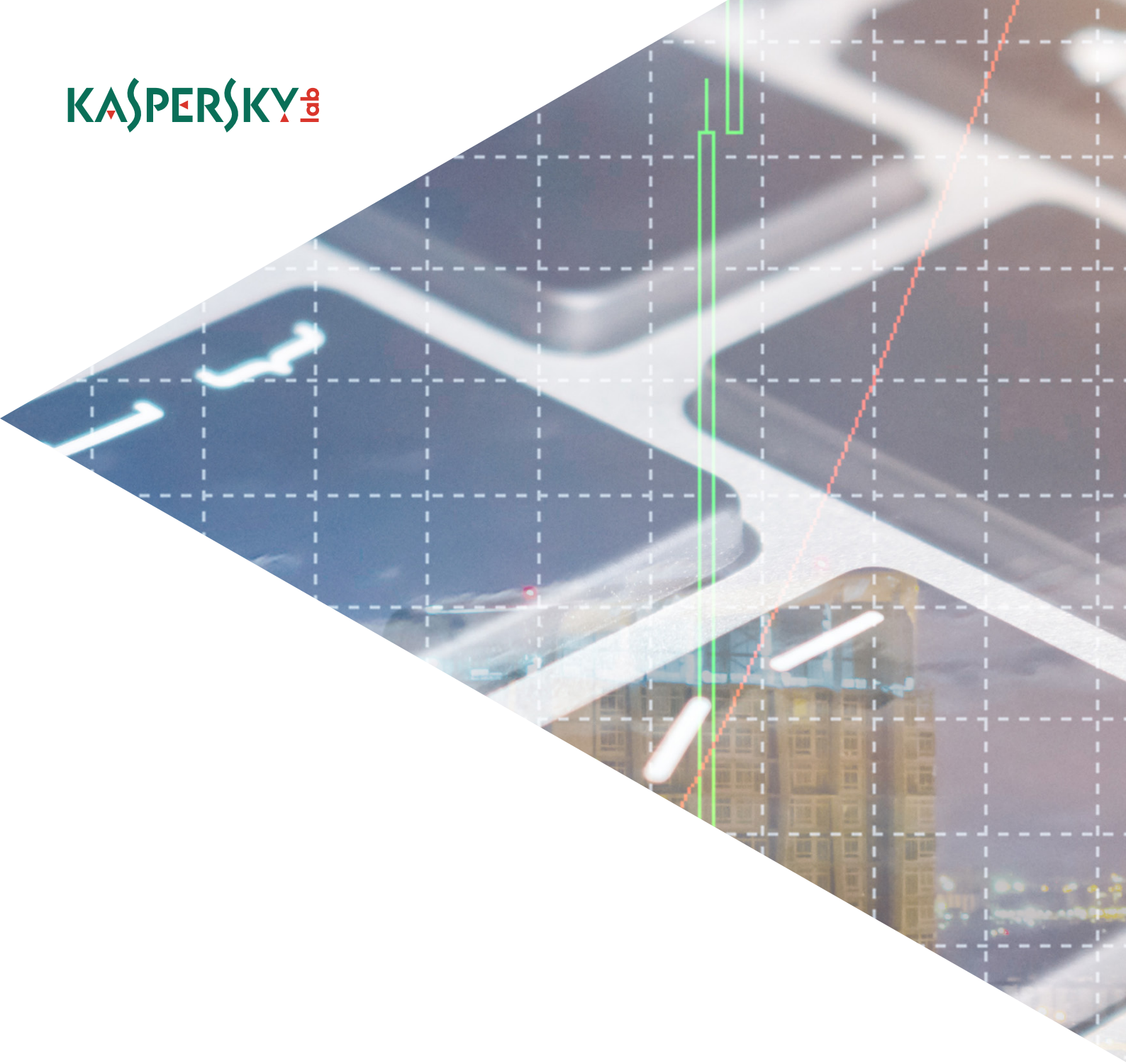


MEASURING FINANCIAL IMPACT OF IT SECURITY ON BUSINESSES

IT Security Risks Report 2016
Kaspersky Lab

CONTENT

INTRODUCTION

As cyber threats against businesses of all shapes and sizes continue to become more sophisticated and prevalent, IT security spend and resources are being more heavily scrutinized and relied upon to protect organizations from attack. Increases in BYOD and mainstream IoT adoption in recent years have also added to the complexity of locking down the IT environment, and opened up even more avenues for cybercriminals to exploit individuals and businesses through system and human vulnerabilities.

With so much reliance on technology for businesses to function and remain competitive, do the economics of budgets set aside to safeguard businesses and the potential financial losses caused by a security incident stack up? To find out, Kaspersky Lab together with B2B International, conducted a global study of more than 4,000 business representatives from 25 countries, looking at their IT security budgets, the complexity of their infrastructure, attitudes towards security threats and solutions, and the real cost of data breaches and security incidents experienced.

Whilst the research revealed that budgets for IT security are set to grow by **14%** over the next 3 years, this still only accounts for a small proportion of the overall IT budget. So what does this mean in practice and is it enough to safeguard businesses against the very real threats which affect them today (and tomorrow)?

INVESTIGATING REASONS BEHIND SECURITY SPENDING

There is no denying that IT security is becoming a key priority for businesses, as the reliance on and complex nature of technology continues to grow. Indeed, for enterprises, the increased complexity of IT infrastructure was the number one driver for wanting to increase IT security spend (**48%**). **42%** of SMBs agreed, with only a quarter (**24%**) of VSBs seeing complexity as the main reason for increasing budgets, citing new business activities/expansion as the top reason (**35%**).

Despite finding it difficult to demonstrate the ROI of investments in IT security to senior management, businesses of all sizes agree that they will continue to invest in improving IT security regardless of ROI, as it is better to be safe than sorry.

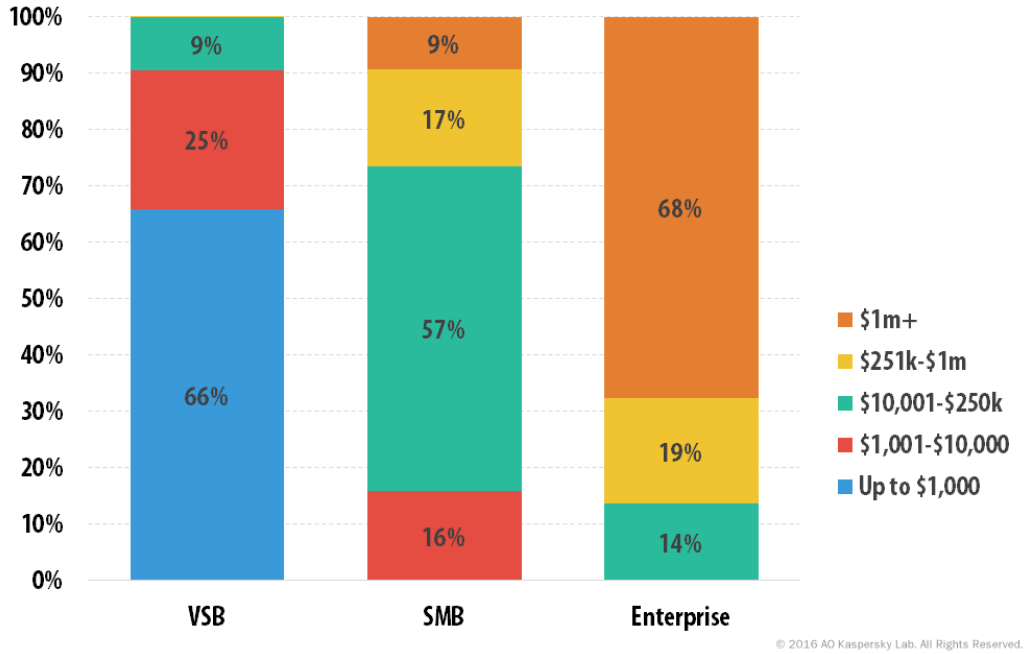
Share of businesses agreeing that they will invest in improving our IT security regardless of the ROI.

Indeed, many businesses find it difficult to demonstrate effectiveness of IT security investment to top management. Among enterprises, **51%** agreed with this statement and **49%** of small and medium businesses also experience difficulties. One of the key findings of the 2016 IT Security Risks survey is that security remains to be a contradicting topic when it comes to budget. On the one hand, the importance of protecting business data from cyber threats is understood universally. On the other, IT spending, measured both relatively and absolutely, is still low for many industries and companies of all sizes.

Currently, businesses only allocate about **17%** of their IT budget to security, with VSBs proportioning a significantly smaller amount than enterprises (**13% vs 21%**).

IT security budget figures	VSB	SMB	Enterprises
% of IT Budget Spent on IT Security	13%	18%	21%
Average IT Security Budget	$2k	$213k	$25.5m
Expected Growth of IT Security Budget (Over 3yrs)	+12.5%	+14.3%	+14.4%

In monetary terms, two-thirds (66%) of VSBs spend less than $1,000 a year on IT security compared to 68% of enterprises who spend over $1 million.



% of Businesses Whose IT Security Budget Falls Into Each Category

When drilling down into different industries, there is also huge variation in budgets. As we see, IT budgets depend on company size, but we found a way to compare different sizes of business by calculating annual investment per IT security specialist.

Industry	Defence	High IP Manufacturing	Financial Services	Transportation & Logistics	Hospitality & Leisure
Avg. IT Security Spend per IT expert	$2,369	$2,255	$2,008	$380	$318

Although there is a desire and clear, key drivers to increase budgets in this area, the predicted rise in IT security spending is a modest 14%. Looking at specific budgets for staff resources to tackle the problem the same story is true, with ambition not necessarily backed up by action.

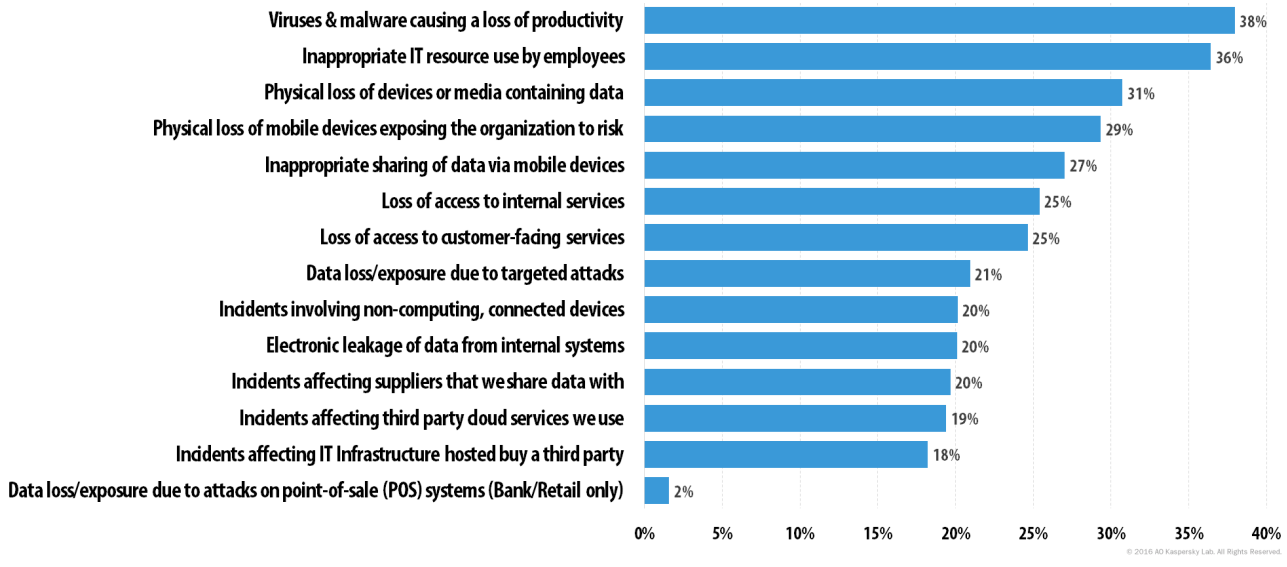
Despite a predicted rise in the number of dedicated IT security specialists over the next 3 years (22% of SMBs expect the number to rise significantly), the money to pay for this is seemingly not available or forthcoming, with only 10% of organizations expecting the proportion of IT security budget spent on wages will increase accordingly.

MEASURING FINANCIAL IMPACT OF SECURITY BREACHES

So with IT security expectations often failing to materialize, will the real cost of a security incident give businesses the wake-up call they need to reassess IT security spending and ensure that available budgets are being allocated in the right way?

For most businesses, spending on IT security can be a mere drop in the ocean when compared to the actual cost to a business of a security incident or data breach. The impact is felt not just in financial terms but through reputational damage, which could affect the long-term prosperity and success of a business.

With over half (52%) of all businesses assuming that their IT security will be compromised at some point, being prepared and using budgets to best effect is essential. Over the past 12 months alone, over a third of businesses (38%) have been affected by viruses and malware causing a loss of productivity, and experienced inappropriate IT resource use by employees (36%). One in five (21%) has experienced data loss or exposure due to targeted attacks.

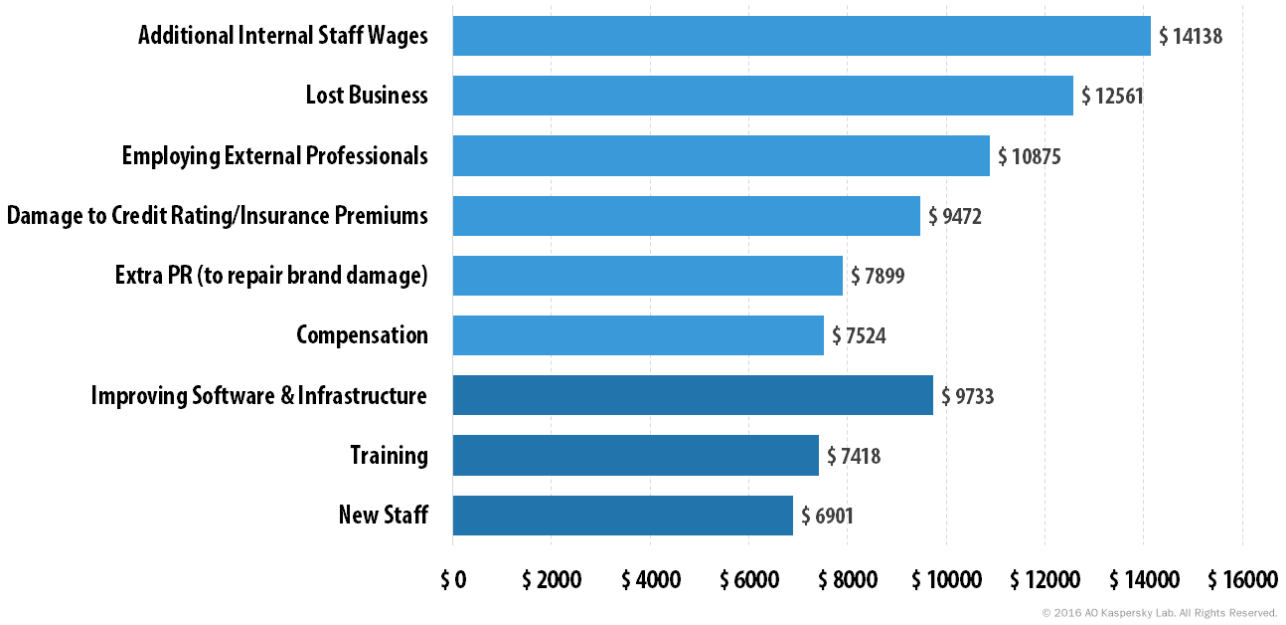


Types of security event experienced in the past 12 months (% of all businesses experiencing each type of attack)

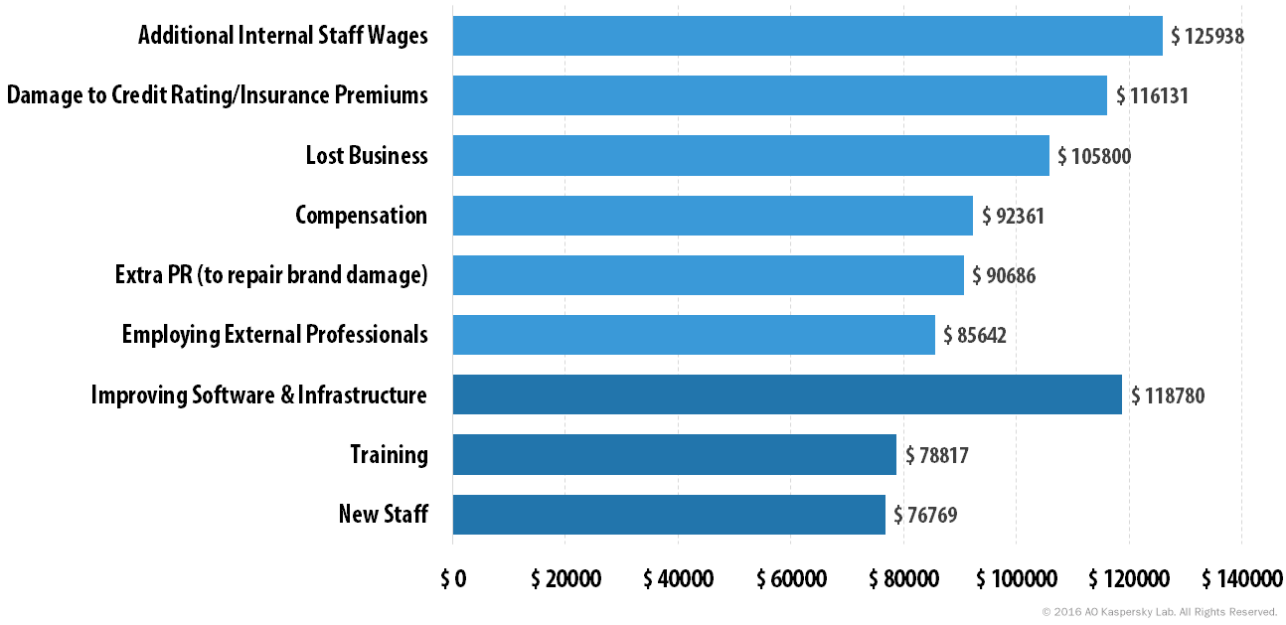
Whilst these figures alone provide good evidence to support increased spend and resource on cyber threat prevention and recovery, it is only when faced with the real costs of these types of incidents does it put it into clear perspective.

For all of the incidents experienced by businesses, almost half (43%) resulted in a data breach, loss or exposure of some kind. Putting this into context, the average financial impact of a single data breach and attack vector for an SMB is an estimated $86.5k and for enterprises a staggering $861k. The reallocation of IT staff time represents the single largest additional cost for both SMBs and enterprises within this estimate.

The breakdown of an average financial impact of a data breach

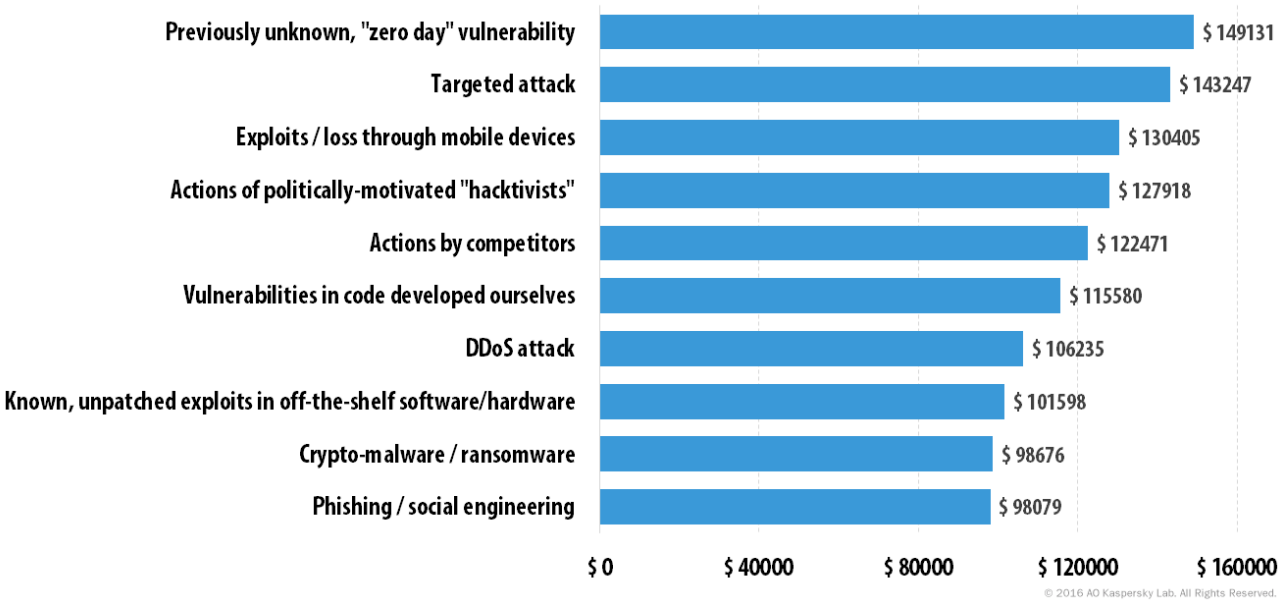


SMB

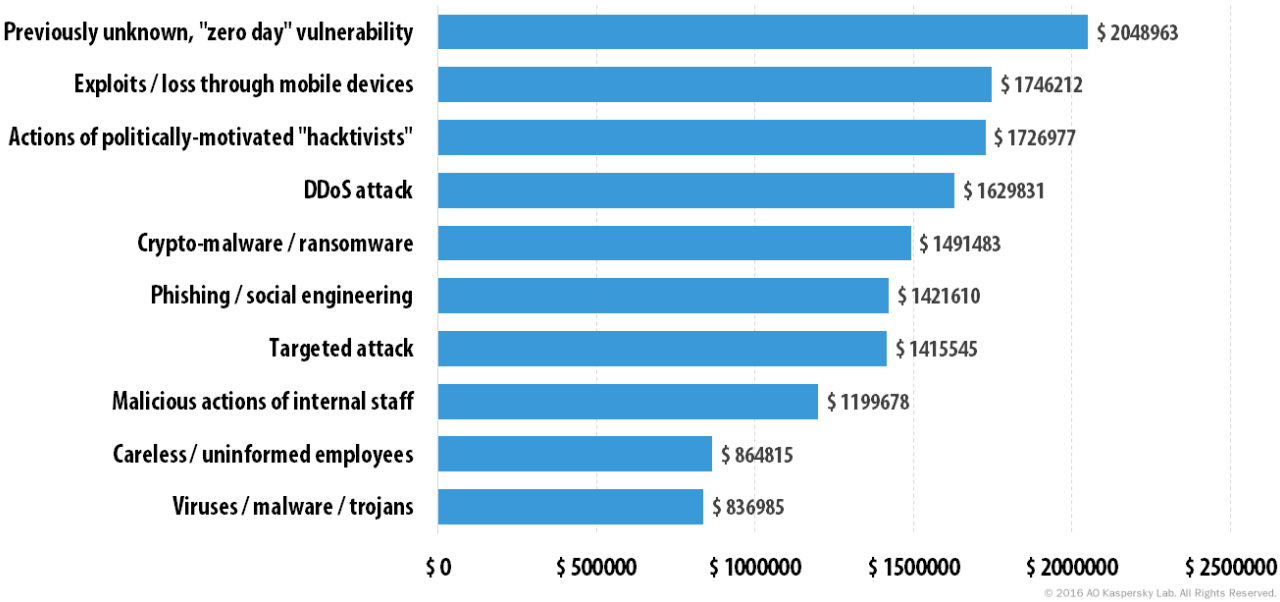


Enterprise

But this is just the average across a range of attack vectors, with some types of attacks costing a business more. Previously unknown "zero" day vulnerabilities – whilst rare - have cost SMBs an estimated $149k and enterprises $2m, with targeted attacks resulting in a financial impact of $143k and $1.7m respectively. Where multiple attacks are coordinated and comprise more than one vector, businesses can be hit even harder. This is especially true for enterprise-level organizations whose total financial impact for an attack consisting of three or more vectors is estimated to be $1.7m (compared to $117k for SMBs).

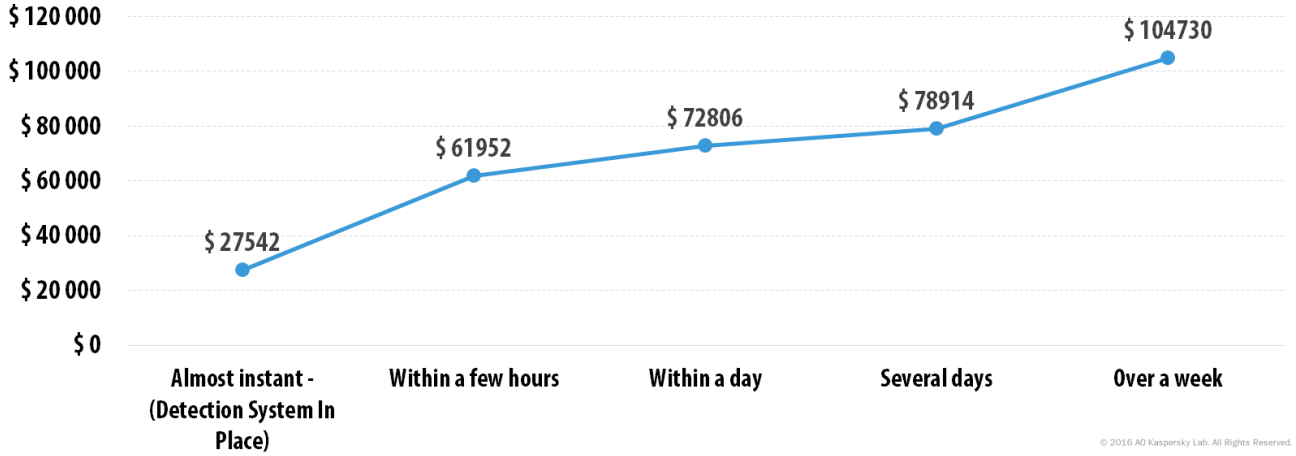


Top ten most 'expensive' security incidents for SMBs

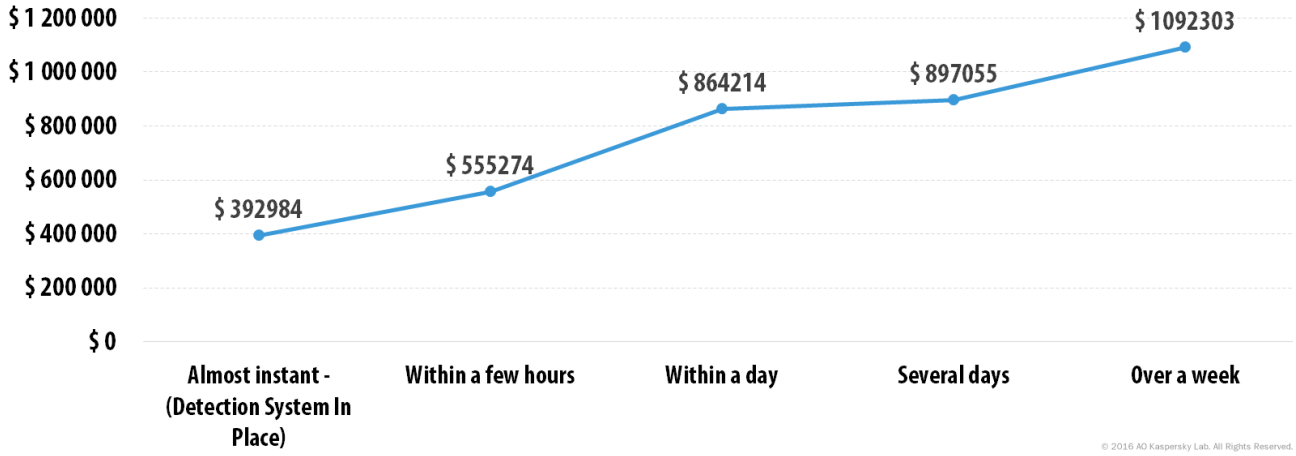


Top ten most 'expensive' security incidents for enterprise

In all cases, the financial impact has been seen to increase with time, with rapid detection of a data breach a key factor in minimizing not only data loss but the financial cost to the business. The longer a breach goes unnoticed, the more it will cost a business in monetary and data integrity terms. Even when breaches are detected almost instantly, SMBs estimate a cost to their business of $28k, rising to $105k if undetected for more than a week. For enterprises, where a detection system is in place the estimated financial damage is still $393k, increasing to over $1m if it remains undetected for over 7 days.



Cost of recovery vs. time needed to discover a security breach, for SMBs



Cost of recovery vs. time needed to discover a security breach for enterprises

Data itself is also more vulnerable the longer a breach goes unnoticed, with an average of 417 sensitive customer/employee records compromised per incident - even with instant detection - and over 70k at risk if undetected for more than a week.

When we compare the average annual IT security spend of SMB and enterprise businesses with the estimated losses of just a single attack, we start to get a real sense and scale of just how tight budgets are and that there is little room for error in how the budget is allocated. Taking the average SMB IT security spend of $213k, and comparing it with the average cost of an attack ($86.5k), SMB IT security provisions only need to prevent 2.5 attacks before they are saving the business significant funds, not to mention reputational damage.

With businesses aware of network vulnerabilities and expecting them to be exploited, the prevalence and success of cyber attacks against businesses is only going to rise. But with IT security budgets only set for a modest increase over the next few years, the financial impact could become even more severe.

CONCLUSION

Whilst cyber attacks are inevitable, the way businesses use available budgets and resource will be vital in the coming years, in keeping the financial (and reputational) impact down. Whilst losses will occur as a result, the key is to minimize them. This is our aim and on average, Kaspersky Lab customers who do suffer a breach experience much less severe financial consequences than our competitors – 30% less for SMBs and 18% less for enterprise customers.

The financial impact can only be curbed by taking a holistic approach to IT security instead of relying just on detection technology to do the job. It is encouraging to see that 45% of companies believe that hardware and software alone won't necessarily solve all IT security incidents. But although this is the case, it is not necessarily backed up by the right resources to provide total protection – with 73% still believing that workstation security software alone is effective.

As evidenced in the research, education of employees should form a key part of a company's arsenal in minimizing the likelihood of cyber attack. With careless employees the second biggest cause of security incident in the past 12 months and the single biggest cause of serious incidents involving data loss or leakage, training and education on cyber threats is vital to creating a savvier and less vulnerable workforce.

Alongside detection technology, clued up and vigilant staff who are more informed and aware of the risks facing businesses today and tomorrow will help improve detection and minimize impact. However, when assessing where security budgets are to be spent, there is a general reluctance on the part of businesses to accept outside help – with only 18% of organizations considering better insights and intelligence on threats as a top method to improve detection.

Despite this feeling, without the benefit of insight and intelligence, organizations will remain unable to improve detection and combat the growing number and severity of cyber threats. Only by moving beyond prevention towards recovery and mitigation will organizations be able to reduce their risk and the inevitable financial consequences of a cyber attack.

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy