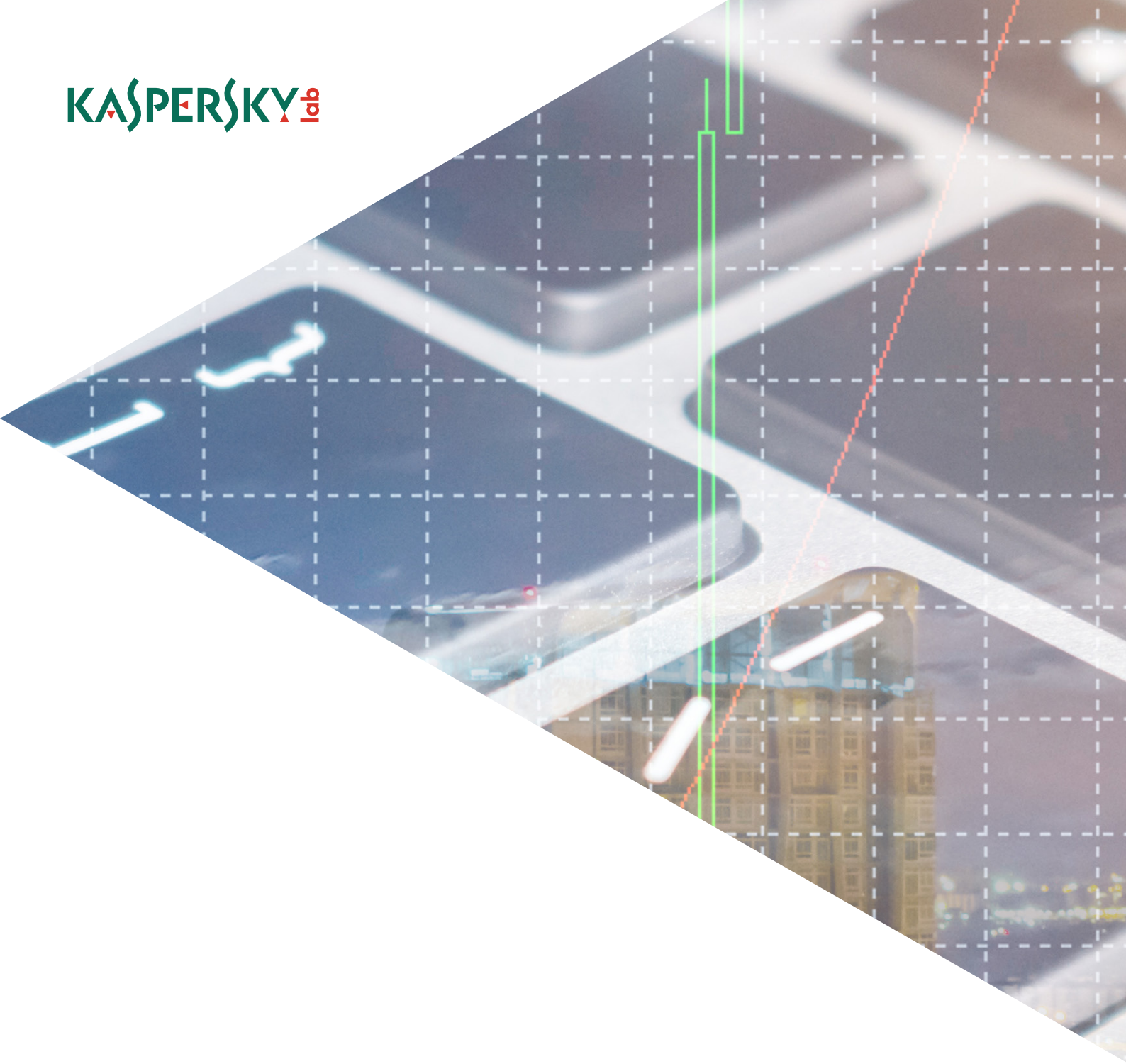


THE FINANCIAL IMPACT OF IT SECURITY ON US BUSINESSES

IT Security Risks 2016
Kaspersky Lab

CONTENT

INTRODUCTION

As more and more information worldwide rapidly migrates into digital form and the ways in which it is accessed and created continues to evolve, so too are the risks from cyberattacks. As a result, cyber security is now a global agenda item for governments, regulators and businesses alike, and more than ever, IT security spend and resources are being heavily scrutinized as they become relied upon for protection.

In the US, BYOD adoption is commonplace - with Gartner suggesting that companies in the United States are twice as likely to allow BYOD than those in Europe - and IoT usage is continuing to rise. But for all of the evolution within the technology landscape in recent years, the associated vulnerabilities and complexities are also rising and not to be underestimated.

To assess the state of the security landscape in the US and across the globe, Kaspersky Lab has partnered with B2B International to find out if the level of budgets set aside to safeguard businesses correlate with the potential financial losses caused by a security incident. The global study of more than 4,000 businesses from 25 countries explores IT security budgets, attitudes towards security threats and solutions, and the cost of data breaches.

For US businesses, an overwhelming majority (**75%**) expect to increase their IT security spending in the next three years, with a third (34%) of companies expecting a rise of between **10%** and **29%**. But is this intention and allocation enough to tackle the very real threats that target US organisations of all sizes?

UNCOVERING BUDGETS

As businesses become more reliant on technology for day-to-day operations, interactions and communications, more emphasis is being placed on IT security to protect the platforms and infrastructures on which we depend. We found that the main driver for increased security budgets in the US is new business and company expansion. Indeed, nearly half (**46%**) of US companies agree that expansion is the main reason for increased budgets, compared to just over a third (**37%**) of companies around the world. The second most popular reason was increased complexity of IT infrastructures (**39%**).

Despite an understanding of the need to increase budgets to meet changing business requirements and an evolving technology landscape, over a third (**35%**) of businesses in the US still find it difficult to secure the spend required to protect their organisation from security threats. This compares to half (**47%**) of all businesses globally. Indeed, when talking about the challenges of implementing IT security measures, over a third (**37%**) say it is difficult to demonstrate the return-on-investment (ROI) of IT security to senior management.

However, US businesses are in agreement with the rest of the world, with over half (**57%** US, **56%** globally) stating that they will continue to invest in improving IT security regardless of ROI, as it is better to be safe than sorry.

When it comes to the reality of IT security spending, when put into context, it still only accounts for a small proportion of the total IT budget, with understanding not necessarily translating into action. In the US, most companies (**73%**) said they spend less than **20%** of the IT budget on security. Although this is higher than the global average of **69%**, in real terms this amount can be nominal, with 1 in 10 US businesses (**10%**) spending less than $2,500 on total IT provision every year (compared to 8% of businesses globally).

For many US companies, they see IT security defences coming in the form of people power – with almost two-thirds (**64%**) expecting the number of IT security specialists employed by their organisation to increase over the next 3 years. Although this is slightly less than the global average (**68%**), over half (**58%**) of US businesses expect the proportion spent on hiring and paying internal IT security specialists to increase, compared to **54%** globally.

COUNTING THE COSTS

When weighing up budgets, most businesses are aware that the actual costs of a security incident or data breach can be huge in comparison, in terms of financial and reputations consequences – with many already having suffered at the hands of an attack.

Over half (**49%**) of US businesses (**52%** globally) assume that their IT security will be compromised at some point. Our research found that over the past 12 months, a third (**34%**) of US businesses have been affected by viruses and malware causing a loss of productivity and **32%** have experienced inappropriate IT resource use by employees.

The physical loss of devices containing data can also have serious consequences. Over a quarter (**27%**) of companies in the US admit that they have experienced the physical loss of devices or media containing data, and for just under a third (**30%**) of respondents, the physical loss of mobile devices has exposed the organization to risk.

When faced with the real cost of these types of incidents, it only serves to highlight the importance of being prepared and using budgets to best effect. Our research uncovered that over three quarters (**77%**) of US businesses have suffered between 1 and 5 separate incidents of data loss, leakage or exposure in the past 12 months (compared to **82%** globally).

As a result of such incidents, **14%** of US businesses have lost access to critical business information for a week (compared to one in ten (**10%**) businesses globally), with **13%** being prevented from trading completely for more than seven days. For one in ten (**10%**) US businesses it can take up to a year to discover that a breach has occurred. This lack of awareness and preparation for what the majority see as an inevitable consequence of our complex technology landscape, can have untold financial implications.

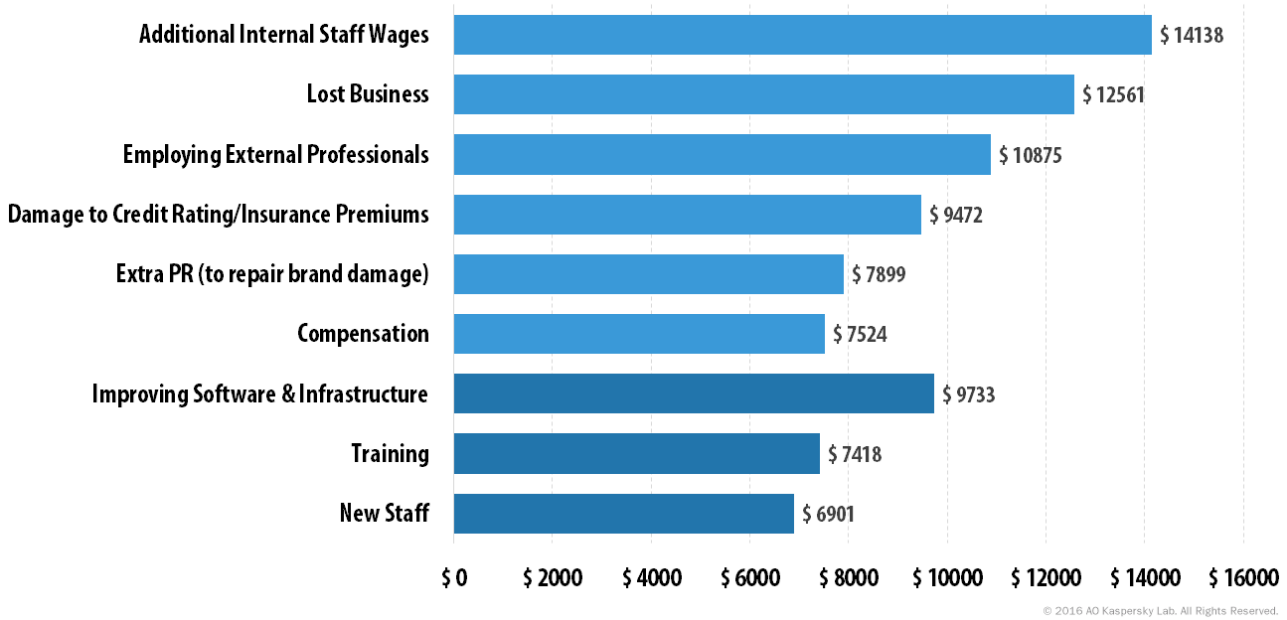
Putting this into context, the average financial impact of a single data breach and attack vector for an SMB is an estimated **$86.5k** and for enterprises a staggering **$861k**. The reallocation of IT staff time represents the single largest additional cost for both SMBs and enterprises within this estimate.

The research uncovered just how tight budgets are and how there is little room for error in the allocation of resources to IT security by comparing the average annual IT security spend of SMB and enterprise businesses with the estimated losses of just a single attack. Taking the average SMB IT security spend of **$213k**, and comparing it with the average cost of an

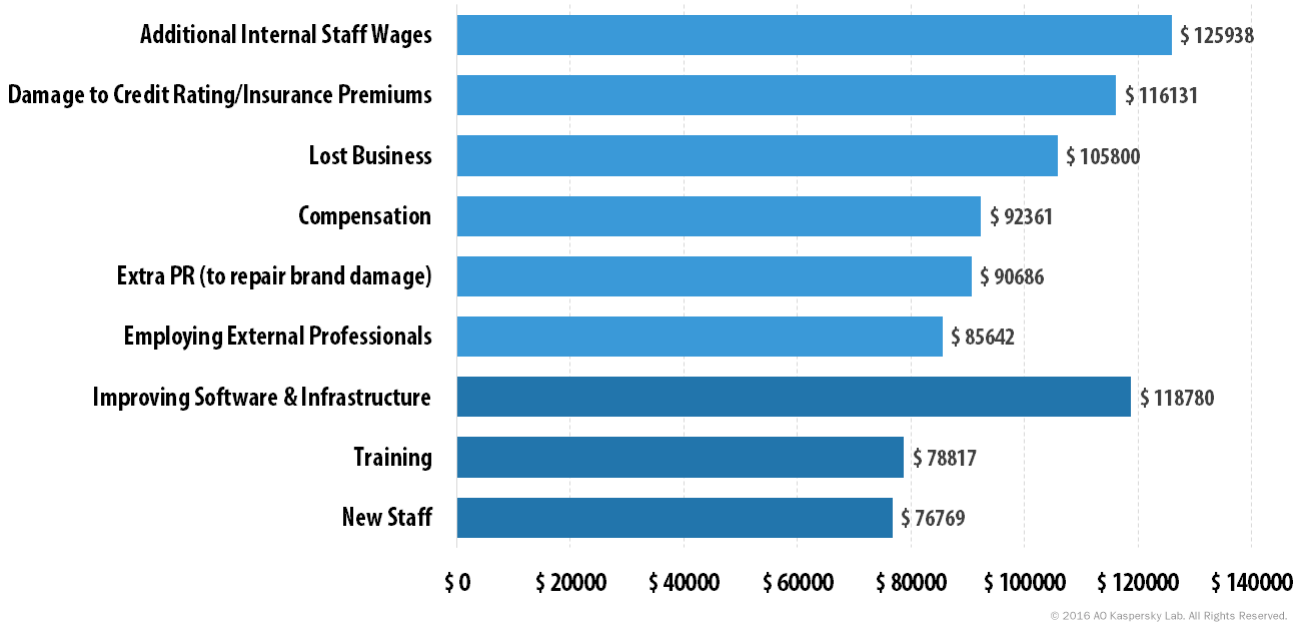
attack (**$86.5k**), SMB IT security provisions only need to prevent **2.5** attacks before they are saving the business significant funds, not to mention reputational damage.

The breakdown of an average financial impact of a data breach

SMB



Enterprise



CONCLUSION

The financial impact of cyberattacks must be seen in the context of the resources that are put in place to combat them. US businesses recognise the need for boosting IT security in the face of increasingly prevalent attacks - with **26%** seeing more internal IT and IT security staff as the answer in the next 12 months, and **41%** considering more sophisticated IT security software as the saviour – but it seems the budgets are not necessarily there to support that.

With IT security budgets only set for a modest increase over the next few years, there is a conflict emerging within US businesses which pits IT security spending against day-to-day operational realities. Business and technology leaders must ask themselves whether small budget increases are enough to combat increasingly sophisticated cyber attacks?

The key to successfully reducing the impact is to take a holistic approach to IT security, instead of relying just on detection technology to do the job. A key part of reducing risk and gaining a real return on any investment in IT security – be it staff or software - is education and intelligence. After all, to be forewarned is to be forearmed and only by moving beyond prevention towards recovery and mitigation will organizations be able to reduce their risk.

Contact us at: intelreports@kaspersky.com (Kaspersky Security Intelligence Service)

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