DAMAGE CONTROL: THE COST OF SECURITY BREACHES

IT SECURITY RISKS SPECIAL REPORT SERIES

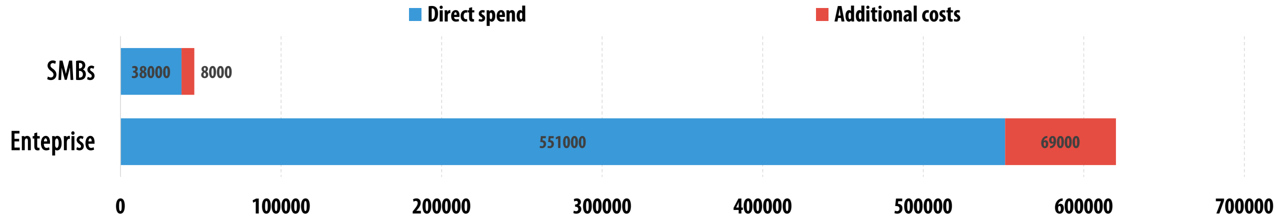
Kaspersky Lab

Corporate IT Security Risks Survey details:

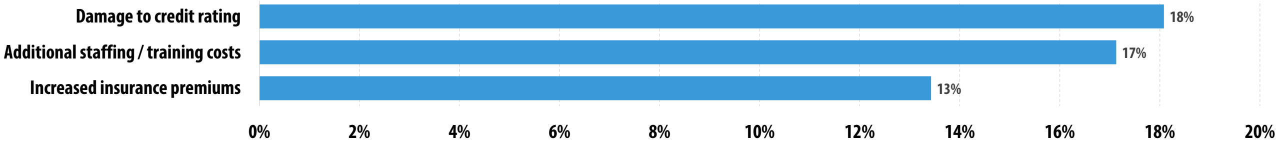
- More than 5500 companies in 26 countries around the world
- Top managers and IT professionals answered questions about security, IT threats and infrastructure
- We specifically asked them about the cost of recovery when they experience a security breach

What we have found:

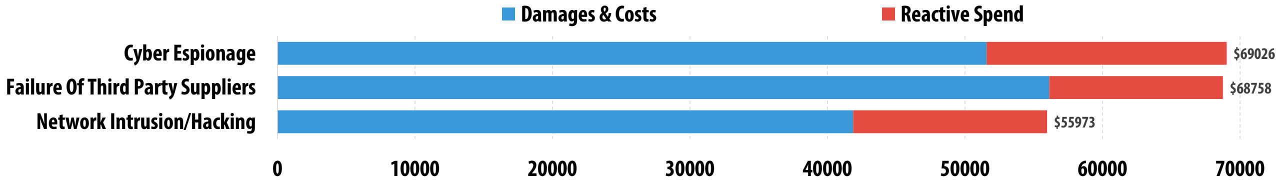
- 90% of businesses admitted a security incident. Additionally, 46% of businesses lost sensitive data due to an internal or external security threat.
- On average enterprises pay US$551,000 to recover from a security breach. SMBs spend 38K. This is direct spend required to recover from an attack.
- In addition, the indirect costs for enterprises are US$69,000, $8,000 for SMBs.



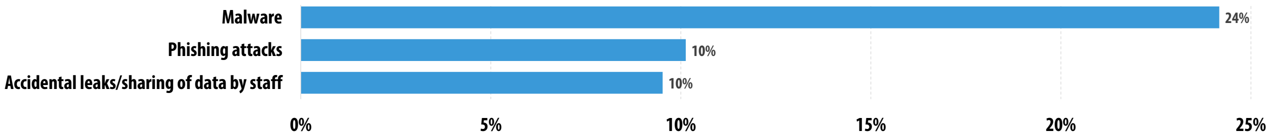
- Top three major consequences of a breach:
  - Loss of access to business-critical information
  - Damage to company reputation
  - Temporary loss of ability to trade



- Top three most expensive types of security breaches:
  - Third-party failure
  - Fraud by employees
  - Cyber espionage



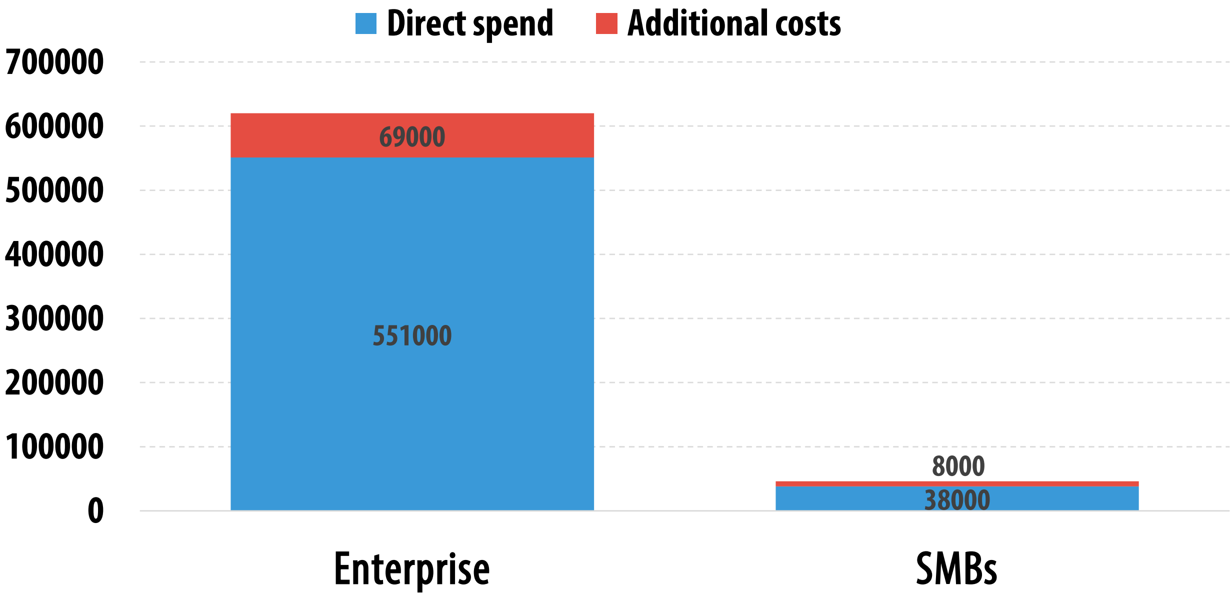
- Top three IT security threats that lead to data loss:
  - Malware
  - Phishing attacks
  - Accidental data leaks by staff



Key finding: Enterprises lose half a million USD on average from a security breach

It's not an easy task to estimate how much a business will lose as a result of a security breach. Figuring out a typical loss is even more complicated. Businesses are cautious of sharing such data, and sometimes they struggle to discern direct financial damage from indirect expenses, also caused by a cyberattack. That is why the results of the 2015 global IT Security Risks survey conducted by Kaspersky Lab in cooperation with B2B International are unique and noteworthy.

We asked companies what type of losses they experienced as a result of a security breach and the budget spent on each major type of loss or expense. Using this data, we estimated a probability of a certain type of loss and calculated a corresponding average expense. Applying the weight of probability we finally calculated an average loss for small and medium businesses (under 1500 seats) and enterprises (1500 seats and more).



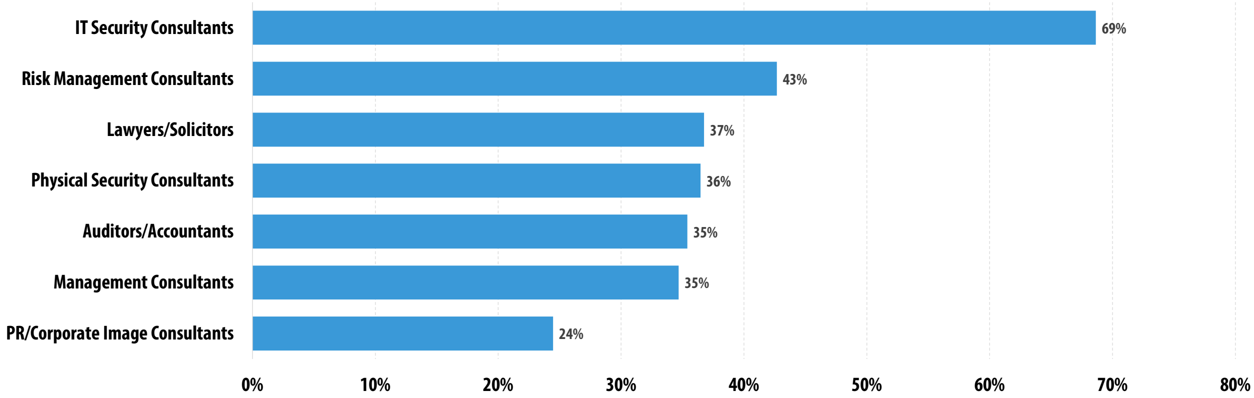
On average, it costs more than half a million US dollars to recover from a security breach for an enterprise. The average expected loss for SMBs is $38,000. These are only direct losses: money businesses have to allocate to pay for professional services, to cover lost contracts and downtime. Indirect damages, i.e. the budget businesses have to allocate for additional staff hiring and training, infrastructure upgrades etc. are on average $69000 for large businesses and $8000 for SMBs. Let's take a look at these findings in detail.

Direct damages

Almost all businesses, regardless of their size, have to invite external experts to recover from a security breach. But these expenses are quite low in comparison with losses from downtime and the lost business opportunities caused by an attack. Not all security breaches lead to downtime, but if this does occur (in about a third of incidents it does), it becomes the most expensive consequence of an attack: up to 1.4 million USD for large businesses.

	SMB		Enterprise	
	Proportion of business incurring this expense	Typical losses	Proportion of business incurring this expense	Typical losses
Professional services	88%	$11K	88%	$84K
Lost business opportunities	32%	$16k	29%	$203K
Down-time	34%	$66K	30%	$1.4M
Total expected typical damage	$38K		$551K	

Professional services do not always mean hiring external IT professionals to help mitigate a security breach. Although this is the most frequently used measure, many companies have to allocate funds to hire risk management consultants and lawyers. About a quarter of security incidents require help from PR consultants, thus indicating that a breach has become known to public. This figure corresponds with the 'disclosure' statistics, available below.



Additionally, we have estimated the financial cost of damage to brand reputation. The value of a brand and corresponding damage are very hard to calculate, but we decided to give it a shot. We have combined consultancy expenses, lost opportunities due to damaged corporate image and spend on marketing and PR activities aimed at reducing the impact to reputation. The average losses for this particular type of damage are $8,653 for SMBs and $204,750 for enteprises.

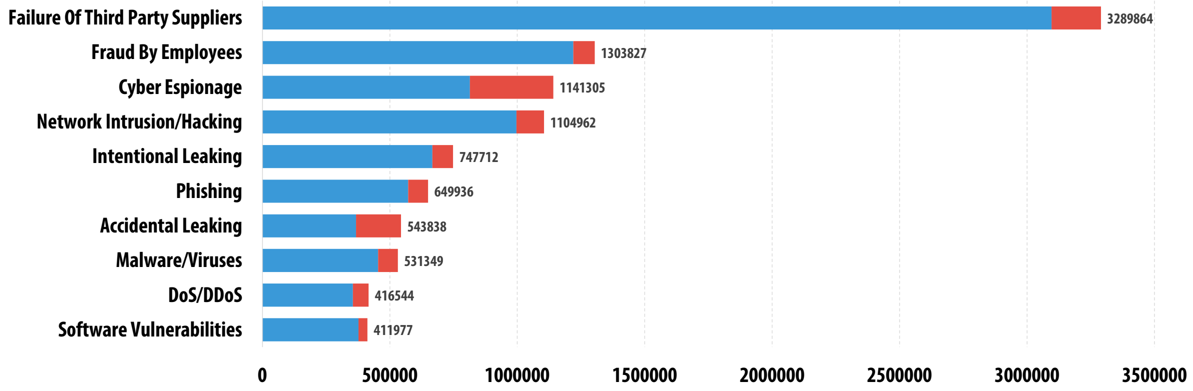
Indirect spend

After the security breach, most businesses try to prevent such incidents from happening in the future. This too requires extra budget, although this cannot be directly attributed to a security breach recovery. 75% of security breaches led to these unexpected expenses.

	SMB		Enterprise	
	Proportion of business incurring this expense	Typical losses	Proportion of business incurring this expense	Typical losses
Staffing	41%	$5.5K	40%	$52K
Training	47%	$5k	53%	$33K
Systems	54%	$7K	54%	$75K
Total expected indirect spend	$8K		$69K	

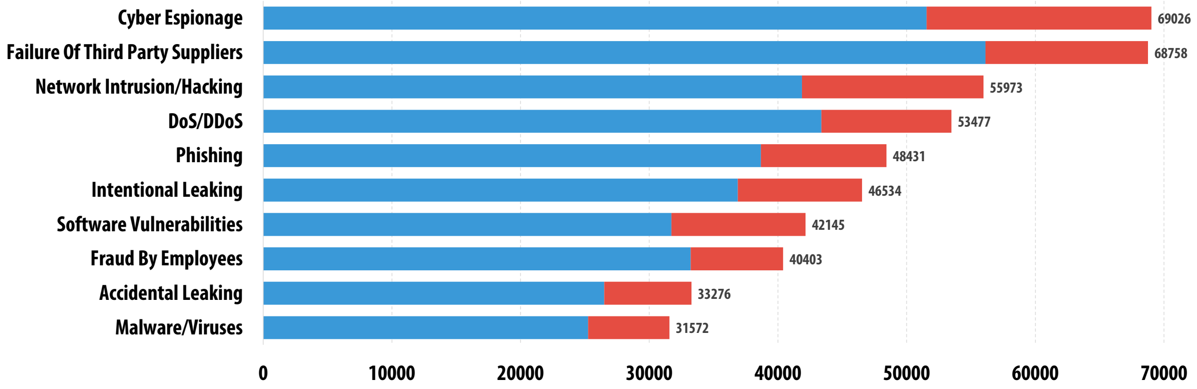
Cost of security incidents by type

Total financial impact of data breaches depends on the type of the incident. When we asked businesses, to attribute a security breach to a certain cause and estimate an amount of loss, we were able to pinpoint the most 'expensive' types of incidents.



Total impact of security incidents by type for enterprises

Incidents involving the security failure of a third-party contractor, fraud by employees, cyber espionage and network intrusion appear to be the most damaging for large companies, with total average losses significantly above other types of security incident.



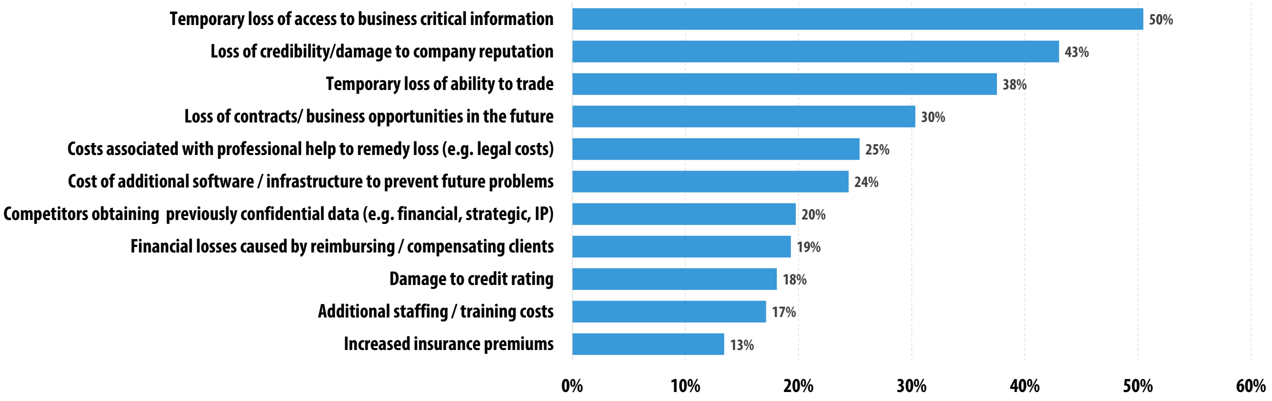
Total impact of security incidents by type for SMBs

The danger level of security incidents is slightly different for SMBs: although they suffer significantly from espionage attacks, third party supplier problems and network attacks, DDoS attacks should also be a major concern.

Security breaches are a top concern

One of the key findings of the 2015 IT Security Risks survey is that IT specialists are taking cyber threats much more seriously than last year. The second half of the past year was rich with security breaches and APT announcements, and this lesson has been learned - 50% of IT professionals list prevention of security breaches as one of their three major concerns. Last year, security breaches were named among top three concerns only by 30% of respondents.

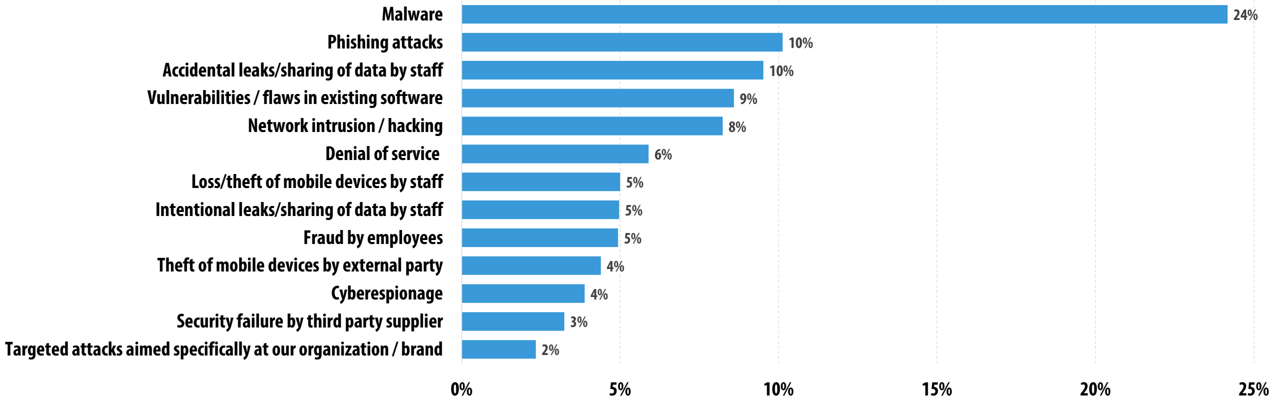
Often, it can be difficult for a business to comprehend the scale of a security breach until after it has happened. At first it may just look like the loss of private data, but the long-term damages can end up costing a lot more. It is the consequences of a security breach that have the worst impact on a business.



Frequency of the three worst (chosen by respondents) consequences of a security breach

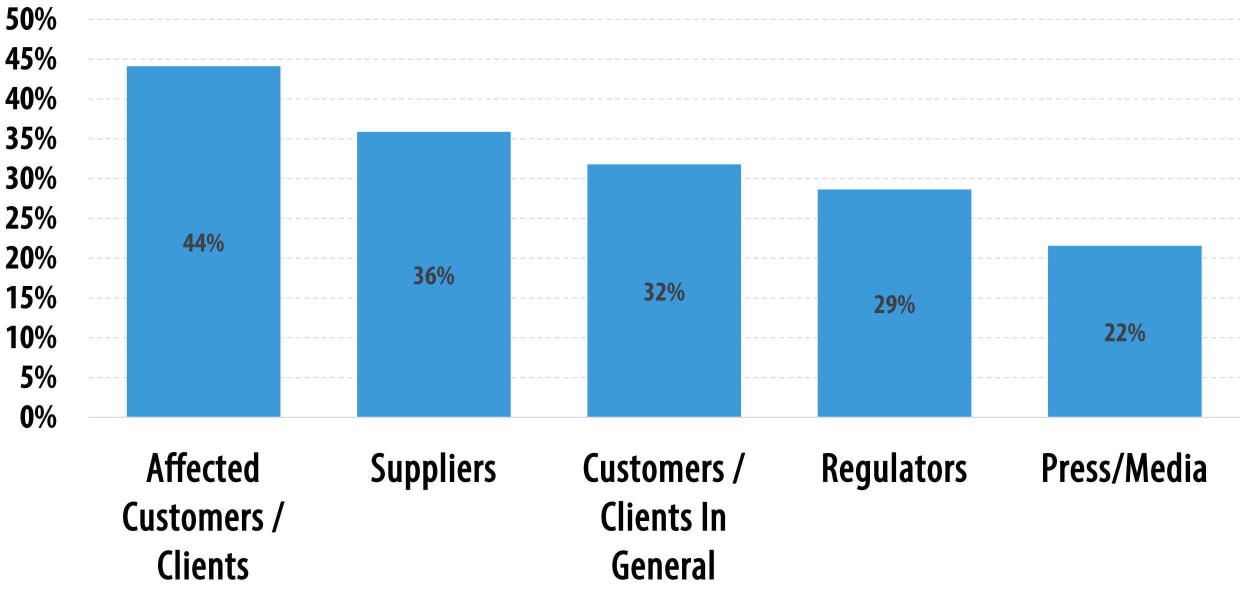
Threats experienced

But what threats are likely to cause data breaches? Almost all (90%) of respondents admitted to security incidents. 46% of businesses told us that at least one security incident in the last year has led to a data loss. This is the breakdown of IT security threats experienced by businesses that have caused severe security breaches:



Disclosure of security breaches

The disclosure of information about security breaches has a serious impact on the brand reputation of a business. Companies that suffered such incidents had to share this information with:



While the severity of 44% of security breaches compels businesses to disclose information to clients and customers, only one incident out of five becomes publicly known.

Conclusion

There are too many variables that contribute to the total impact of a corporate security breach. The consequences are also different: for some businesses it's the slight increase of the total IT budget, for others it's a significant financial and reputational damage, and for some it's going out of business with all assets wiped out. One thing is certain - the cost of a security breach is always higher than the cost of protection: the ability to reduce the risk and avoid the shaky path of recovery always pays off.

Although real damages can be very different from our average estimation, in this report we've made a unique attempt to connect potential risks and real consequences of a security breach, defined in dollars, not gigabytes of data and hours of downtime. 90% of the companies we asked admitted they had to deal with security incidents, ranging from malware attacks to DDoS and targeted intrusions.

We now also have a high-level understanding of how much businesses spend, in order to recover from a successful attack. Using this methodology, we will be able to see how the constantly evolving threat landscape affects the price that victims of cybercrime have to pay, now and in the future.