KASPERSKY lab

IT SECURITY:

COST-CENTER OR STRATEGIC INVESTMENT?

Investigating the new business attitude towards IT security budgets

Contents

Introduction

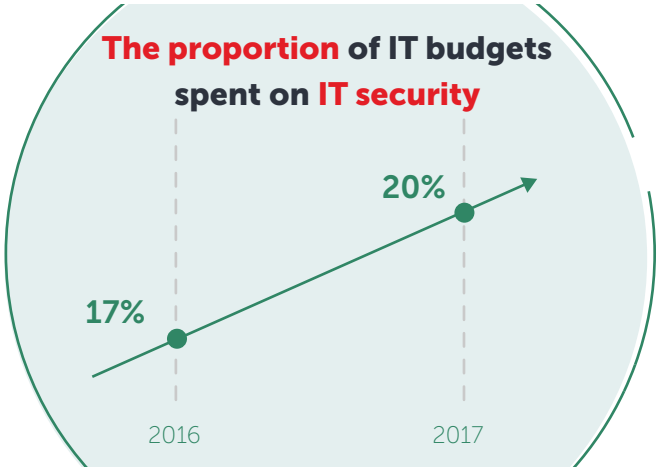
The cyber landscape is continuing to evolve at pace and businesses across the globe are having to constantly adapt to keep up. No matter what sector or sized business you operate in, it's likely that security is becoming an increasingly important part of your firm's IT budget.

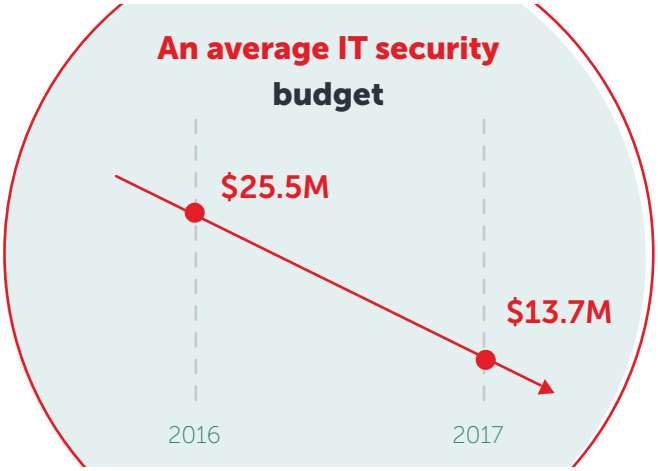
The Kaspersky Lab Global Corporate IT security Risks Survey is an annual study into the state of IT security within organisations across the world. Now in its 7th year, this study builds upon the findings of our previous reports, asking important questions about IT security spend, the threats businesses 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 threat landscape, by questioning business decision makers about their attitudes to IT security budgets.

?

This year, we consider the important question – do businesses view IT security as a **cost centre** (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)?

The question is an important one because our study has found that IT budgets are being squeezed on a global scale.





With their budgets under pressure, IT security teams are up against it – 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.

Introduction

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.

2017, March & April

5,274 interviews

30 countries

3 types of companies

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 & medium sized businesses with 50 to 999 employees) and Enterprises (businesses with over 1,000 employees). Not all survey results are included in this report.

Key findings

- **Cyberthreats are becoming harder and more expensive to fight for companies of all sizes.** Among SMBs the average total impact of a data breach amounts to $87.8K, but this is more than ten times higher for enterprises ($992K). These costs, moreover, have grown since last year ($86.5K for SMBs and $861K for enterprises in 2016).

- **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 but particularly among enterprises with over 1,000 employees, where the IT security budgets have risen from an average of a fifth of the overall IT security budget to almost a quarter in the last 12 months.

- **However, IT security budgets are declining overall.** The average IT security budget for enterprises was $25.5M last year but dropped to $13.7M in 2017. So, while IT security has been granted with a larger proportion of overall IT budgets, IT security teams have faced having to do more with less.

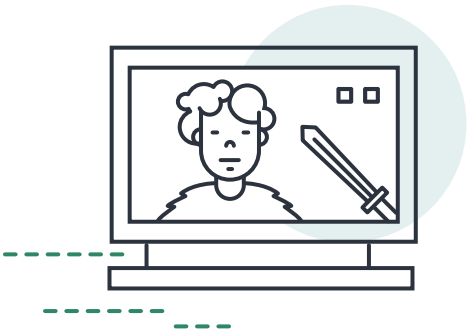
- **With data breaches getting more expensive to recover from, protection might soon become an issue for firms that do not prioritise IT security spend.** Indeed, our study has shown that SMBs tend to suffer most with an average $13K loss of business when a data breach occurs, while enterprises pay out an average $134K in compensation.

- **39% of businesses cite pressure from key stakeholders - including shareholders, investors (15%) and customers (24%) 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 – 63% in 2017 compared to 56% 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. This in turn, will have a knock-on effect on whether businesses view their cybersecurity spend as a cost-centre, or an investment that will help them avoid the larger financial penalties associated with an attack.

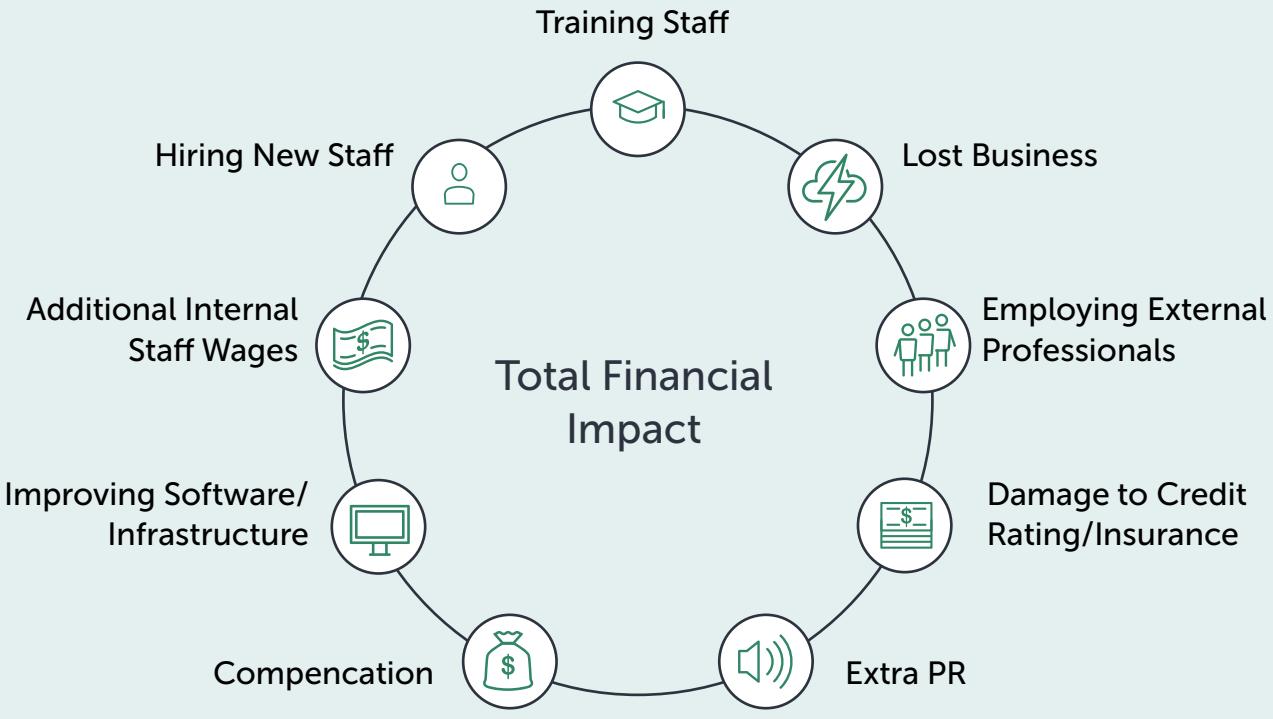
Serious data breaches are getting more expensive



The attacks that make business decision makers worry – such as those against the 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 specialist 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 organisations to estimate how much money they had spent/lost in the aftermath of a data breach, experienced within the last 12 months.

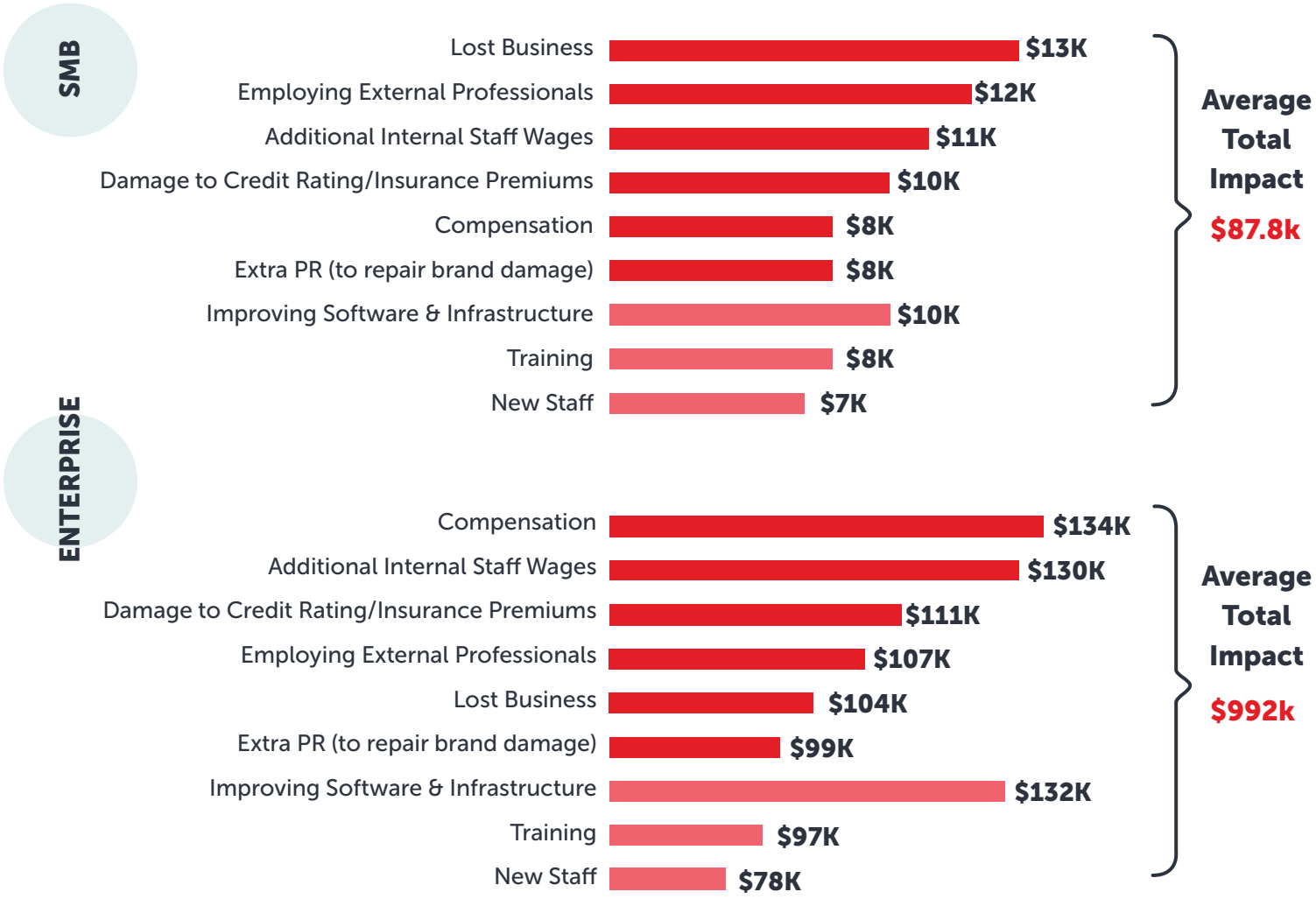
All businesses with **50 or more employees** were asked to **estimate the costs** they incurred in each of the following categories, after a breach:



The cost of IT security incidents

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

We have shown results separately for SMBs and enterprises below, as the picture is very different for different sized firms. Among SMBs, for example, the average total impact of a data breach amounts to $87.8K, and this is more than ten times higher among enterprises ($992K), demonstrating that cyberthreats are expensive to fight for companies of all sizes.



Base: 1,229 SMBs/ 919 Enterprises Suffering At Least One Data Breach

The cost of IT security incidents

While it's perhaps 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 represented the single largest additional cost for both SMBs and enterprises, this year the picture has changed, with SMBs and enterprises having different experiences. The top pain points for SMBs include **lost business** and **costs related to employing external professionals**, while compensation was one of the lowest figures. By contrast, enterprises incur the largest costs due to **compensation** and spend on internal security in the form of **additional staff wages** and **improved software/infrastructure.**

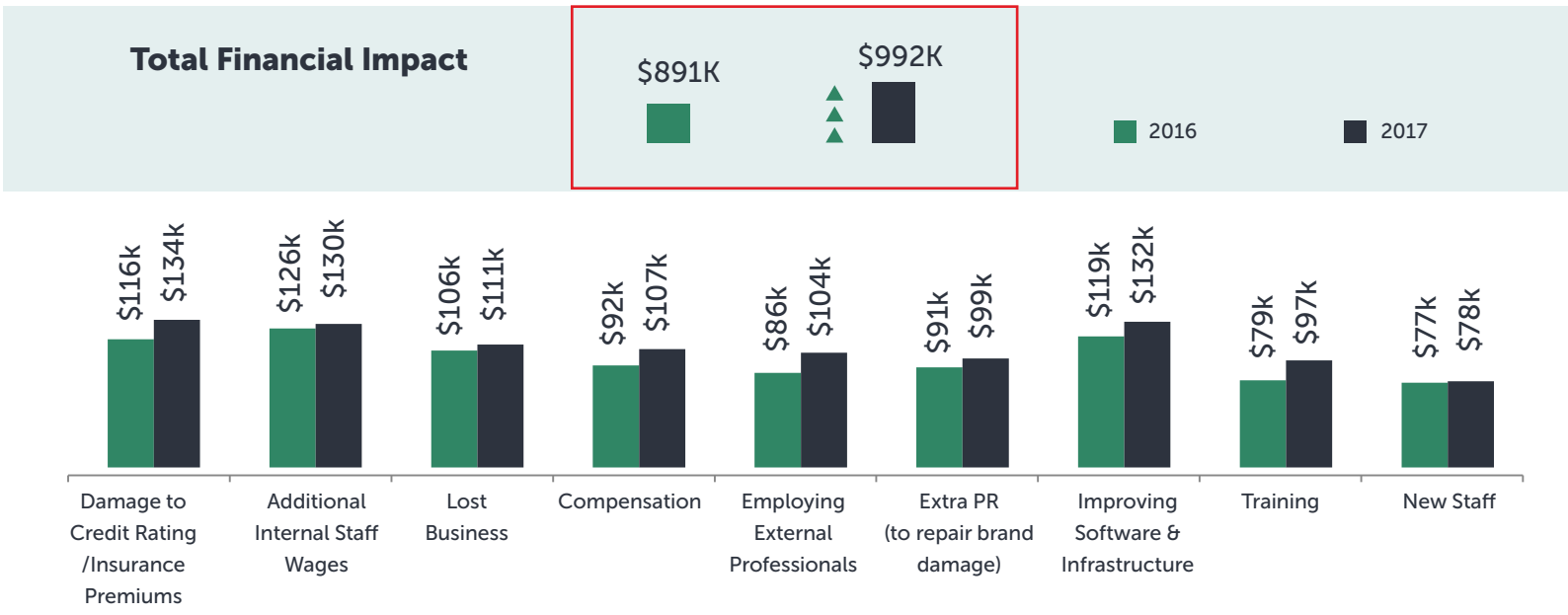
In addition, spend on training in the aftermath of a security breach is particularly expensive for enterprises – at $97K on average – with businesses realising the need to increase the cyber awareness of their staff, once they have been stung by a security incident and highlighting the need for these businesses to have better threat intelligence.

The different costs experienced by enterprises and SMBs directly reflects the current capabilities of most organisations 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 $134K spend on compensation per data breach.

The financial impact of evolving legislation

With the average cost of a data breach rising 11% for enterprises in 2017, where have the increased costs come from? Our study found that some of the largest increases in costs have stemmed from the need to try and prevent - or at least limit - reputational damage, both in terms of credit ratings, PR costs, and compensation.



Base: 919 Enterprises Suffering At Least One Data Breach

The cost of IT security incidents

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.

One such market is Japan, where the average cost of a data breach for enterprises more than doubled this year from $580K in 2016 to $1.3M in 2017. The Japanese government, aware of the problem of data breaches, has taken measures to harden data security regulations with new legislation that came into effect in 2017, resulting in the sudden spike in related costs.

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 since 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 8 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 from May 2018, and which will greatly limit how businesses treat EU citizen data.

With legislation changing across the world, but with cyberthreats evolving faster, 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. Incidents affecting infrastructure hosted by a third party **($140K)**

2. Incidents involving non-computing connected devices **($112K)**

3. Electronic leakage of data from internal systems **($111K)**

4. Targeted attacks **($108K)**

5. Incidents affecting third party cloud services they use **($100K)**

The cost of IT security incidents

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

1. Incidents affecting suppliers that they share data with **($1.8M)**

2. Incidents affecting infrastructure hosted by a third party **($1.6M)**

3. Incidents involving non-computing connected devices **($1.6M)**

4. Electronic leakage of data **($1.2M)**

5. Incidents affecting third party cloud services they use **($1.2M)**

What's immediately clear is that often attacks which result from the security failures of business partners are amongst the most damaging to businesses of all sizes. 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 organisations 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 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.

Both SMBs and enterprises 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. And, 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-centre, 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

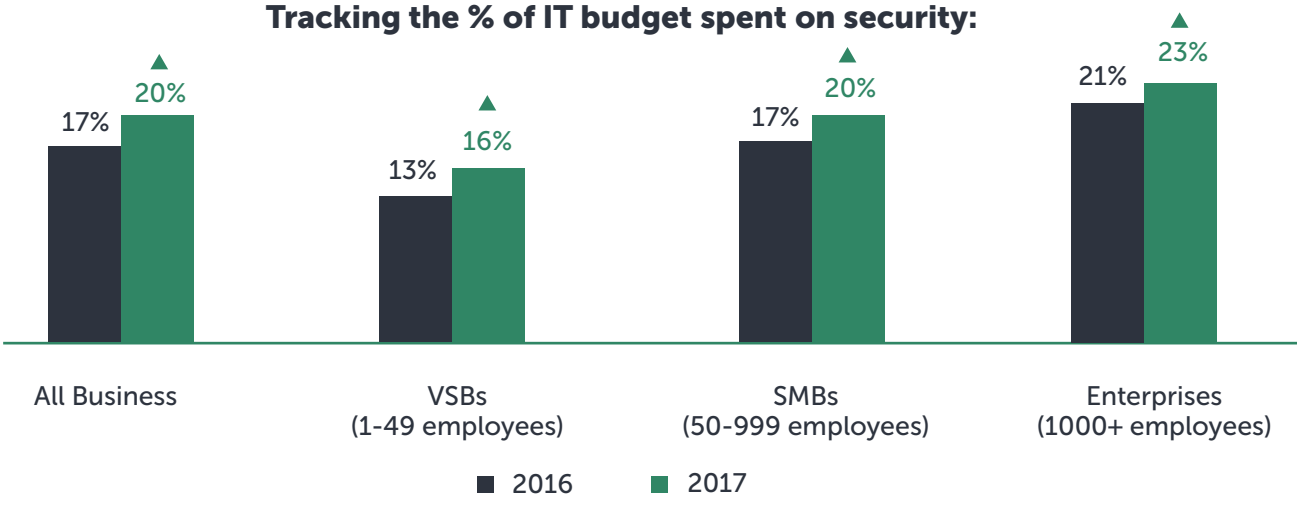
This year, we've seen that cost saving and outsourcing efforts appear to have resulted in a reduction in overall IT budgets amongst larger businesses. Despite this (or perhaps because of it) the proportion of IT budgets which is spent on IT security is rising. This is a pattern that is consistent across businesses of all sizes 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.

Even among very small businesses, where resources are in short supply, the percentage of IT budget which is going towards security has risen – from a worryingly small 13% in 2016 to a slightly healthier 16%.

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-centre.

Nonetheless, the study does still demonstrate a decline in IT security budgets. The average IT security budget for enterprises was $25.5M last year but dropped to $13.7M in 2017. So, while security is getting a larger proportion of the IT budget pie, the pie itself is getting smaller. This is a concern when the stakes are high, and when the prospect of an attack is an expensive one.

Tracking the % of IT budget spent on security:



Base: 4,576 All Respondents Able To Estimate Budget

Investing in reducing the risk

IT security top spenders

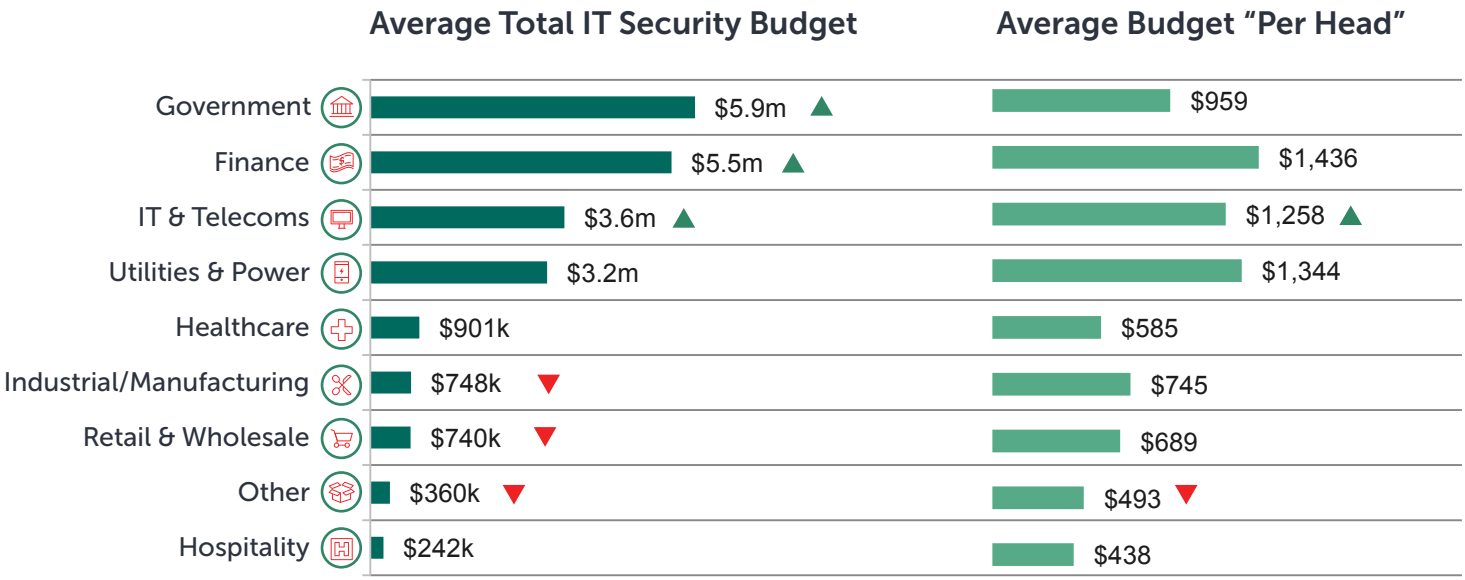
Government
≈ $5M

Finance
≈ $5M

IT & Telecoms
≈ $3M

Perhaps unsurprisingly, organisations involved in government (including defence) 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 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 organisations 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, and this rises to $1,344 in utilities companies and $1,436 in financial firms. Yet, government organisations spend just $959 per head by comparison.



N.B IT budget and IT security budget figures show a trimmed average – by removing a small percentage of the largest and smallest values prior to calculating the mean, the skewing effect of outliers is reduced.

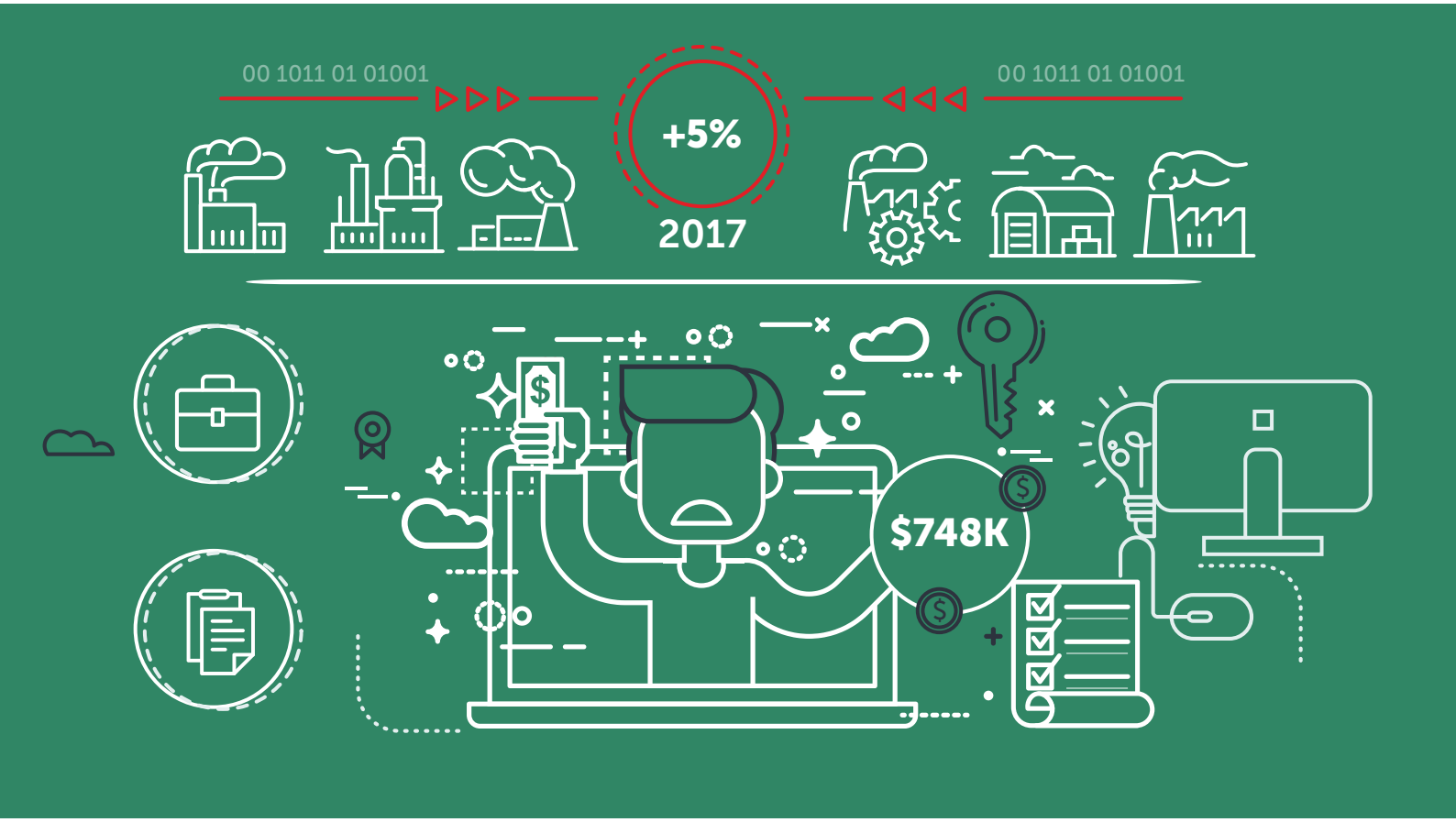
▼ Significantly Lower ▲ Significantly Higher Base: 4,576 All Respondents Able To Estimate Budget

Investing in reducing the risk

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 organisations, 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 organisations 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 organisations 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 organisations and their important business processes.



Investing in reducing the risk

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, significantly more companies admitted that they will invest in cybersecurity regardless of ROI – 63% in 2017 compared to 56% in 2016. This indicates that more firms understand there is a need for them to invest in IT security.

IT & security budgets

Tracking motivation for increased spend

Main Reason For Wanting To Increase IT Security Budget

Base: All Respondents Expecting To Increase IT Security Spend

Investing in reducing the risk

They may not expect to see a return, yet businesses cite pressure from key stakeholders - including shareholders and investors (15%), and customers (24%) as a reason to increase their IT security spend. This suggests that businesses are recognising it is of strategic benefit to spend more on IT security – as well as allowing businesses to defend themselves against attack, it 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 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 38% this year compared to 33% in 2016). Consultant advice is also on the rise, with 17% of businesses citing this as a factor this year, compared to just 13% 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 dropped – falling from 37% last year to 32% in 2017. This reduction is particularly noticeable among the 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 organisations and feel the need to protect themselves better.

Conclusion

From the massive impact of the WannaCry and exPetr attacks, which the global business community fell victim to this year, to the threat of targeted hacks such as that suffered by HBO in recent months, the cyber landscape is changing rapidly, and businesses are having to adjust their protection strategies to suit.

Businesses are increasingly having to do the maths on the cost of proactively fighting cybercrime vs. the cost of being a victim.

Our report has demonstrated that even data breaches that don't hit the headlines can have an expensive and damaging impact on a business. We have 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 insecure.

The maths, therefore, is getting more crucial. Perhaps as a result of this, businesses across the globe are granting a greater proportion of their IT budgets to security. This year, significantly more companies admitted that they will invest in cybersecurity regardless of ROI – 63% in 2017 compared to 56% in 2016.

In the face of increasingly expensive cybersecurity incidents, those firms calculating that IT security is an investment, and are prepared to spend accordingly, are likely to be the most ready to defend themselves against attack. Where do you stand?