KASPERSKY lab

IT SECURITY RISKS SURVEY 2014: A BUSINESS APPROACH TO MANAGING DATA SECURITY THREATS

Table of contents

Introduction

It is difficult to imagine a modern, competitive company without a reliable IT infrastructure. These days, it's a critical component for the success of any commercial organization. Yet typically, as the significance of IT components grows in daily business processes, so do the risks associated with day-to-day functions, as does the probability that one day, an internal or external factor will upset a corporation's IT services, ultimately leading to business interruptions. Another key risk associated with a company's IT infrastructure is the risk of losing confidential data.

The efforts of the IT security development industry as a whole are, at the corporate level, aimed at achieving the maximum level of protection against those types of situations. As a leader on the corporate security software development market and a provider of a variety of professional services in the field of data security, Kaspersky Lab keeps abreast of the changes affecting data security risks posing a threat to business. Kaspersky Lab also knows how to meet companies' needs when it comes to protecting corporate IT infrastructures and confidential data against cyber attacks.

In order to understand the resources that a business needs, how it perceives the state of the security of its own IT infrastructure, and how these correlate to the actual state of affairs in the world of cyber threats, Kaspersky Lab works with other prominent international analysis agencies to conduct regular surveys among the representatives of thousands of companies around the world. These surveys have been conducted every year since 2011.

In 2014, Kaspersky Lab collaborated with B2B International to conduct the fourth annual survey. The resultant data conveys the opinions of the surveyed companies on the most relevant IT infrastructure security matters within their companies, and illustrates the changes that have taken place since the three previous studies. Comparing new data with that of prior years' helps identify key trends in the area of study and to better describe those trends, which in the end give the fullest possible picture — and the most objective, in our opinion — of the threats, problems, and future trends in business data security.

In 2014, Kaspersky Lab and B2B International also conducted three additional subject-specific surveys on counteracting financial fraud on the Internet, DDOS attacks, and the secure use of virtualization resources.

Key figures

According to the survey results, the following trends constitute today's key data security threats and their countermeasures:

- Spam is external threat No. 1 and was named by 64% of respondents. Previously 66% of respondents had named malware attacks as number one. Based on the 2014 survey, viruses, worms, Trojans, and other types of malware were problems for 61% of respondents.

- Some 94% of companies encountered cyber security issues, the sources of which were outside the perimeter of the company — that's 3 percentage points higher than in 2013.

- About 12% of companies had run-ins with targeted attacks. In 2013, this percentage did not exceed 9%.

- The protection of confidential data against leakages is now the top priority for most of the companies (38%) surveyed.

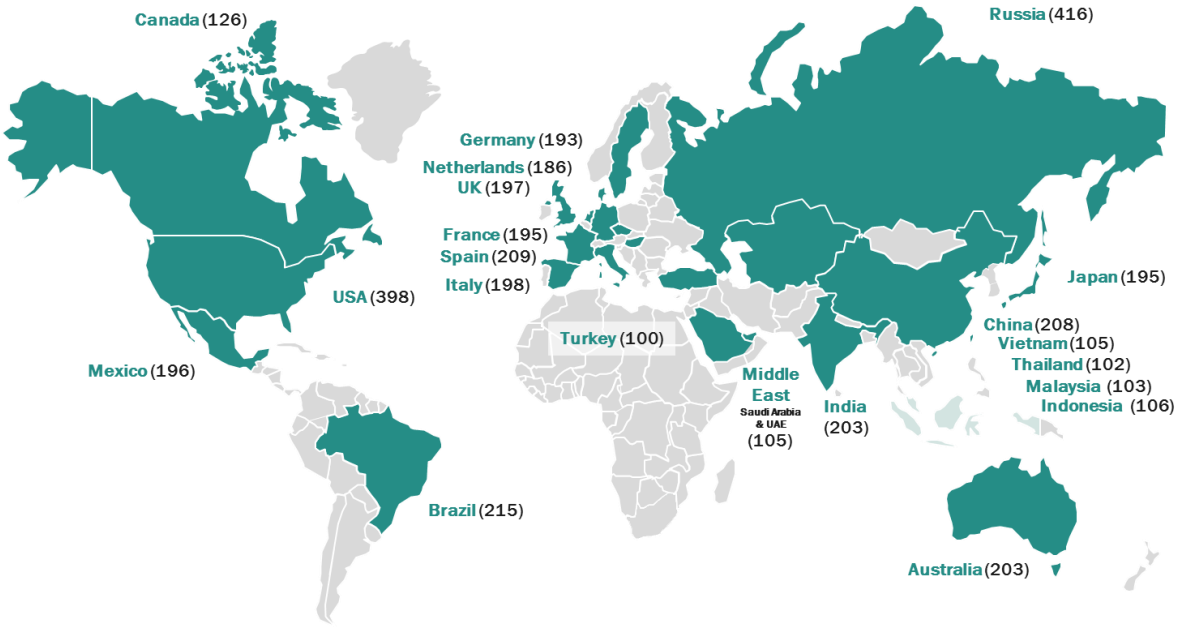
- Damages from one data security incident were estimated at an average of $720,000.

- Damages from one successful targeted attack could cost a company as much as $2.54 million.

- Most often, a company that finds itself on the receiving end of cyber-security incidents loses data about their internal operations (43%), client data (31%), and financial data (22%).

The factors affecting the survey results and the changes in responses from the 2013 are addressed in more detail below.

Methodology



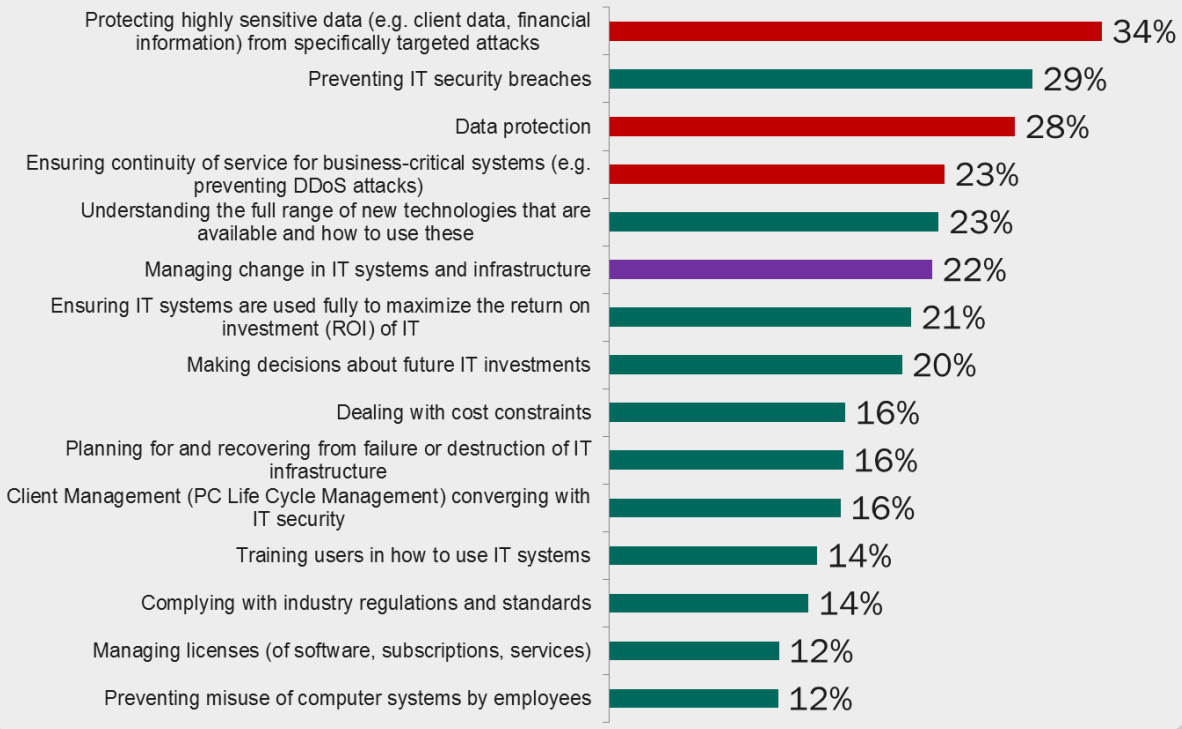
A total of 3,900 respondents from 27 countries — representatives of companies of all sizes — took part in this year's survey. Compared to the previous year, the survey grew both in total size and global scope (the 2013 survey included 2,900 respondents in 24 countries). Over 54% of the participants were mid-sized, large, and very large companies. Approximately 17% of the respondents were corporations in the Large Enterprise segment (with anywhere from 5,000 - 50,000 employees), while 12% of the survey participants fit into the Large-Medium category (1,500 to 5,000 employees). About 25% of the survey participants were companies with anywhere from 250 to 1,500 employees, and the remaining respondents represented small and very small businesses.

All of the companies that took part in the survey answered dozens of questions concerning the main obstacles that both the company's general management and IT management face, specifically when building and maintaining a reliable, smooth-running IT infrastructure. Additionally, respondents also answered questions about the resources allocated by their companies for tackling IT problems, including data security problems. The survey questions asked respondents about business conditions within a period of the previous 12 months, from April 2013 through May 2014.

Concerns and priorities of IT managers: data comes first

The protection of confidential data (client data, financial data, and other kinds of information) against targeted attacks is a key problem for the IT management teams of over one-third of all of the companies surveyed (34%).

TOP CONCERNS OF THE IT FUNCTION



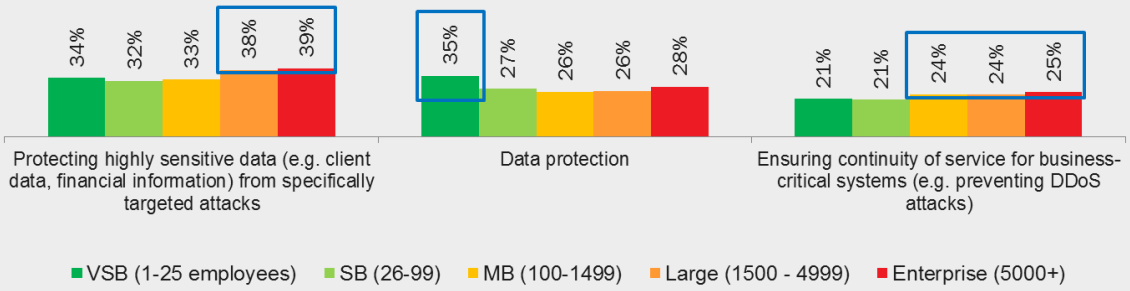
Remarkably, during the last survey period, targeted attacks were not named among the top IT-related problems. Respondents began to name this type of threat only when the subject matter addressed a narrower segment of IT, namely data security. This year it was different – protection against targeted attacks outranked more "general" issues of data security breach prevention (29%) and data security (28%).

Some recent examples of major targeted attacks in the headlines last year could be one reason for heightened attention of IT management teams when it comes to specific tasks. For example, over the survey period, Kaspersky Lab discovered three major cyber espionage campaigns designed to steal secret data from corporations and government organizations around the world. The attack launched by cybercriminals against the major retailer Target serves as an example of just how destructive a targeted cyber attack can be — malicious users got their hands on the personal data of roughly 70 million clients of the store. Large companies in particular see targeted attacks as a major threat, with 38% of companies with 1,500 – 5,000 employees, and 39% of companies with over 50,000 employees naming targeted attacks as

their number one concern. Mid-sized and small businesses were less worried about targeted attacks; no more than 34% of the respondents in this size category named protection against targeted attacks as a key priority.

Some 23% of respondents also named DDoS attacks as a key threat to the wellbeing of their business's IT infrastructure.

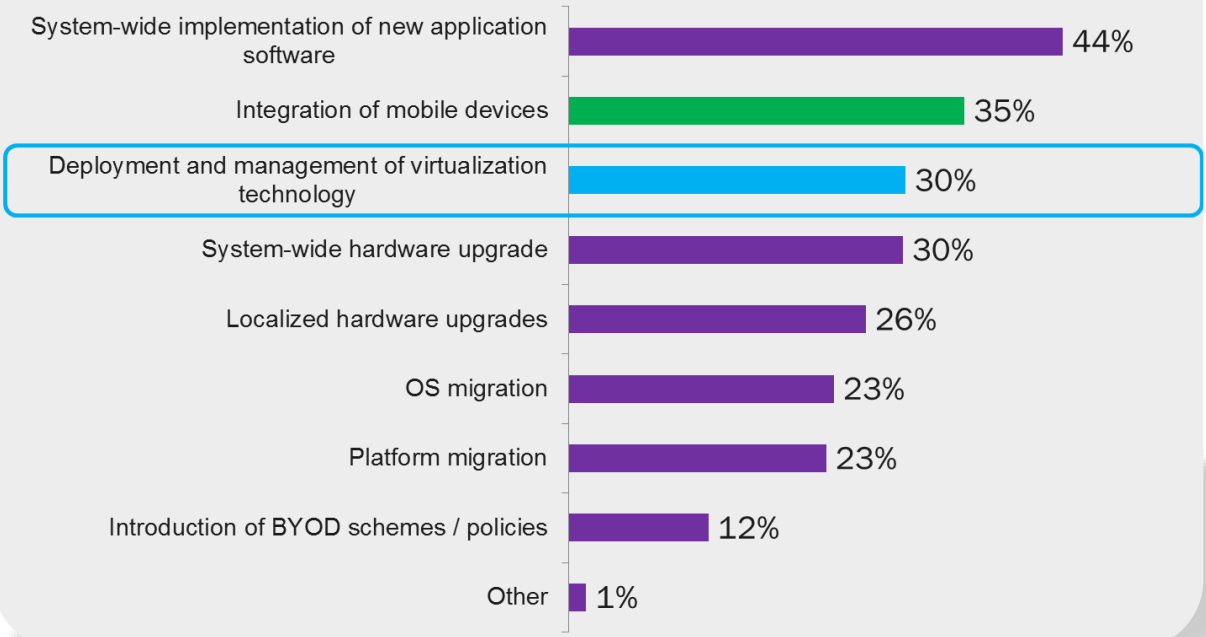
LOOKING AT DATA PROTECTION AND BUSINESS CONTINUITY IN MORE DETAIL…



The IT infrastructure management task named as most critical is centralized software updates (44%). Compared with the results of the previous survey (49%), this is still the most important problem, but for a smaller proportion of companies. Meanwhile, many more respondents named mobile device integration with the corporate IT environment — 35% in 2014, compared to 30% in 2013.

A "newcomer" among the most important tasks was also noted: the development of virtual servers and workstations — 30% of those surveyed reported prioritizing this task. Companies are doing their best to streamline expenses for expanding and maintaining their IT infrastructures, leading more companies to choose virtualization-based software solutions. However, along with the advantages of virtualization, there are also some challenges related to rolling it out, managing virtual IT, and keeping it secure. The companies that named this as a top concern are located in China (53%), Russia (46%), countries with developing markets (36%), and countries in the Middle East (31%).

MANAGING CHANGE IN IT SYSTEMS



The top IT security priorities named by companies for 2014 include preventing data leaks (28%), maintaining the fail-safe operation of critical IT systems (27%), and maintaining the security of mobile devices (24%). Incidentally, companies in the VSB segment are especially concerned about mobile security, with 31% of respondents in that field reporting that their organization will be working on this issue this year. Another 31% of small business representatives are also taking measures to secure their companies' workstations against malicious programs. At the same time, fewer survey respondents (24%) named protection against malware as the main task in data security efforts.

Just 14% of those surveyed stated that they plan to undertake virtual IT data security over the next 12 months. Meanwhile, one out of every five companies (21%) with 5,000 or more employees are seriously looking into plans for maintaining secure virtual servers and workstations to protect them against cyber attacks in the year ahead.

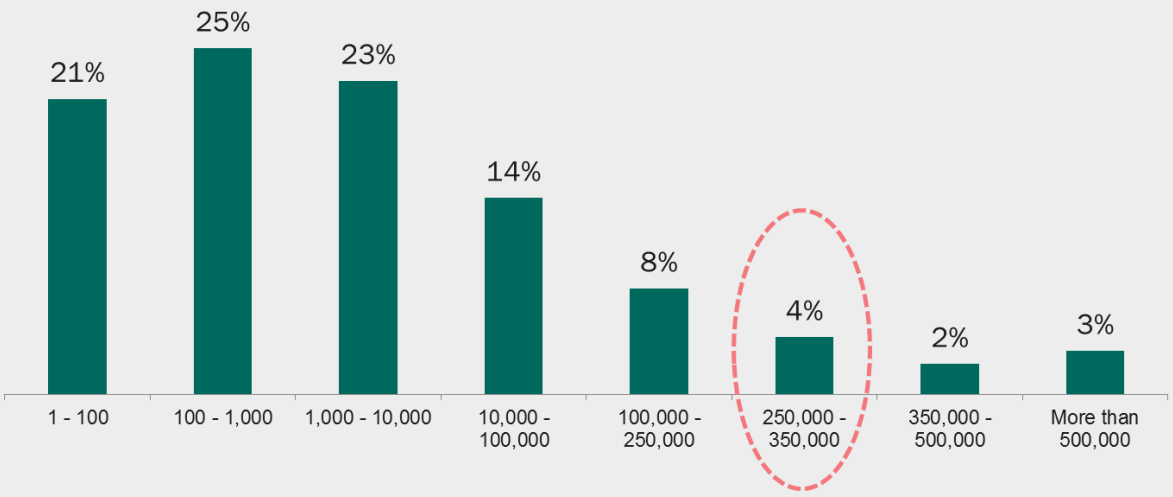
It stands to reason that when making decisions about which actions to take to maintain data security within a company's own IT infrastructure and to protect confidential data, a company will make every effort to mitigate risks — including those risks that it encountered in the past.

Data security risks: incidents and responses

An understanding of the risk level posed by cyber threats is one indicator of just how prepared a company is to effectively counteract the potential impact of a cyber attack. While it remains a relative factor, being well informed of the developments in the world of cyber threats is still a significant marker of that understanding. In order to better convey the level of awareness of cyber threats, for the second year in a row Kaspersky Lab and B2B International asked respondents to assess the number of new malicious programs emerging on a daily basis.

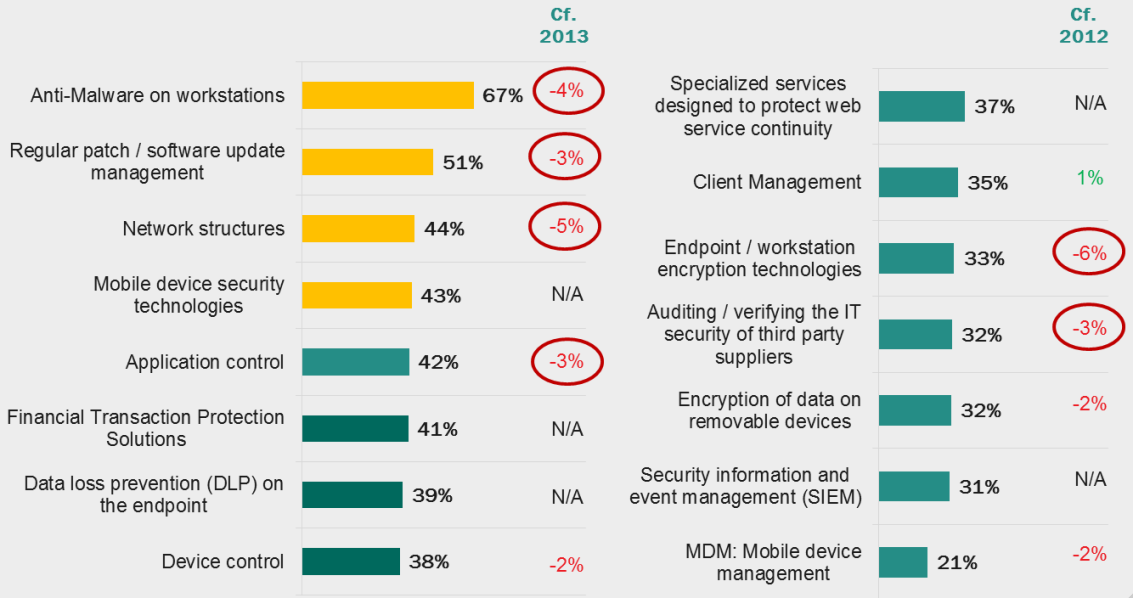
According to Kaspersky Lab's data, in 2013, company experts detected an average of 315,000 new variants of malicious programs daily. Based on the survey results, only 4% of respondents named a figure comparable to that of Kaspersky Lab estimates, while over 91% of those surveyed grossly underestimated that number. Incidentally, the awareness level in the 2013 survey was notably higher at 6%.

PERCEPTION OF DAILY MALWARE DISCOVERY RATES



The perception of the threat level naturally affects the measures taken by a company to ensure protection against cyber threats. For example, 67% of respondents reported that security software was installed on their companies' workstations. This is 4 percentage points lower than in the 2013 survey.

MEASURES TAKEN TO AVERT SECURITY RISKS



Also down by 5 percentage points was the percentage of respondents (44%) stating that their companies are using a system to assign differentiated access rights to different sections of their companies' IT infrastructures. The percentage of companies that use encryption to protect data stored on employee workstations also fell by 6 percentage points.

These changes are associated with several factors, one of which is the relatively high usage rate of these data security resources at companies. Antivirus software, encryption programs, and software used to manage external devices have all been regular features of the "classic" set of data security tools for several years now at companies worldwide. They are already widely used and, as a result, fewer respondents in our surveys are including them in the list of new resources being used in the survey period. This high level of deployment does not entirely account for the decrease in new demand, however. For example, the number of respondents reporting that they require a data security audit from their suppliers and partners working with the company's IT infrastructure (i.e., with remote access) fell by 3 percentage points to 32%.

At the same time, affiliates and contractors often serve as a way to get around security and are used by cybercriminals to infiltrate a targeted company's network. This method was used in the attack against Target, and Kaspersky Lab experts have previously seen signs of a similar approach being used during the Icefog espionage campaign that was exposed in September 2013.

According to survey results, employees who are the decision makers when it comes to choosing how to set up protection for a company's IT infrastructure still demonstrate the tendency to not see major cyber attack threats posed by contractor IT networks. This phenomenon can be easily explained: the targets of attacks launched via contractor networks are more likely to be

large companies in possession of confidential data that holds substantial value on the black market. As a result, respondents representing that class of company typically reported that they do in fact ask their contractors to perform data security audits. Meanwhile, representatives of small and mid-sized businesses, which constitute the majority of survey respondents, work with contractors less frequently and thus the risk of a targeted attack via affiliates or contractors is lower and less relevant for them.

The companies that took part in the 2014 survey named several new efforts being made to ensure data security, such as: financial transaction security systems (41%), data loss prevention systems (39%), as well as resources to maintain the functionality of web services and protection against DDoS attacks (37%). Nearly 31% of respondents stated that their companies use Security Information and Event Management (SIEM) programs, which among other things help to identify any data security incidents within a company's network.

Antivirus software is most commonly used in North America, where 79% of respondents in that region reported that their companies use such products for protection against cyber attacks. Antivirus programs are also commonly found in the Asian Pacific and the Middle East (72% each) and Western Europe (70%). These programs are least often used to protect corporate computers in Russia (61%), Japan (53%), and China (49%).

When it comes to protection against vulnerabilities in legitimate software, i.e., patch management, the Middle East is in the lead (64%), followed by North America (62%), and Western Europe (54%). Countries in the Asian Pacific, Japan, and China are all on the other end of this spectrum, with 45%, 39%, and 36%, respectively.

Specialized security resources for online financial transactions are most often used in the Asian Pacific (48%), in countries with developing markets (46%), North America, (45%), and the Middle East (40%).

In general, the survey results show that most companies see antivirus programs as the main tool for maintaining data security, while companies who reported the need to use additional resources — patch management tools, data leak protection, critical business information interception — remain in the minority. That is how it has been for many years now, while the cyber threat landscape never stops changing.

External threats: targeted attacks go mainstream

Companies of any size and based in any country regularly face data security problems. During the survey conducted by B2B International and Kaspersky Lab, it became clear that over the past 12 months, 94% of companies encountered at least one data security incident, the source of which was external to the company. One year prior, during the previous study, that number was 91%.

It is remarkable that this year, the number one external threat was spam, which was reported by 64% of respondents, while in 2013 malware attacks was in first place (named by 66% of respondents). According to the 2014 survey results, viruses, worms, Trojans, and other forms of malware were a problem for 61% of respondents.

EXTERNAL THREATS EXPERIENCED

	Globally	Russia etc.	China	N. America	W. Europe	E. Markets	APAC	Mid-East	Japan
Base	4,438	518	208	400	1,576	611	822	105	198
Spam	64%	75%	63%	72%	63%	63%	65%	62%	38%
Viruses, worms, spyware and other malicious programs	61%	78%	59%	66%	54%	62%	68%	51%	45%
Phishing attacks	38%	25%	41%	57%	41%	33%	39%	24%	23%
Network intrusion / hacking	25%	21%	40%	21%	22%	23%	35%	24%	21%
Theft of mobile devices	22%	15%	25%	19%	25%	23%	25%	8%	15%
Denial of service (DoS), Distributed denial-of-service attacks (DDoS)	18%	17%	34%	15%	17%	17%	20%	22%	13%
Theft of larger hardware	16%	11%	20%	12%	16%	18%	22%	9%	7%
Corporate espionage	16%	24%	26%	6%	12%	16%	21%	10%	9%
Targeted attacks aimed specifically at our organization / brand	12%	9%	20%	10%	10%	12%	18%	13%	6%
Criminal damage (including fire/arson)	6%	5%	6%	5%	5%	8%	10%	3%	3%
None	6%	3%	1%	7%	7%	6%	4%	11%	20%

The percentage of respondents reporting that their company was subjected to at least one targeted attack rose substantially, having been reported by 12% of respondents, while that number remained at 9% or under in the 2012 and 2013 studies.

The “popularity” of targeted attacks among malicious users varies depending on a company’s field of business. Organizations in the government and defense sector encounter targeted attacks most frequently. Some 18% of respondents representing those types of companies reported having run into at least one targeted attack. Remarkably, targeted attacks in that sector take place even more frequently than DDoS attacks, for example, which were named by 12% of respondents in the government and defense sector.

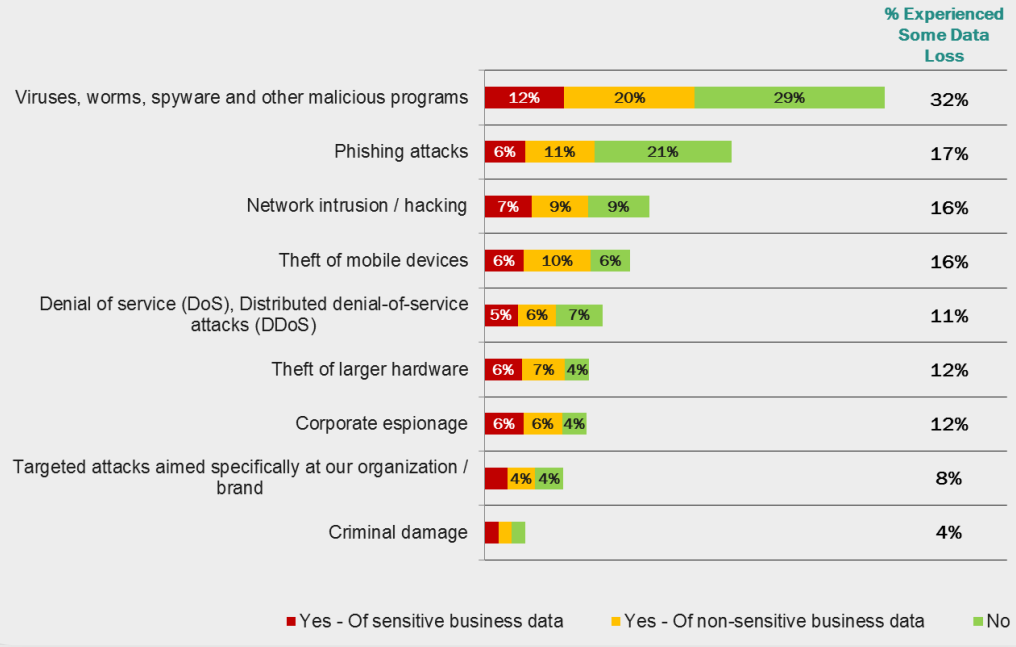
	Manufacturing	IT/ Software Etc.	Financial Services	Business Services	Construction/ Engineering	Government /Defence	Education	Healthcare /Services	Consumer Services	Other	Transportation /Logistics	Telecoms	Real-Estate	Utilities & Energy	Media /Design	Non-Profit /Charitable	E-commerce /Online Retail
Base	724	613	328	305	294	292	279	199	535	187	140	116	99	95	93	71	68
Spam	63%	58%	59%	68%	66%	71%	72%	58%	68%	67%	61%	66%	71%	57%	71%	68%	60%
Malware	60%	59%	59%	60%	61%	62%	68%	67%	62%	65%	56%	68%	61%	61%	68%	58%	46%
Phishing attacks	37%	39%	43%	40%	35%	39%	44%	40%	32%	27%	35%	39%	44%	43%	48%	34%	28%
Network intrusion / hacking	26%	32%	27%	20%	23%	25%	31%	27%	20%	16%	23%	30%	25%	27%	24%	14%	28%
Theft of mobile devices	23%	24%	23%	21%	21%	23%	22%	32%	19%	18%	22%	26%	19%	22%	24%	11%	24%
Dos/DDoS	15%	27%	20%	18%	13%	12%	19%	23%	16%	12%	14%	29%	20%	25%	16%	13%	21%
Theft of larger hardware	16%	16%	17%	14%	15%	17%	19%	23%	15%	16%	14%	22%	11%	15%	8%	11%	21%
Corporate espionage	18%	18%	19%	15%	18%	12%	11%	15%	13%	10%	15%	16%	13%	22%	15%	6%	22%
Targeted attacks	14%	12%	16%	10%	11%	18%	12%	12%	8%	7%	16%	17%	8%	12%	9%	13%	10%
Criminal damage	5%	6%	7%	4%	6%	7%	9%	10%	5%	4%	7%	9%	6%	6%	3%	11%	10%
None	6%	6%	7%	8%	5%	4%	3%	6%	7%	12%	9%	2%	6%	5%	8%	7%	10%

Targeted attacks were also reported by 17% of respondents in the telecom industry, 16% of those in financial services, and another 16% of companies in transport and logistics. Companies in real estate, consumer services (8% each), and media (9%) were rarely the victims of targeted attacks.

Mobile devices were found to be stolen or missing most often in healthcare organizations (32% compared to an average of 23% for all companies surveyed). Another relatively high percentage of theft took place in telecom (26%), media outlets, and e-commerce businesses (24% each).

One of the main consequences of a successful cyber attack — regardless of what kind of attack it is — is the loss by the targeted organization of critical information. In general, 28% of those surveyed reported that during the past 12 months, their organizations had faced at least one data security incident, the source of which was external to the organization, and which was the reason for a leakage of important business data. Compared with the results of the prior year's survey, that number fell by 7 percentage points, which may indicate that IT management teams are dedicating more time and effort to data security.

DATA LOSS EXPERIENCED (EXTERNAL THREATS)



Among the different types of external threats, the most dangerous from the standpoint of data leakages are still attacks involving malicious software — 32% of respondents noted that their companies had lost important business information after attacks with viruses, Trojans, and other forms of malware. Compared with the results from the previous survey, this number fell slightly (by 3 percentage points). Phishing attacks were named as the second most dangerous threat, just like in last year's survey. Roughly 17% of those surveyed stated that similar incidents had led to leakages of critical data.

Targeted attacks also caused data leaks according to 8% of the survey respondents. While compared with malware attacks, the percentage of targeted attacks that lead to data leakages is considerably lower, typically an attack targeting a specific company will help malicious users to get their hands on much more valuable information that will cause much more serious damage.

Furthermore, external threats are just one of the dangers companies today have to deal with; internal threats can cause just as much harm.

Internal threats: vulnerabilities, employees, and mobile devices

Company data security can also fall victim to yet another threat that is just as significant as external threats — and they come from within. Just like last year, the main internal risks are still vulnerabilities in the software programs used by companies (36%), in addition to employees who are not familiar with IT security rules and regulations, which lead to unintentional data leaks (29%), and the loss or theft of mobile devices used for processing and storing important corporate data.

	Globally	Russia etc.	China	N. America	W. Europe	E. Markets	APAC	Mid-East	Japan
Base	4,438	518	208	400	1,576	611	822	105	198
Vulnerabilities / flaws in existing software	36%	50%	38%	33%	32%	37%	37%	23%	26%
Accidental leaks/sharing of data by staff	29%	34%	42%	26%	26%	25%	34%	25%	23%
Loss/theft of mobile devices by staff	26%	19%	27%	22%	29%	24%	29%	25%	28%
Intentional leaks/sharing of data by staff	21%	22%	32%	12%	18%	21%	30%	18%	14%
Information leaked/inappropriately shared on a mobile device	20%	18%	30%	16%	18%	22%	27%	13%	11%
Security failure by third party supplier	16%	10%	25%	14%	15%	17%	23%	11%	10%
Fraud by employees	16%	17%	18%	11%	14%	18%	21%	15%	11%
None	17%	14%	9%	26%	19%	14%	11%	30%	27%

One positive factor here is the fact that the number of respondents reporting vulnerabilities in corporate software is steadily declining. In 2011 when the survey was conducted for the first time, 41% of companies reported problems with software vulnerabilities; in 2012 that number fell to 40%, and was down again in 2013 at 39%. Compared to the 2013 survey results, the latest numbers are down by 3 percentage points, which could be the result of using software update management tools. In 2013, nearly 54% of those surveyed included these types of solutions on their list of the most important resources for ensuring data security at their organizations.

In addition to the percentage of incidents stemming from vulnerabilities, over the past 12 months, the percentage of unintentional data leaks caused by employees also fell (by 3 percentage points), as did the loss or theft of mobile devices (4 percentage points). At the same time, the number of reported incidents in which staff members intentionally caused a data leak increased (from 19% in 2013 to 21% in 2014). Looking at a breakdown of these incidents by industry, one can see that the amount of internal data security incidents varies greatly from one sector to another. For example, companies in the e-commerce sector are least often victimized by vulnerabilities — only 16% of respondents from that category of company indicated errors in corporate software as a reason for any data security incidents. Meanwhile, other industries

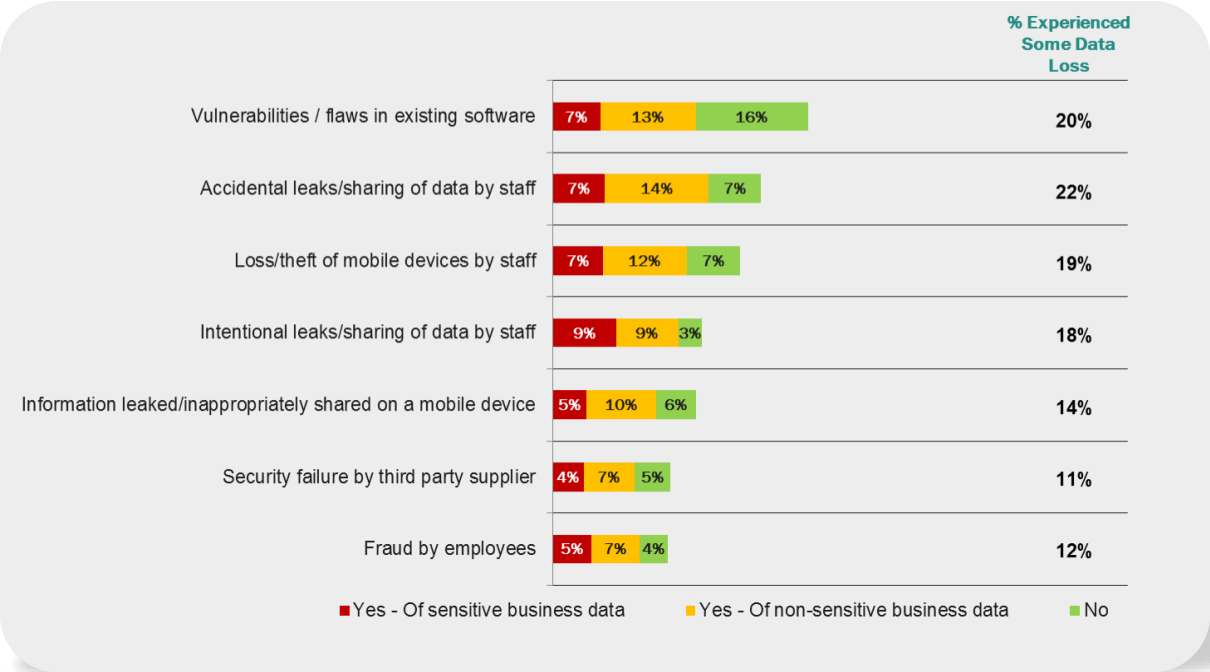
(save for nonprofits and charitable organizations, representing 28% of the answers) demonstrated roughly the same results in a range from 33% to 40% of responses. The e-commerce field did have a particularly high incident rate for data leaks intentionally caused by employees (31%, compared to the 22% average).

	Manufacturing	IT/ Software Etc.	Financial Services	Business Services	Construction/ Engineering	Government /Defence	Education	Healthcare /Services	Consumer Services	Other	Transportation /Logistics	Telecoms	Real-Estate	Utilities & Energy	Media /Design	Non-Profit /Charitable	E-commerce /Online Retail
Base	724	613	328	305	294	292	279	199	535	187	140	116	99	95	93	71	68
Vulnerabilities / flaws in existing software	35%	37%	38%	29%	36%	40%	40%	36%	34%	34%	36%	35%	33%	40%	40%	28%	16%
Accidental leaks/sharing of data by staff	31%	28%	28%	30%	26%	32%	29%	32%	25%	25%	31%	42%	27%	33%	22%	27%	25%
Loss/theft of mobile devices by staff	29%	26%	30%	23%	27%	27%	25%	26%	20%	25%	26%	28%	36%	22%	26%	24%	25%
Intentional leaks/sharing of data by staff	22%	23%	26%	14%	22%	18%	20%	25%	21%	14%	24%	22%	18%	18%	15%	8%	31%
Information leaked/inappropriately shared on a mobile device	21%	19%	21%	22%	16%	22%	23%	21%	17%	14%	24%	23%	25%	25%	24%	17%	16%
Security failure by third party supplier	18%	17%	18%	13%	16%	19%	17%	16%	17%	12%	14%	17%	15%	14%	18%	7%	15%
Fraud by employees	18%	15%	25%	8%	16%	15%	12%	17%	16%	9%	19%	22%	19%	21%	13%	10%	16%
None	13%	15%	13%	26%	14%	14%	19%	18%	21%	27%	16%	12%	16%	12%	19%	24%	19%

Accidental leaks of confidential information took place most often at telecom companies (42% of responses, with a 31% average), while incidents associated with fraudulent employee actions were most frequently noted at financial organizations, where one-fourth of respondents in this industry indicated that such incidents had taken place at their companies over the past 12 months.

It stands to reason that these types of incidents caused the company to lose secret information. On average, nearly 27% of companies lost confidential data as the result of an internal data security incident.

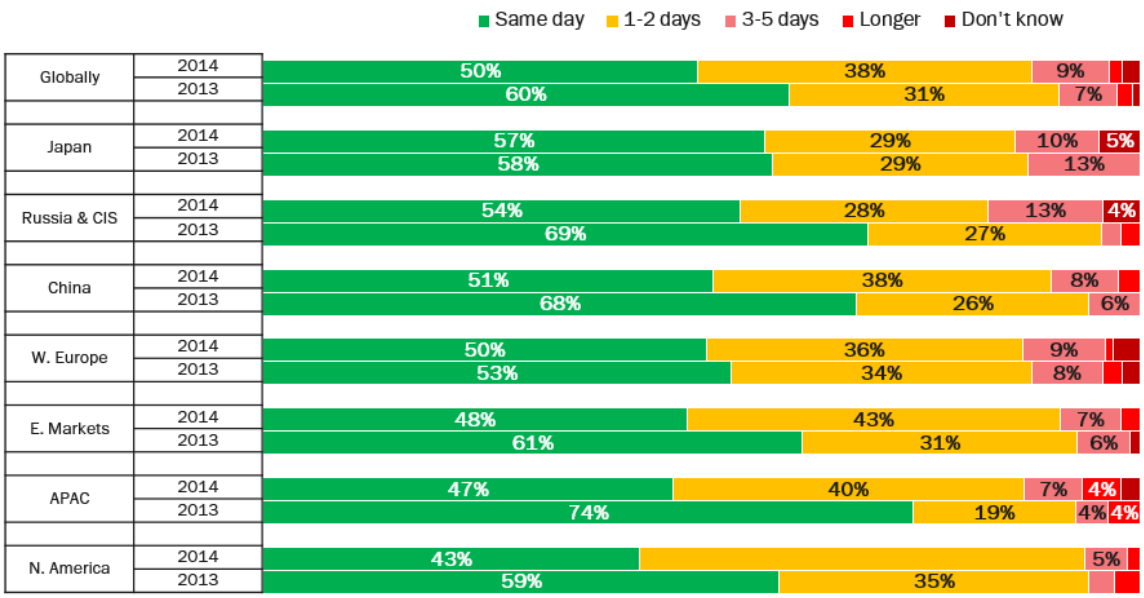
Although according to the number of reported incidents that led to the disappearance of business-related information (including non-confidential data), vulnerabilities are in the lead, together with accidental leaks and leaks resulting from the loss or theft of mobile devices. Meanwhile, the most dangerous from the point of view of the loss of secret data are intentional data leaks orchestrated by employees. Half of the 18% of respondents reporting these types of incidents also pointed out that insiders had stolen secret information. When it came to other incidents, that number ranged anywhere from 4 to 7%.



The percentage of internal incidents linked to vulnerabilities and which led to the loss of secret information decreased over the year by 3 percentage points, while the percentage of incidents caused by the loss or theft of mobile devices, but with a similar outcome, fell by 2 percentage points.

AVERAGE TIME TAKEN TO REPORT THEFT OF MOBILE DEVICES

AROUND 50% REPORTED THAT ON AVERAGE, MOBILE DEVICE THEFT WENT UNREPORTED FOR MORE THAN A FULL DAY, THIS WAS UP FROM 40% IN 2013



While the data may show a slight decrease (2%) in data loss attributed to missing mobile devices, the fact that 19% of businesses which suffered a missing mobile device experienced some form of resulting data loss remains a significant threat vector. The survey uncovered another interesting factor – the time it takes employees to report missing devices. As mobile usage grows across businesses, it turns out employees are actually becoming slower to respond to missing devices. According to the survey, more than one-third of employees (38%) take up to two days to notify their employers of missing mobile devices. The percentage of employees who notified their employers the same day the incident occurred decreased from 60% to 50% from 2013 to 2014.

The landscape of external and internal threats encountered by companies over the past 12 months clearly demonstrates the need to use comprehensive security solutions. The very fact that these incidents take place also goes to show that companies' IT infrastructures are not sufficiently secure. There are many reasons and factors for the current state of affairs, which include inadequate threat assessment and others, such as, the belief that any financial damages caused by a cyber attack will be lower than any investments in purchasing and deploying security solutions; based on the survey results, roughly 28% of respondents hold that view.

Yet as the survey results have shown, the damages caused by cyber attacks can turn out to go far above the budgets that many companies set aside for data security.

Damages: an average of $720K per incident

Cyber attacks can translate into major financial losses. This thesis has already been confirmed for the second year in a row by the results of the survey conducted by B2B International and Kaspersky Lab. Just like in the 2013 survey, when assessing financial damages caused by cyber attacks, experts asked company representatives about incidents of confidential data leaks that resulted from data security incidents.

The respondents were asked if attacks caused direct financial losses, and if there were any additional expenses incurred by the targeted company as a result of the attack. The estimates also included responses from respondents that were able to disclose a specific amount of losses incurred by their company following an attack.

AVERAGE IMPACT OF DATA SECURITY BREACHES

Estimated Average For SMBs	Overall	Brazil	China	France	Germany	India	Italy	Japan	Russia	Spain	UK	USA	Mexico	Turkey	Australia
Base	1,397	186	218	150	110	190	134	101	339	151	123	156	163	120	112
Total Expected Damages	33K	37K	110K	50K	33K	38K	28K	30K	16K	52K	35K	26K	36K	42K	40K
Total Reactive Spend	10K	11K	24K	24K	20K	13K	11K	8K	7K	17K	14K	14K	8K	11K	10K
Overall Financial Impact	42K	49K	134K	74K	53K	51K	39K	38K	23K	70K	48K	40K	44K	53K	51K

Estimated Average For Enterprises	Overall	Brazil	China	France	Germany	India	Italy	Japan	Russia	Spain	UK	USA	Mexico	Turkey	Australia
Base	464	39	50	58	29	65	25	60	67	34	39	85	24	25	39
Total Expected Damages	636k	1.67M	817K	1.17M	394K	783K	419K	354K	421K	581K	1.50M	372K	363K	597K	512K
Total Reactive Spend	84K	124K	240K	137K	76K	77K	256K	93K	51K	50K	158K	61K	48K	71K	76K
Overall Financial Impact	720K	1.80M	1.06M	1.31M	471K	860K	675K	448K	472K	631K	1.66M	433K	411K	668K	588K

Significantly lower Significantly higher

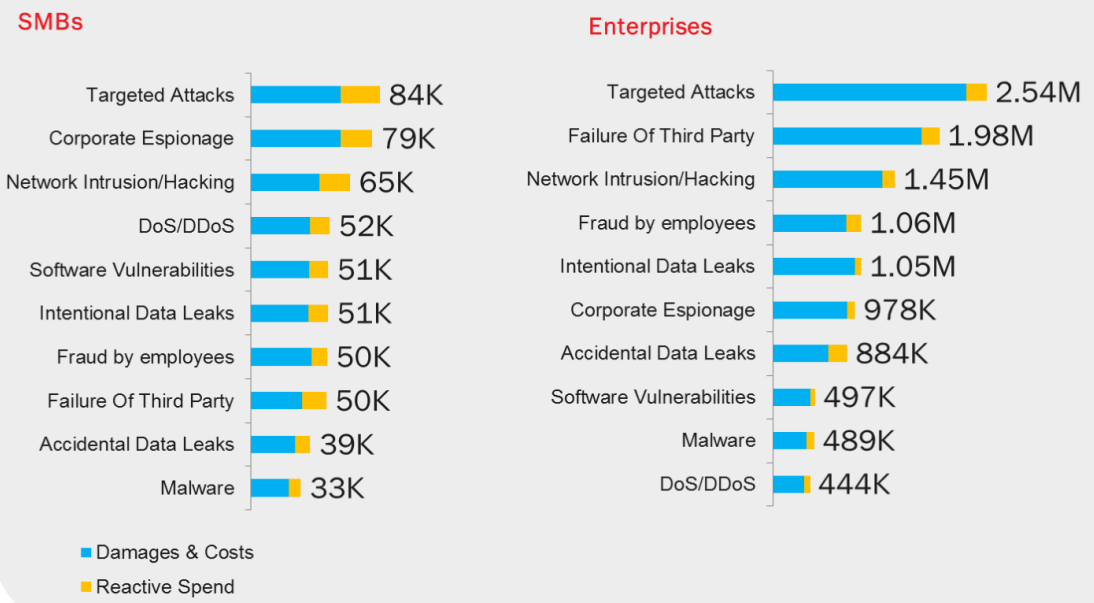
Using the data collected about losses and expenses for additional services that a company would have been forced to commission after an attack against its IT infrastructure as well as the average cost of these types of services on the markets in various countries, the experts at B2B International were able to estimate the financial damages incurred by companies that fall victim to cyber attacks.

As a result, it became clear that on average, large companies stand to lose roughly $720,000 from one data security incident, while SMEs face the potential loss of about $49,000. In 2013,

the average losses for large companies was $649,000, or 14% less than this year, while SME losses were estimated at an average of $50,000 (12% higher than in 2014).

Depending on the type of attack launched against an organization, the damages could increase.

AVERAGE IMPACT OF DATA SECURITY BREACHES BY TYPE



For example, a successful targeted attack against a large company can cost up to $2.54 million in losses plus additional expenses; an attack via a supplier's IT infrastructure can cost up to $1.98 million, and a successful network hack can cost $1.45 million.

The estimated range of losses for SMEs is considerably lower. However, this difference is offset by the scale and size of the business — SME revenues are a fraction of the revenues generated by large corporations, which means that comparable smaller losses can strike a huge blow even to healthy small and mid-sized enterprises.

As we noted above, the total amount of damages is based on two types of expenses: the losses incurred by the company directly resulting from the incident, and response expenses that a company will have to take on after the incident for remediation and prevention purposes.

Losses stemming from the incident are comprised of expenses for professional services (external IT professionals and data security experts, legal counsel, PR experts, etc.), lost business opportunities (tarnished reputation, breach of contract resulting from the incident, etc.), as well as damages from forced interrupted functioning of the IT infrastructure and, as a result, overall operations and business process interruptions stemming from the data security incident.

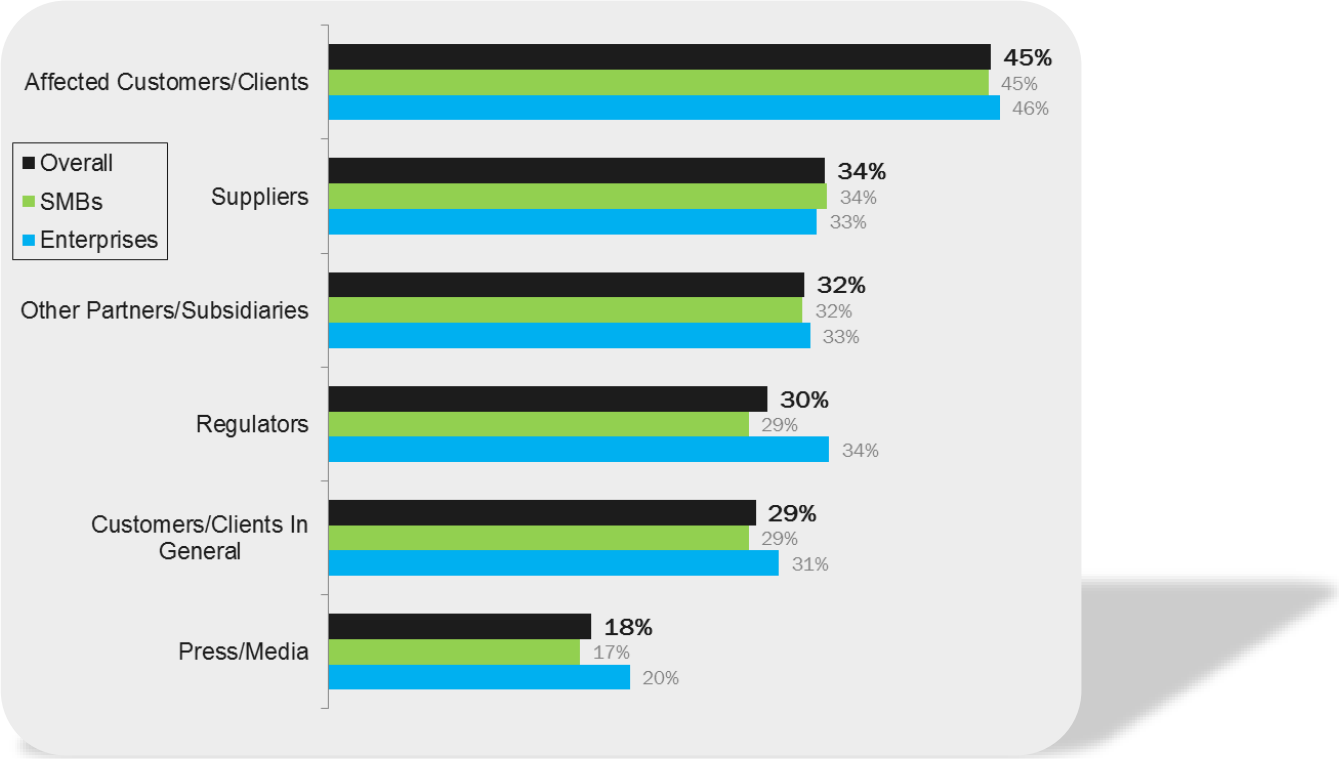
Data losses cause a total of $33,000 for SMEs. Companies that fall within the Enterprise category stand to incur a total of $636,000 in losses.

A major factor in the total amount that a company stands to lose as a result of a significant data security breach are the additional response expenses a company will need to take on in order to deal with the consequences of the breach and prevent any such incidents from taking place in the future.

These expenses are comprised of the cost of hiring additional employees, holding data security training, and purchasing software and hardware to protect the company's data systems against both external and internal incidents. Those costs can come to about $10,000 for SMEs, and $84,000 for large companies.

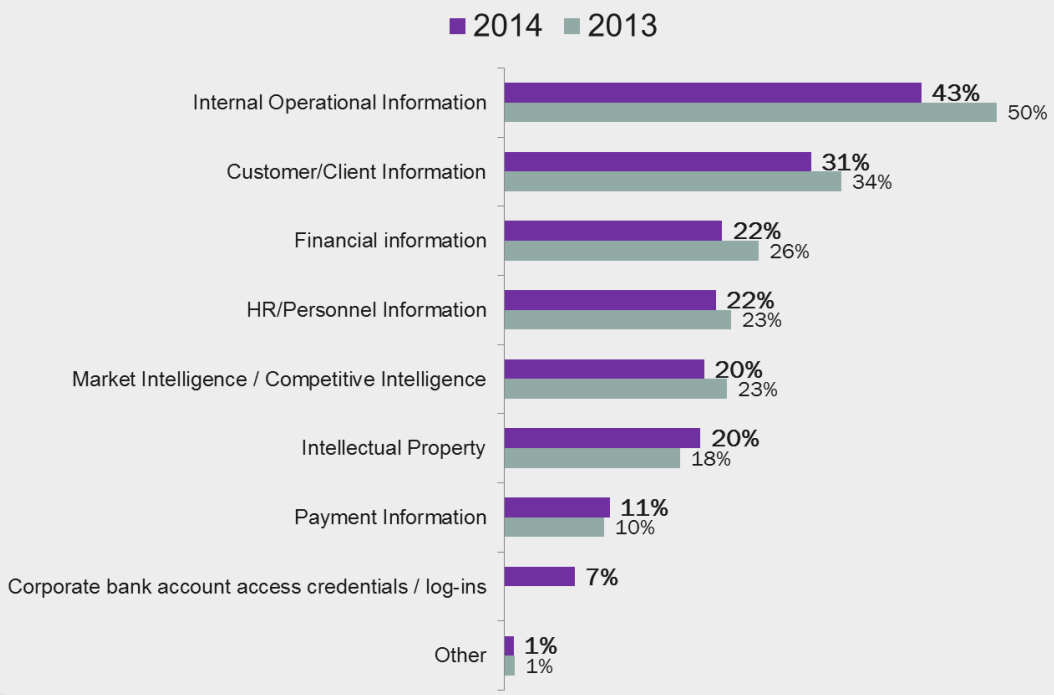
Other losses: reputation damages and confidential information

In addition to financial losses, a data security breach can also harm a company's reputation. For example, 72% of the companies that took part in the survey reported that they have had to publicly acknowledge an incident and notify any clients who may have been harmed as a result of the incident (45% of cases), in addition to suppliers (34%), other affiliates (32%), regulators (30%), all clients without exception (29%), and media outlets (18%).



As a result of a data breach, a company will most often lose its internal operating data (42%). Incidentally, compared with the prior survey the percentage of leakages of this type of information dropped considerably, by 7 percentage points. Client data was in second place in terms of loss frequency (31%) and financial information was ranked third (22%). Notably, just like with the instances involving internal company data, the percentage of client and financial data breaches fell by 3 and 4 percentage points, respectively. However, some other types of data started to leak from companies more frequently.

TRACKING TYPES OF DATA BEING LOST



In particular, one out of every five (20%) respondents reported that their company had lost intellectual property (2 percentage points higher than in 2013). The percentage of those who indicated that a data breach had led to the loss of data about payments from corporate accounts changed only slightly (11% compared to 10% in 2013). In 7% of cases, third parties were able to get their hands on the data required to access those accounts.

Most often, intellectual property was lost from companies in e-commerce (34%) and the telecom sector (23%). Financial data was most frequently lost by financial organizations (32%), transportation (27%), and construction (26%) companies. Market and competitive intelligence information was often lost by companies in real estate (28%), the media and design (25% each), and production companies (24%).

While the amount of respondents reporting that their organization suffered a breach of client information fell from the 2013 results, concerns about the loss of this type of data are key for many, and 22% of respondents named this as the number one risk. Financial data was in second with 20% of responses, and internal operations data and intellectual property were both in third with 14%.

WHAT BUSINESSES FEAR LOSING

Even though concerns about the loss of financial data (including data about company revenues, expenses, profits, etc.) rank second, there are also other types of risks that are closely associated with a company's financial operations. In particular, 7% of the respondents are concerned about losing payment information, while 5% are worried about corporate bank accounts and information needed to access those accounts online (usernames and passwords). In total, 32% of all of the responses were related to financial data.

That makes perfect sense, since clearly a loss of financial information, especially when linked to access to corporate accounts, is associated with a higher probability of monetary loss than any other data security risk. The survey respondents are right to be concerned about having that kind of data compromised in a cyber attack, as the result of an insider's actions, or unintentional errors on the part of employees.

Overall, the results of this component of the survey illustrate that company concerns about the loss of various types of data match up with what third parties do actually get their hands on after a data security breach. This may mean that companies are more or less adequately assessing data security risks. Meanwhile, the fact that the percentage of theft of specific types of data has dropped since last year means that the measures companies are taking to secure their data are effective. All the same, these actions are still insufficient to trigger a major drop in the number of data security breaches or rule them out completely.

Conclusion: the importance of choosing the best possible protection

The main conclusion that can be drawn from the results of the survey conducted by B2B International and Kaspersky Lab is that, unlike last year's results, companies are demonstrating a more pragmatic and precise approach to data security for their IT infrastructures.

In last year's study, concern No. 1 for IT management teams was the prevention of data security breaches as a whole. However this year, the main concern is a more narrow and complicated task: protecting against targeted attacks. This change in priorities speaks to the fact that companies are, at the very least, developing a better understanding of what's behind existing data security risks and how to protect themselves against specific risks, rather than the broader idea of malware in general.

Other major trends among threats posed against companies include significant growth in the percentage of targeted attacks against companies. This indirectly conveys a negative trend, where illegal services to carry out these types of attacks are in greater demand, which means that in light of the "customization" of the scenarios and application of targeted attacks, it will become even more of a challenge to protect companies against them.

Another important trend to note is that even though some threats facing companies are becoming less frequent than last year, in general the percentage of organizations that encounter any type of cyber threat at least once every 12 months is on the rise. The amount of financial damages incurred by companies as the result of these incidents is also growing, including due to higher market costs for the services that companies are forced to commission in order to deal with the consequences of a security breach and prevent any similar incidents in the future.

Today's data security resource market is already fairly well developed, and sufficiently so for clients to choose from a dizzying array of security solutions for just about any component of a company's IT infrastructure. The problem with this situation is becoming how to choose the proper combination of components needed to ensure that the company is reliably protected against cyber threats. Based on the results of this latest survey, Kaspersky Lab has prepared a number of recommendations which will help companies significantly boost their level of protection against cyber threats.

Antivirus is not enough

This statement is nothing new, although recently — and especially in connection with the heightened number of targeted attacks meant to steal critically important confidential data and money — it is more relevant than ever. Antivirus software is a must when it comes to

protecting workstations, but equally important is software for monitoring and promptly patching vulnerabilities, providing protection against DDoS attacks and targeted attacks, as well as protection for corporate mobile devices, among other things.

In other words, companies ought to apply a comprehensive approach to data security. At the same time, businesses operating in a specific field, such as banking and other financial service organizations, should employ specialized security solutions dedicated to minimizing the risks specific to their business operations, such as financial fraud.

All components of an IT infrastructure need protection

Many companies understand that they need to secure their IT infrastructures, and their understanding is that it includes office computers, servers, and network equipment — basically everything that keeps day-to-day business operations up and running. However, things such as production equipment, trade terminals, vital service systems, and physical safety control systems are generally overlooked when companies are considering what needs protection against cyber attacks — even though these systems typically operate on the very same hardware and software base as the office and is often integrated with it. This situation opens up technological opportunities for malicious users to launch attacks against these less recognized components of the IT infrastructure, and companies ought not neglect their protection, both by imposing special security policies and the appropriate customization and settings, as well as by using security solutions developed especially for these parts of the infrastructure.

Security software doesn't mean much without effective security policies

Although many companies today recognize the need to use a variety of security solutions within their IT infrastructure, these solutions alone are simply not enough. As the results of our survey have shown, a major share of data security breach incidents leading to the leak of confidential data are the result of employee actions, be they intentional or unintentional. In order to prevent accidental leaks, companies need to boost the level of data security awareness among employees. In particular, this means building a stronger understanding of working with and handling corporate information stored on mobile devices. Security policies setting out an employee's responsibilities and accountability when it comes to the disclosure of confidential information is yet another action that can considerably boost the level of corporate data security.