KASPERSKY lab

IT Security: Cost center or strategic investment?

Investigating the new business attitude towards IT security budgets

Table of Contents

Introduction

The cyber landscape is continuing to evolve at a steady pace and businesses across the globe are having to constantly adapt to keep up. No matter what sector or sized business you operate in, it's likely that security is becoming an increasingly important part of your organization's IT budget.

The Kaspersky Lab Global Corporate IT Security Risks Survey is an annual study that provides an update on the state of IT security within organizations across the world. Now in its seventh year, this study builds upon the findings of our previous reports, asking important questions about IT security spend, the cyberthreats businesses are up against, and the financial impact of being targeted by these threats. The study also monitors how businesses around the globe are reacting to changes in the global cyberthreat landscape by questioning business decision makers about their attitudes toward IT security budgets.

This year, we considered the important question – do businesses view IT security as a cost center (a necessary evil that they must stump up the cash for), or are they starting to consider it as a strategic investment (something crucial to their business continuity in the face of growing threats, and which brings measurable benefits)?

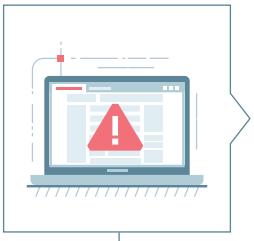
Our study has found that IT budgets are being squeezed on a global scale. While the proportion of IT budgets spent on IT security is rising globally – from an average 17% in 2016 (16% in North America) to 20% (18% in North America) in 2017, still, the absolute figures are falling dramatically globally, with an average IT security budget reaching $25.5M for enterprises last year and just $13.7M this year.

With their budgets under pressure, IT security teams are facing a real challenge – having to do more with less, while the threats continue to rise. With the overall reduction of IT budgets and increasing number of incidents, protection might soon become an issue for businesses around the globe. Crucial to their success, will be their attitude towards IT security spend. This report delves deeper into the threats faced by businesses large and small, and IT security spending habits.

Background and methodology

The Kaspersky Lab Corporate IT Security Risks Survey is a global survey of IT business decision makers which has been conducted annually since 2011. The most recent wave of data was collected in March and April of 2017, with a total of 5,274 interviews conducted in over 30 countries and across businesses of all sizes. Throughout the report, business sizes will sometimes be referred to as VSBs (very small businesses with fewer than 50 employees), SMBs (small- and medium-sized businesses with 50 to 999 employees) and enterprises (businesses with over 1,000 employees). Not all survey results are included in this specific report and more results will be announced throughout the year.

Key findings for the North American region



Cyberthreats are becoming harder and more expensive to fight for companies of all sizes in North America. Among SMBs the average total impact of a data breach amounts to $117K, but this is more than ten times higher for enterprises ($1.3M).

The proportion of IT budgets which is spent on IT security continues to rise in North America. Businesses on average spent 16% of budgets on IT security in 2016 and today, they are spending 18%. This is a pattern that is consistent across businesses of all sizes, except enterprises with over 1,000 employees, where the IT security budgets stagnate, according to the research.

With data breaches getting more expensive to recover from in North America, protection might soon become an issue for firms that do not prioritize IT security spend. SMBs tend to suffer the biggest financial loss from losing business ($21K) and having to employ external professionals ($21K) when a data breach occurs, while enterprises spend the most on additional internal staff wages ($207K).

Businesses in North America sometimes cite pressure from key stakeholders –including shareholders, investors (11%) and customers (23%) as a reason to increase their IT security spend. This suggests that some businesses at least, are starting to view IT security spend as a strategic investment, but not every business sees it that way. This year more companies admitted that they will invest in cybersecurity regardless of ROI – with 60% in 2017 compared to 59% in 2016.

The cost of IT security incidents

The cost of cybersecurity incidents is changing, with businesses having to deal with multiple considerations – from PR to new staff – in the aftermath of a breach. This year we have seen a continued evolution in the financial impact of a data breach with the recent Equifax breach for example. This in turn, will have a knock-on effect on whether businesses view their cybersecurity spend as a cost center, or an investment that will help them avoid the larger financial penalties associated with an attack.

Serious data breaches are getting more expensive

The attacks that make business decision makers worry – such as those against the National Health Service (NHS) in the UK, Sony, or HBO's recent leak of confidential Game of Thrones files – are generally massive in scale and involve millions of records. But these are the exception rather than the rule. Most cyberattacks on businesses don't exactly make the headlines. In fact, aside from possibly being mentioned in media, they go largely unnoticed.

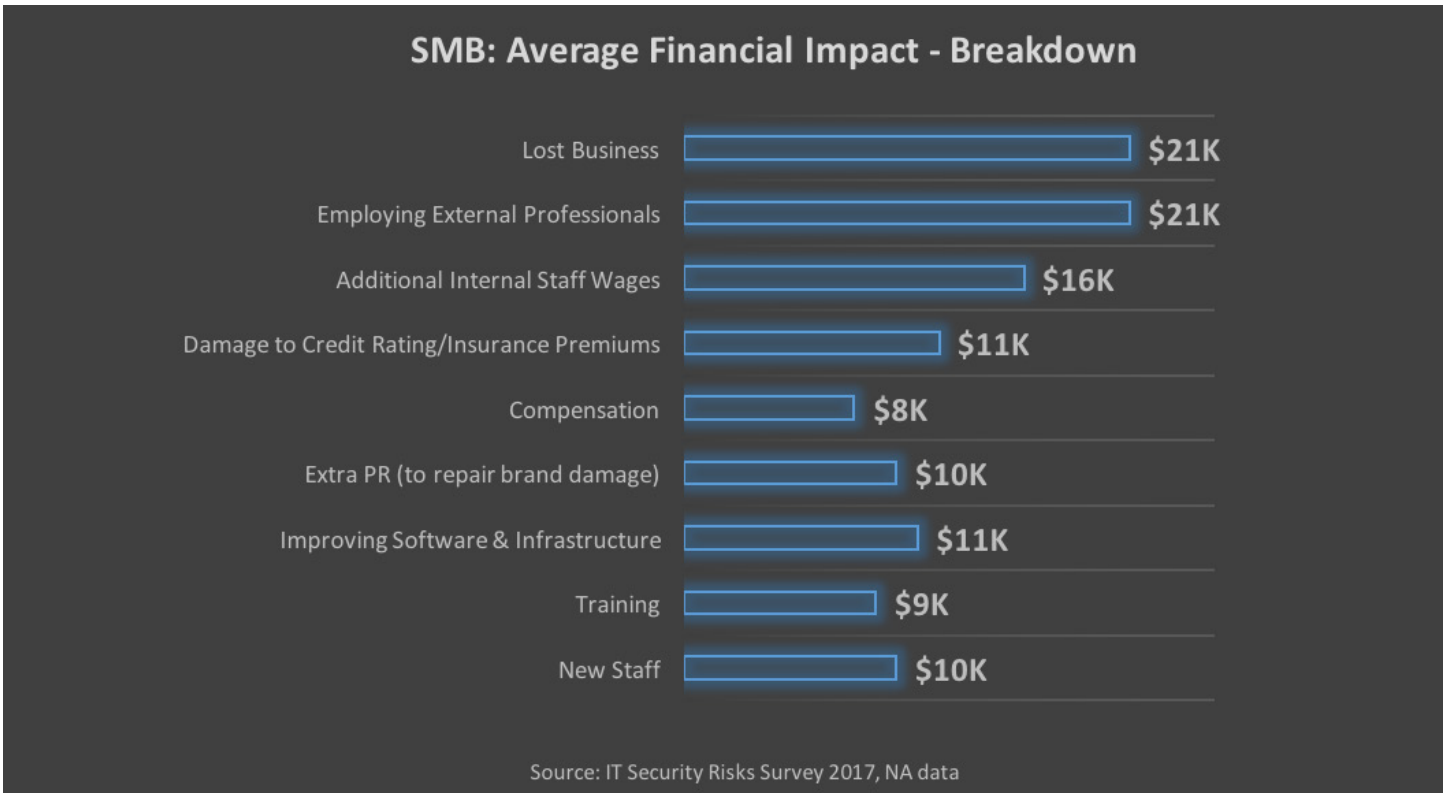
Yet, despite slipping under the radar, and despite their size, the majority of smaller attacks can still be extremely damaging to the businesses they affect. So, how much can businesses expect a "typical" data breach to cost? Our study asked organizations to estimate how much money they had spent or lost in the aftermath of a data breach experienced within the last 12 months.

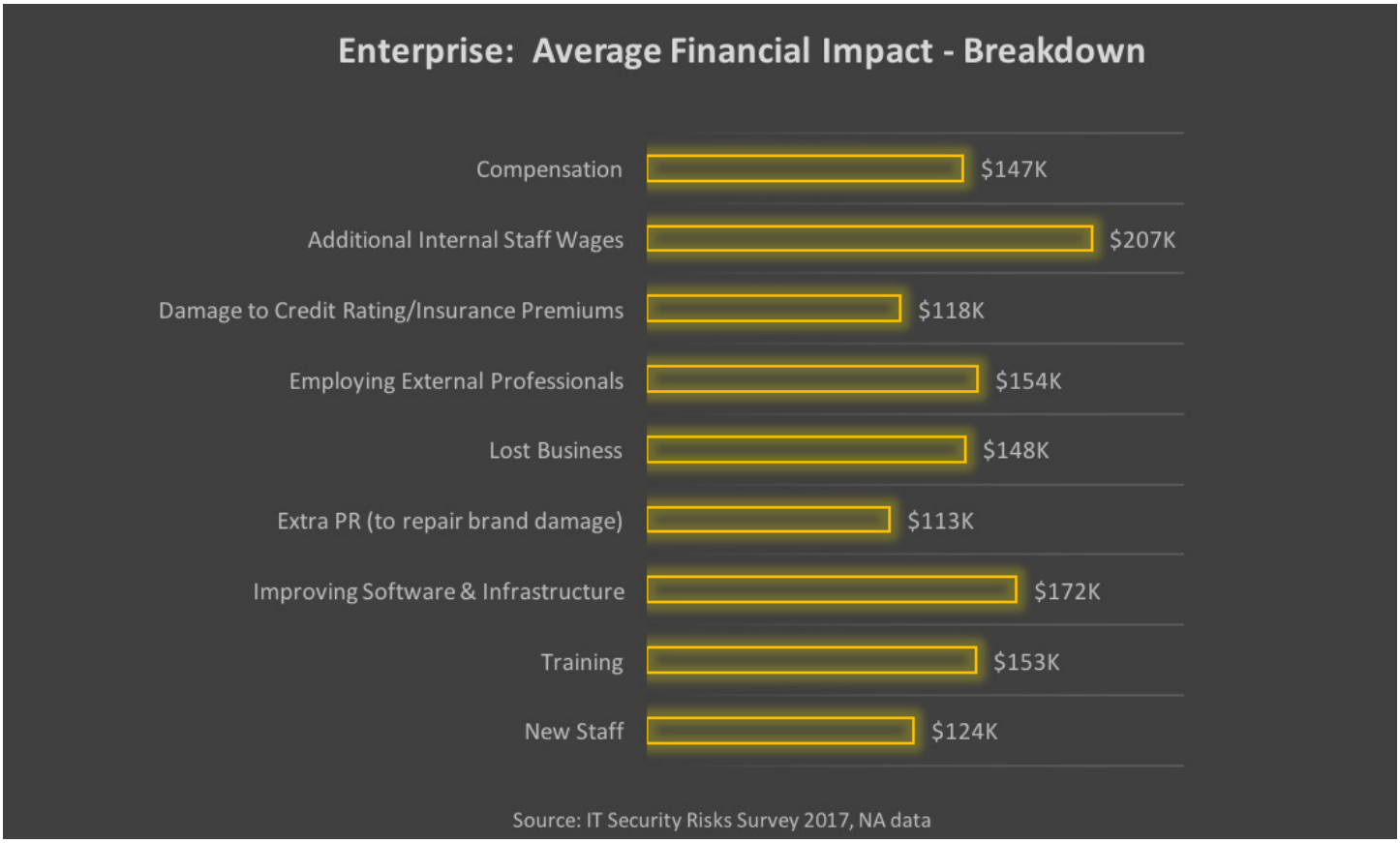
All businesses with **50 or more employees** were asked to **estimate the costs** they incurred in each of the following categories, after a breach:

Additional Internal Staff Wages +
Lost Business +
Employing External Professionals +
Damage to Credit Rating/Insurance +
Extra PR +
Compensation +
Improving Software/Infrastructure +
Training Staff +
Hiring New Staff +
= **Total Financial Impact**

The figures were then added together to provide an **estimate of the total financial impact** for that organization and an average cost was calculated across these businesses to gain an estimate of the **typical cost of data breaches for businesses**.

We have shown results separately for SMBs and enterprises below, as the picture is very different for different sized businesses in the North America. Among SMBs, for example, the average total impact of a data breach amounts to **$117K**, and this is more than ten times higher among enterprises spending on average **$1.3M**, which demonstrates that cyberthreats are expensive to fight for companies of all sizes.





While it's not surprising that the average total financial impact of a data breach is much higher for enterprises than for SMBs, it is interesting to see how the costs break down.

Whereas last year we saw that the reallocation of staff time representing the single largest additional cost for both SMBs and enterprises, this year the picture has changed, with SMBs and enterprises having different experiences.

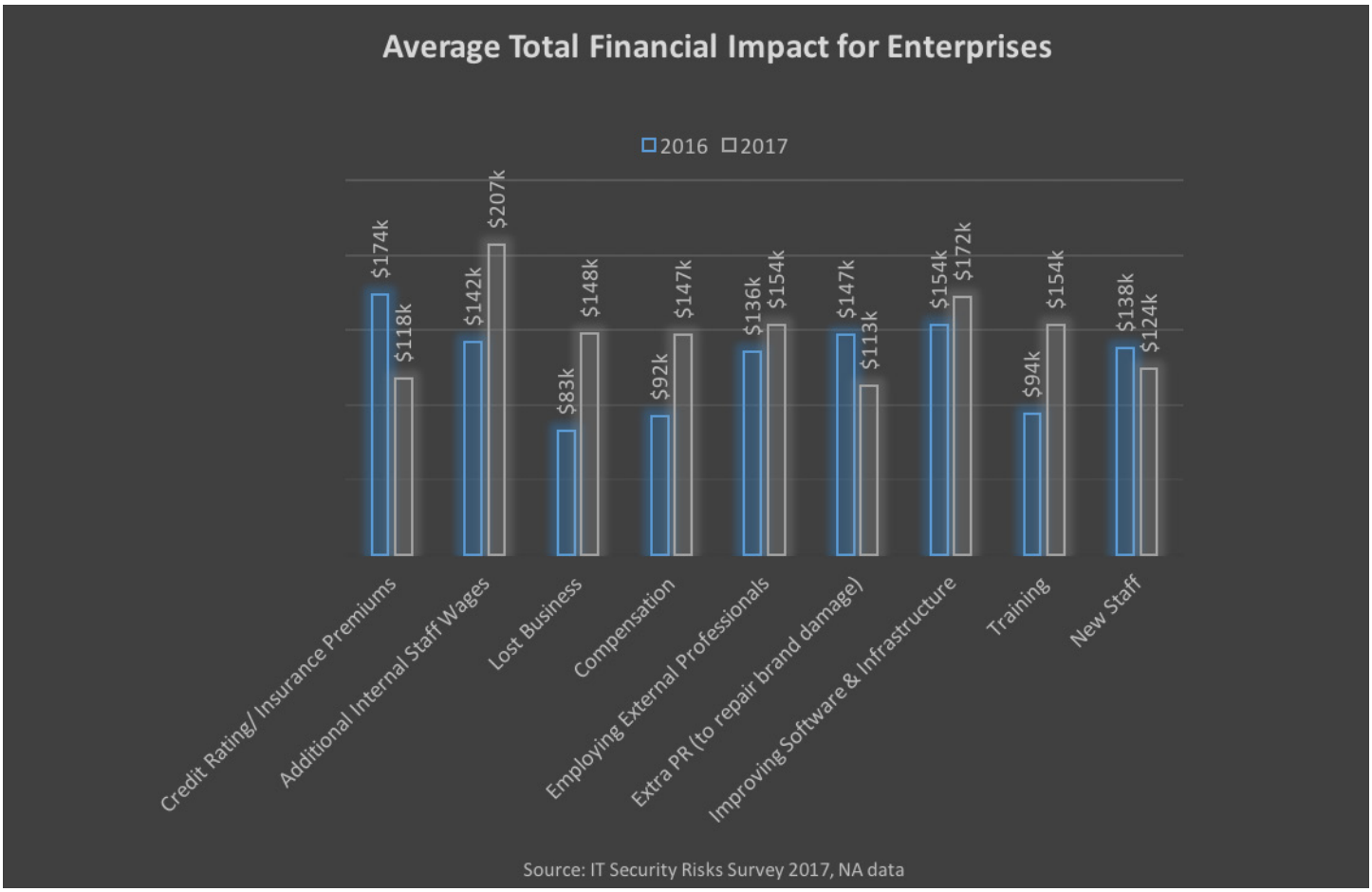
In North America, the top pain points for SMBs in 2017 include **lost business** ($21K) and **costs related to employing external professionals** ($21K), while compensation was one of the lowest figures. By contrast, enterprises in North America incur the largest costs due to additional internal staff wages ($207K) and **improved software/infrastructure** ($172K).

In addition, spend on training in the aftermath of a security breach is particularly expensive for enterprises – at $153K on average – with businesses realizing the need to increase the cybersecurity knowledge of their staff, once they have been stung by a security incident.

The different costs experienced by enterprises and SMBs directly reflects the current capabilities of most organizations of these sizes, with smaller businesses clearly struggling to deal with the problem themselves and therefore seeking third-party expertise. At the same time, they are vulnerable to losing business as a result of these attacks, but are less likely to need to pay compensation (possibly due to the less formal nature of their business relationships).

For larger businesses, their greater internal capabilities change the balance between the money spent on responding to the threat, and the damages suffered. Compensation, however, remains a serious concern, with an average $147K spent on compensation per data breach.

The average cost of a data breach has risen by 11% for enterprises globally in 2017. Overall in North America, the average cost of a data breach for enterprises grew this year from $1.2M in 2016 to $1.3M in 2017.



The financial impact of evolving legislation

Cost rises are likely to continue as governments rush to introduce new legislation, requiring businesses to publicly announce data breaches that they experience, and provide better transparency about how they protect personal data.

Developing and enacting laws takes time, and this is a huge problem in the face of such a rapidly changing business IT landscape and the proliferation of cybersecurity threats. For example, the Japanese legislation was agreed upon in 2015 but has taken two years to come into force. And indeed, it is worth noting that for many, the legislation came too late, as there were a number of high profile failures among Japanese firms in the interim. One example is that of travel agency JTB Corp., which experienced a massive data breach in 2016, resulting in almost eight million customers having their details (including names addresses and passport numbers) stolen.

This is symptomatic of a wider global challenge – with threats moving fast, but businesses and legislation changing slowly. Yet another example is that of the impending European General Data Protection Regulations (GDPR), which will be enforceable in May 2018, and which will greatly limit how businesses treat EU citizen data.

With legislation changing across the world, and cyberthreats evolving faster than these regulations, businesses need to remain mindful of the gap between legislation and reality, and prepare their defences accordingly, if they are to protect their customers and their reputations. They need to start thinking about being compliant with new regulations ahead of deadlines - for the security of their data and that of their customers - rather than waiting for legislation to catch up with them before changing their policies or worrying about GDPR fines.

Their weaknesses are yours too: paying for partners' cybersecurity failures

It is also important to take a closer look at the types of attack vectors cybercriminals employ, in order to achieve these data breaches in the first place. This, in turn, will help us to understand which types of attacks typically result in the most expensive data breaches.

Our study found that, for SMBs, the incidents expected to have the most severe financial impact were:

1. Targeted attacks ($188K)
2. Incidents involving non-computing connected devices ($152K)
3. Physical loss of devices or media containing data ($83K)
4. Inappropriate IT resource use by employees ($79K)
5. Viruses & malware ($68K)

By comparison, the picture is somewhat similar for enterprises but with some differences:

1. Physical loss of devices or media containing data ($2.8M)
2. Incidents affecting IT infrastructure hosted by a third party ($2.2M)
3. Electronic leakage of data ($1.9M)
4. Inappropriate IT resource use by employees ($1.1M)
5. Viruses & malware ($519K)

What's immediately clear is that often attacks which result from the security failures of business partners are amongst the most damaging to enterprises. This is clear in the experiences of businesses working with third parties for their cloud or other infrastructure, and also among enterprises that share data with suppliers.

As soon as you give another business access to your data or infrastructure, their weaknesses become your weaknesses. However, as we've seen earlier, this is not something that most organizations give proper consideration to. As such, it should not be a surprise that these incidents can be so devastating; as any boxer will tell you, it's usually the punch you don't see coming that knocks you out.

Another type of attack that stands out in the SMB sector is incidents affecting non-computing connected devices. The Internet of Things (IoT) is the most rapidly expanding area of data traffic around today, and is another example of how the potential weak points of business security are increasing. In particular, the widespread use of factory default passwords and weak security measures employed on IoT devices has made them ideal hosts for botnets like Mirai, which are capable of harnessing huge numbers of vulnerable devices, to conduct large scale DDoS attacks on critical targets.

North American SMBs that experienced attacks on their non-computing connected devices also reported particularly large increases in their insurance premiums and related costs. It seems that even insurance companies have been underestimating the risk these sorts of attack pose. Additionally, the reassessment of insurance premiums following an attack could reveal gaps in a business's security which can be expensive to fill. The weaknesses in these devices, can be a business's weakness too.

Investing in reducing the risk

As our study has shown, IT security threats are clearly significant and growing. In the face of these threats, and at the crux of the debate about whether IT security is viewed as a cost center, or a discipline that can deliver real value to a firm, are the IT security budgets themselves.

These demonstrate the attitude businesses have towards IT security, the value business leaders place on the discipline of protection, and also how much they are willing to risk.

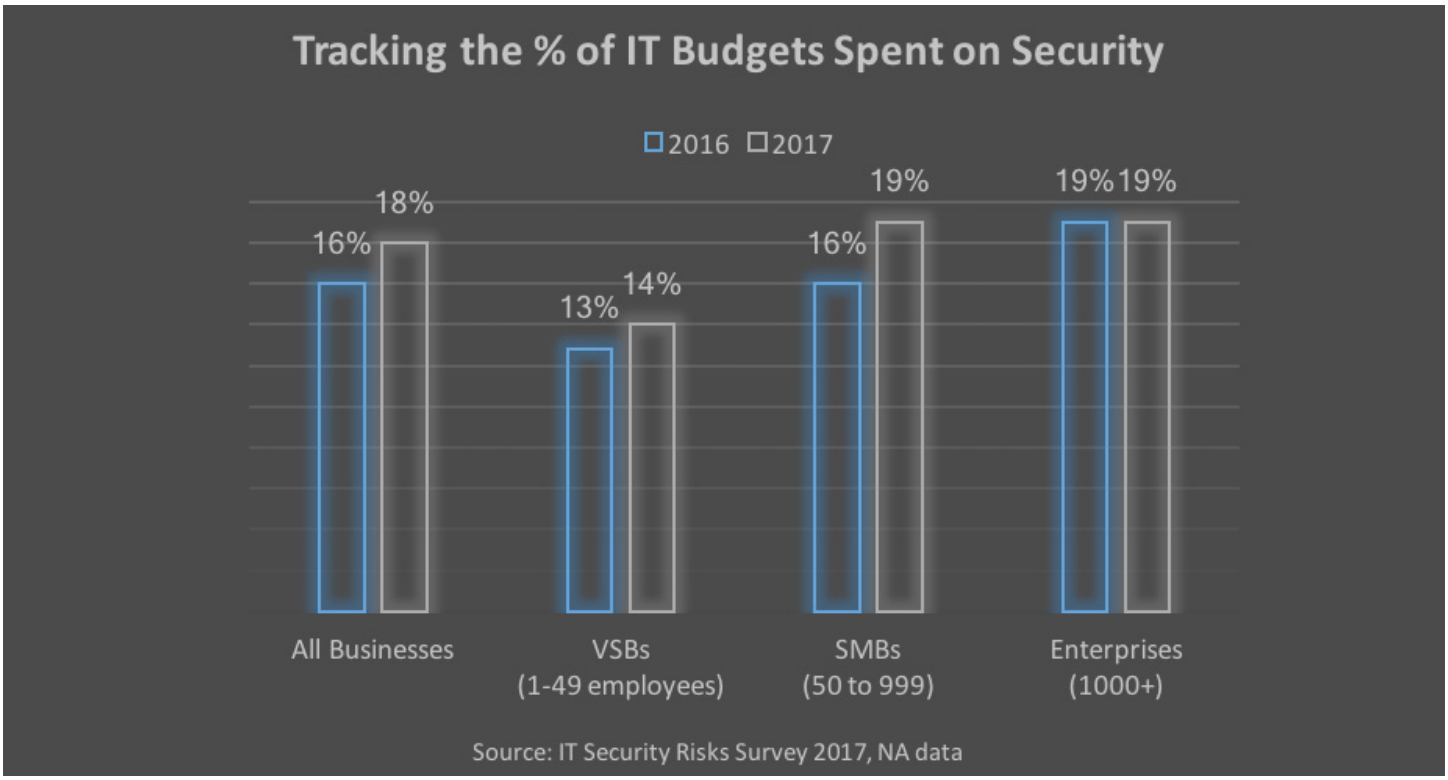
IT security budget: a larger part of a smaller pie

This year, we've seen that cost saving and outsourcing efforts appear to have resulted in a reduction in overall IT budgets among larger businesses worldwide. Despite this (or perhaps because of it) the proportion of IT budgets which is spent on IT security is rising. This is a pattern that is consistent across businesses of all sizes globally but particularly among enterprises with over 1,000 employees, where the IT security budgets have risen from an average fifth of the overall IT security budget to almost a quarter in the last 12 months.

As for North America, even among very small businesses, where resources are in short supply, the percentage of IT budget which is going towards security has risen – from an alarmingly small 13% in 2016 to a slightly healthier 14%.

This represents a healthy growth in the importance being placed on IT security – something promising and indeed necessary, if businesses are to start viewing IT security as an investment rather than a cost center.

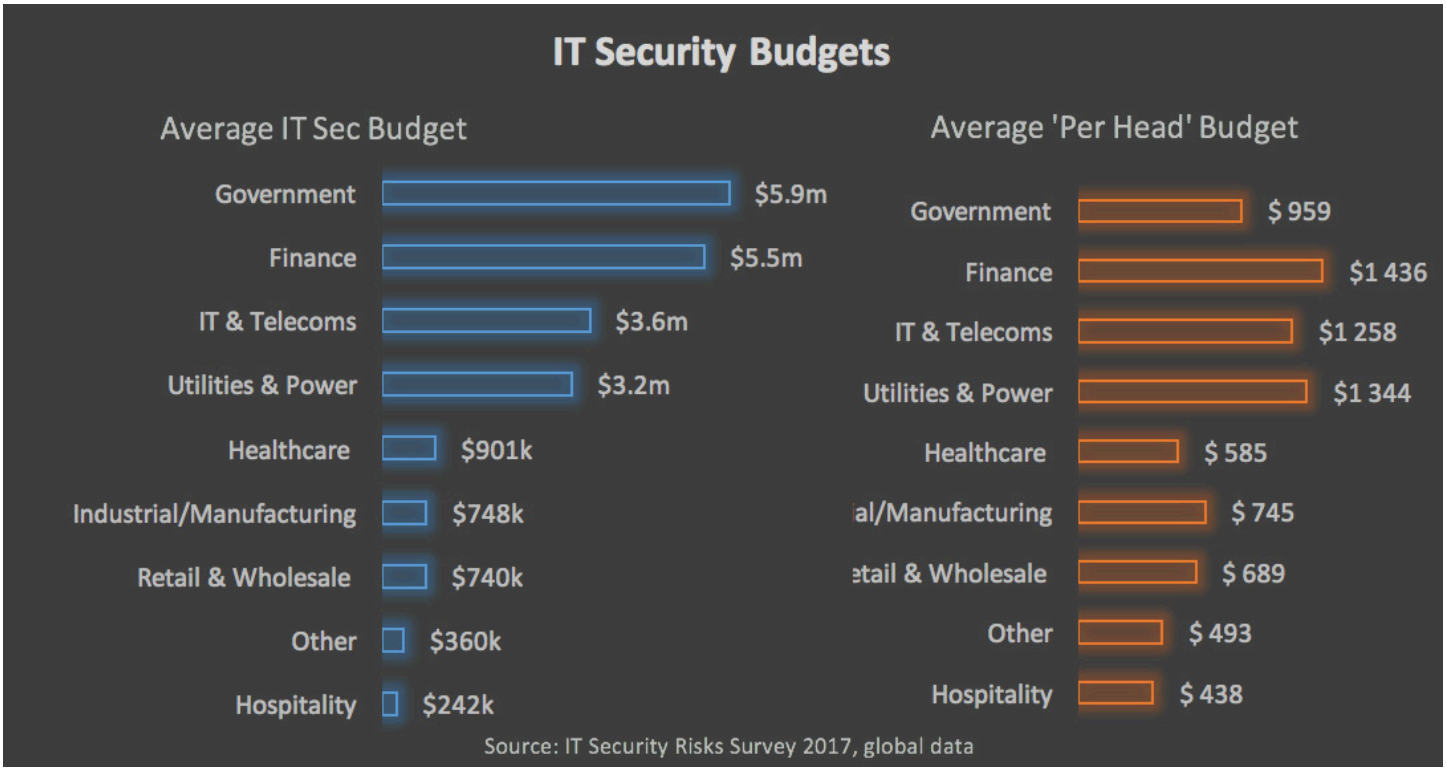
Nonetheless, the North American study does still demonstrate a stagnation in IT security budgets among enterprises. This is a concern when the stakes are high, and when the prospect of an attack is an expensive one.



IT security top spenders worldwide: Government, Finance and IT & Telecoms

Perhaps unsurprisingly, organizations involved in government (including defense) and financial institutions reported the highest expenditure on IT security this year, with both sectors reporting budgets over $5M on average. It is worth noting that IT & telecoms companies and utilities and power companies worldwide also spent more than the average on IT security, although companies in these sectors spent closer to $3M than to the $5M+ spent by their government and finance counterparts.

Interestingly, however, when we consider how much was spent on IT security "per head," government organizations tend to fall lower down on the high spending list. On average, IT and telecoms firms spend around $1,258 per head on IT security, this rises to $1,344 in utilities companies, and $1,436 for financial firms. Yet, government organizations spend just $959 per head by comparison.



In both IT and telecoms, and utilities, the high spend on IT security per head is likely to be linked to concerns over the protection of intellectual property at these businesses. In the case of utilities and power organizations, this may be driven by the fact that these businesses are becoming increasingly vulnerable to the activities of malicious groups that target them.

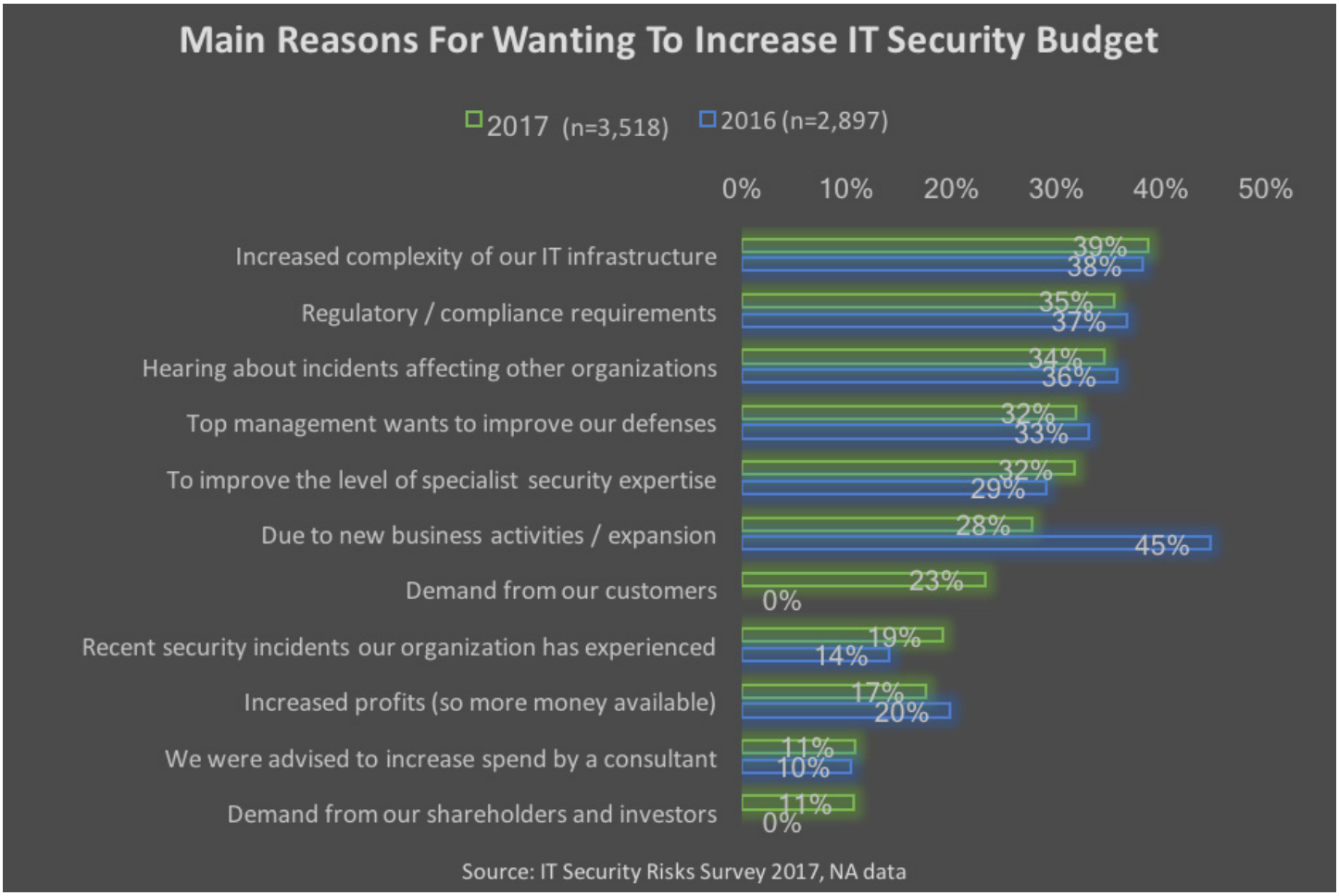
For these firms, certainly, investment in IT security isn't just a cost that must be budgeted for. It is an increasingly crucial part of business continuity plans that will help organizations continue to function. When considering the cost of a cyberattack for these firms, IT security is, arguably, an investment with measurable benefits.

Yet it is interesting that the same attitude doesn't seem to exist among industrial firms, which tend to rely on industrial control systems (ICS infrastructure) to keep their processes moving. Attacks on ICS infrastructure are increasing, up 5% in 2017 compared to 12 months ago. However, IT security budgets at these organizations are among the lowest compared to other sectors, at just $748K on average, and are significantly lower this year, raising concerns about the long-term security of these organizations and their important business processes.

Motivations for investing in IT security

With this wide spectrum of spending among different vertical sectors, it is important to ask what motivates a business to spend precious budgets on IT security. This, too, is crucial for our understanding of whether a firm considers its money spent on IT security to be money 'down the drain', or whether it views this budget as an investment.

This year, a few more companies in North America admitted that they will invest in cybersecurity regardless of ROI – 60% in 2017 compared to 59% in 2016. This indicates that more businesses understand that there is a need for them to invest in IT security.



They may not expect to see the ROI, yet North American businesses cite pressure from key stakeholders - including shareholders and investors (11%), and customers (23%) as a reason to increase their IT security spend. This suggests that businesses are recognizing it is a strategic benefit to spend more on IT security. In addition to protecting themselves from an attack, investing in IT security also allows them to demonstrate to customers that their data is in safe hands, and ensure business continuity for investors.

The most popular reason for businesses in North America to increase their IT security spend is to protect their increasingly complex IT infrastructures (39%). However, the need for businesses to improve the level of specialist security expertise they have is becoming increasingly important (up to 32% this year compared to 29% in 2016).

Consultant advice is also rising, with 11% of businesses citing this as a factor this year, compared to 10% last year. These figures indicate a need to bolster IT security expertise – both internally and through seeking the help of third parties. Indeed, both SMBs and enterprises are becoming more open to seeking advice from consultants, while investing in maintaining internal resources in their fight against cyberthreats.

Meanwhile, the need to increase security spend due to new business activities or expansion has dramatically dropped – falling from 45% last year to just 28% in 2017. This reduction is particularly noticeable among the North American SMB community, and is perhaps a reflection of the macro-economic factors that these businesses are vulnerable to. Compared to their larger counterparts, however, SMBs are increasingly investing in IT security because they have heard about incidents affecting other organizations and feel the need to protect themselves better.

Conclusion

The massive impact of the WannaCry and exPetr attacks this year shook the global business community and opened many eyes to the cyberthreats organizations can face in the world today. The cyber landscape is changing rapidly and businesses need to check their security posture and adjust their protection strategies to suit.

This means that businesses are increasingly having to do the math on the cost of proactively fighting cybercrime vs. the cost of becoming a victim. Our report has demonstrated that even data breaches that don't make news headlines can have an expensive and damaging impact on organizations of all sizes.

Through this research, we also found that legislative changes across the globe are adding to the cost of security incidents – meaning that businesses have to adjust, or risk being both non-compliant and vulnerable to cyberthreats.

Therefore, understanding the math behind the cost of a cyberattack is more crucial now than ever. Perhaps as a result of this report, businesses across the globe will grant a greater proportion of their IT budgets to security. In fact, we did find that this year, slightly more companies admitted that they will invest in cybersecurity regardless of ROI – 60% in 2017 compared to 59% in 2016, which is a good sign of businesses' taking a proactive approach to prepare for a potential cyberattack.

In the face of increasingly expensive cybersecurity incidents, those organizations calculating IT security as an investment who are prepared to spend accordingly, are likely to be the most ready to defend themselves against future threats to their business. Where does your organization stand?

True Cybersecurity for Business

Kaspersky Lab's True Cybersecurity approach combines multi-layered security with cloud-assisted threat intelligence and machine learning to protect against the threats your business faces. True Cybersecurity not only prevents attacks, but also predicts, detects and responds to them quickly, while also ensuring business continuity for your organization.

About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company celebrating its 20 year anniversary in 2017. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

Learn more about internet security: www.securelist.com

www.usa.kaspersky.com
#truecybersecurity

AO Kaspersky Lab
500 Unicorn Park, 3rd Floor Woburn, MA 01801 USA
Tel: 866-563-3099 | Email: corporatesales@kaspersky.com