>
Total Expected Damages	\$36K	\$72K	\$51K	\$34K	\$21K	\$46K	\$41K
Total Reactive Spend	\$14K	\$20K	\$22K	\$17K	\$16K	\$15K	\$18K
Overall Financial Impact	\$50K	\$92K	\$73K	\$51K	\$37K	\$61K	\$58K

Estimated Average For Enterprises	Overall	Targeted Attacks	Network Intrusion	Fraud/Deliberate Leaking	Phishing	Exploits	DoS/DDoS
<b>Base</b>	<b>271</b>	<b>6</b>	<b>22</b>	<b>29</b>	<b>17</b>	<b>28</b>	<b>16</b>
Total Expected Damages	\$566k	\$2.17M	\$1.44M	\$884K	\$660K	\$506K	\$407K
Total Reactive Spend	\$83K	\$224K	\$231K	\$100K	\$198K	\$155K	\$120K
Overall Financial Impact	\$649K	\$2.40M	\$1.67M	\$984K	\$858K	\$661K	\$527K

 Significantly lower
  Significantly higher

Small bases and heavy influence from factors such as size, revenue and knowledge levels mean that it is harder to assess the relative severity of types of security breach for enterprises

The amount of damage that could be suffered by a company as a result of an IT security incident was also affected by the type of attack which caused the incident. Both for large companies and for those in the small and medium-sized business segment, targeted attacks were the most 'expensive'. Large corporations could lose up to \$2.4 million due to an incident of this kind, medium-sized and small companies faced costs of up to \$92,000. Penetration of the network infrastructure by hackers was also an extremely expensive type of attack – an average of \$1.67 million for large corporations and \$73,000 for small and medium-sized businesses.

Overall, it is obvious that successful cyberattacks can inflict real financial damage even to small companies. B2B International researchers tried to make their damage assessments as conservative as possible, which means that the actual amounts of financial damage may have been much more substantial.



## Conclusion and Recommendations

---

Although the majority of companies are as yet unable to assess the actual scope of cyberthreats, on the whole businesses realize the importance of effective protection. Malware, together with a broad range of attack scenarios involving company employees and their personal mobile devices, have become the main source of incidents in which companies lost valuable business data.

The loss of that data could result in real financial costs which might reach millions of dollars for a single incident, not counting reputation damage, which is difficult to assess in financial terms.

Bring Your Own Device is a major technology-related concept, which has already seen significant evolution. Its influence on security will only increase in the future. Most companies already recognize BYOD as one of the main threats to data security. However, only a relatively small proportion of companies are currently prepared to respond to this threat with well-designed and effective mobile device security policies and dedicated solutions to protect and manage these devices.

Based on the survey results, Kaspersky Lab offers the following recommendations, which could significantly increase the level of IT security in any organization.

### **Investment in security**

IT security incidents can cause real financial and reputation damage. These losses can significantly exceed the cost of putting in place IT security tools which would help to avoid leaks of important data, downtime and other unplanned expenses. This is why it is important to invest in the security of the corporate IT infrastructure.

### **Professional protection and management**

It is impossible to cope with the constantly growing number and variety of malicious programs without dedicated tools. Entire groups of cybercriminals are involved in creating and distributing viruses, Trojans and spyware. These people are prepared to invest large amounts of money into developing this dangerous software. Cybercriminals increasingly use vulnerabilities in popular software to infect corporate computers. This means that it is impossible to ensure the required level of security without an effective system which provides software updating and management of the corporate workstations on which this software runs. It is equally impossible to ensure protection without a high-quality anti-malware solution.

### **Controlling BYOD is important**

The regular use of personal mobile devices by employees in their day-to-day work is already commonplace. However, the fact that this situation has become widespread does not make the threats that it brings with it any less dangerous. This means that if a company allows the use of personal devices for work, it needs to use professional solutions to manage these personal devices and protect them against malware.

### **Policies and training**

The development, implementation and systematic enforcement of IT security policies in a company will make a significant contribution to its overall security. Importantly, employees, who very often become the actual sources or agents of serious data leaks, fail to comply with or accidentally violate security policies. This is why it is crucial to focus on informing and training staff in the area of cyberthreats and ways of combating them.

### **Integrated approach**

The variety of security threats to the corporate IT infrastructure is so great that there is no single commercial solution capable of resolving all corporate IT security issues once and for all. Using advanced software to protect and manage the corporate IT infrastructure will make an enormous contribution to enhancing the company's security. However, to safeguard the company against all IT threats, adequate attention should be paid to all aspects of the

---

issue: be aware of changes in the area of threats and the latest protection against them, competently select and implement the necessary hardware and software, maintain a high level of employee awareness, and not just among staff whose work is IT-related. Applied together, these measures will provide the company with truly reliable protection.