



On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives

Kaspersky Lab



Contents

Introduction	2-4
Methodology	5
Key findings	6
The average cost of data breaches	7-8
Why are the costs growing?	9-13
The costliest attacks: All about data on the go	14-17
IT security has a place on the boardroom agenda	18-22
Motivations for investing in IT security	23-25
Conclusion.	26

Introduction



It's a challenging time to be in business. The world is getting smaller, and we live in a new age of the 'now' consumer, where customers demand immediate results, where the competition is moving faster than ever before, and where **70% of consumers** agree that technology makes it easy for them to take their business elsewhere.

47%
of CEOs
are being challenged
by their boards to
digitally transform

Against this backdrop, multiple businesses are embarking on digital transformation strategies, indeed, **Gartner has found that almost half (47%) of CEOs** are being challenged by their boards to digitally transform to improve their growth prospects and customer relationships. Many are, for example, moving an increasing amount of their platforms and data to the cloud, allowing them to scale, or respond to market trends as needed, and with the necessary agility to keep competitors at bay.

Indeed, this data now forms the cornerstone of digital transformation. Data-driven initiatives have grown to play a leading role in organizations of all sizes, providing business leaders with the insight needed to successfully execute both short and long-term strategies.

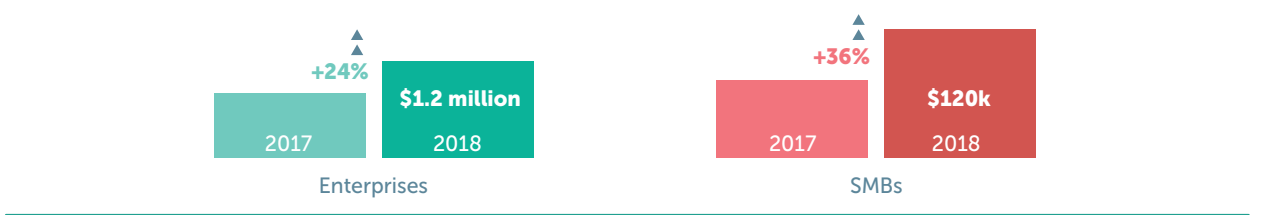
And as businesses digitally transform, cybersecurity considerations are increasingly having to play a strategic role in business, something that is reflected by [current debates around CISO reporting structures](#) and the often quoted need to give information security a place around the c-suite table.

The drivers for taking cybersecurity seriously in business are clear – as businesses become increasingly reliant on digital platforms, they simply can't afford for those platforms to go wrong. And here lies a problem – because the world of IT security risks is an ever-evolving one. New threats emerge every day, and as business infrastructures adapt, new vulnerabilities form too.

Understanding the complexities and pressures of IT security is our mission, so that businesses can help protect what's most important to them. Continuing our annual research into the economics of IT security, this survey thus builds on data from previous years to identify how organizations are responding to changes in the threat landscape, and to understand the IT security spending habits that could be making or breaking businesses around the world. This is an overview of our findings.

Attacks are becoming more sophisticated and devastating

The unwelcome news for businesses in all industries is that the financial impact of cyberattack and the subsequent costs of recovery, are continuing to increase. **For enterprises globally, the average cost of a data breach is now just over \$1.2 million, a 24% increase from 2017 and a 38% increase from 2016. And the story is the same for SMBs globally, with the financial impact of a data breach growing 36% over the last 12 months from \$88k in 2017, to \$120k in 2018.**



Improving software and infrastructure is now the costliest outcome of a security breach for enterprises and the joint-costliest for SMBs. This highlights how much damage the various ransomware epidemics, damaging exploits and supply chain attacks over the last 12 months have done to corporate infrastructure, painting a picture of the extent of the work required to get these systems renewing and more sustainable in response to an attack.

For enterprises globally, making infrastructure improvements after a breach now sets them back \$193k on average, more than a 46% increase on the **\$132k** it cost them in 2017. Indeed, this figure is the highest or joint-highest for enterprises in all regions except Latin America, illustrating how the majority of enterprises are in the same boat when it comes to the financial implications of a data breach. Our study also emphasizes how cybersecurity incidents can directly harm the way they do business, with damage to credit ratings/insurance premiums (**\$180k**) and lost business (**\$131k**) both being in the top five costliest outcomes of a data breach.

A significant amount of money is also being spent on improving the level of knowledge and expertise that enterprises have access to, either through training their employees (**\$137k**), employing external professionals (**\$126k**) or hiring new staff (**\$106k**). The challenge for all businesses is that the continuing industry-wide skills shortage is making it increasingly difficult to find the right talent at an affordable price. This is likely the reason why enterprises are focusing so much more on training their current workforce, rather than recruitment.

Digital transformation strategies are being put at risk

This year's results have shown that the costliest incidents are related to cloud infrastructure. What's apparent is that the booming cloud and mobile trends have presented plenty of opportunities for cybercriminals to exploit. They are also opening businesses up to risks related to human error, while the distributed nature of cloud infrastructure presents management complexities. The use of cloud computing platforms has been on the rise for some time within both enterprises and SMBs which, although offering multiple benefits to businesses, also puts corporate data at risk.

Looking at the top three most costly threat types, security incidents affecting IT infrastructure hosted by a third party had the biggest impact for SMBs **(\$118k)** and the second-biggest financial impact for enterprises **(\$1.11m)**. Incidents affecting third party cloud services that the company uses also have a significant financial impact on SMBs **(\$89k)**, signifying that business digital transformation strategies (and cloud adoption as a part of this) may be at risk from IT incidents if businesses cannot find a way to mitigate the risks.

Security is becoming increasingly strategic



To combat these threats, security is being given an increasingly loud voice in business. Organizations are starting to feel the real impact of cybersecurity on business, with the results of the study showing that fears of the cost of an incident **are forcing business leaders to give cybersecurity a larger portion of the IT budget (23%) and more attention in the boardroom than in previous years.**

Enterprises expect their IT security budgets to grow by 15% over the next three years. The same is true for VSBs, representing a significant investment for businesses with less than 50 employees where resources are often in short supply, while SMBs expect to see a 14% growth in their cybersecurity spend by 2021. Enterprises in META meanwhile, expect their IT security budgets to increase by nearly a fifth (19%) over the next three years, in significant contrast to enterprises in Japan (12%) and North America (11%) at the opposite end of the scale.

One potential reason for this is that growing regulatory controls, for example the introduction of the GDPR legislation in the EU, is likely having an impact on the importance placed on IT security – the legislation will hold businesses accountable for the protection of customers' personal data and promises strict fines for non-compliance. This makes it somewhat surprising that enterprises in Europe expect their IT security budgets to increase by just 13% over the next three years, which is low compared to some other regions.

These findings not only highlight the growing costs associated with defending against cyberattacks, they also illustrate the value and importance that business leaders are placing on being able to protect their businesses against the latest threats – there's a drive for IT security from the top down.

Indeed, the involvement of top management in the cybersecurity provisioning debate is a sure sign that security is becoming increasingly wrapped up business strategy. One thing remains clear from our study – responding to, and recovering from security incidents and data breaches is now more important than ever. Read on, to find out more detail.

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. **A total of 6,614 respondents from 29 countries were asked about their organization's spending on IT security, the types of threats they have faced and the costs of recovering from attacks.** The regions covered consist of LATAM (Latin America), Europe, North America, APAC (Asia-Pacific with China), Japan, Russia and META (Middle East, Turkey and Africa).

Throughout the report, businesses are referred to as either 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

- ▶▶▶ **The cost of data breaches jumped up by over a fifth for both enterprises and SMBs.** The average financial impact of a data breach now stands at **\$1.23 million** for enterprises, increasing by 24% from **\$992k** in 2017. The same is true for SMBs, with costs rising from **\$88k** last year to **\$120k** in 2018 – a 36% increase.
- ▶▶▶ **Businesses in APAC, Japan and North America experience the highest recovery costs.** Suffering a data breach is most expensive for enterprises in Japan (**\$1.7 million**), followed by North America (**\$1.6m**) and APAC with China (**\$1.5m**). North America comes out on top for SMBs (**\$149k**). For both enterprises and SMBs, the average financial impact of a data breach is lowest for those based in Russia, at **\$246k** and **\$74k** respectively.
- ▶▶▶ **Average security budgets have increased across all company sizes.** Enterprises now spend an average of **\$8.9m** on cybersecurity, while SMB security budgets have grown from **\$201k** in 2017 to **\$246k** in 2018. The increase has been the greatest in VSBs, with average security budgets raised from **\$2.4k** to **\$3.9k** over the last 12 months, proving that even the smallest of businesses are now taking IT security seriously.
- ▶▶▶ **The costliest threats are related to data leaving the business premise.** Incidents affecting IT infrastructure hosted by a third party is one of the most expensive threats for both enterprises (**\$1.09m**) and SMBs (**\$118k**) to recover from, closely followed by inappropriate data sharing by mobile devices and incidents affecting third party cloud services.
- ▶▶▶ **Infrastructure complexity and a lack of knowledge drive IT security investments.** More than a third of businesses cite the increased complexity of their IT infrastructure (34%) and a need to improve the level of specialist security expertise (34%) as motivations to invest in cybersecurity.

The average cost of data breaches

Businesses big and small now have a range of cost factors to consider following a data breach, from personnel costs to paying fines and compensation. But what exactly does a 'typical' data breach look like from a financial perspective? For enterprises, the average cost of a data breach now stands at over \$1.23 million, increasing from \$992k in 2017. While the biggest costs come from improving software and infrastructure (\$193k), factors such as damage to credit ratings/insurance premiums (\$180k) and training (\$137k) are also having a major impact.

And the story is the same for SMBs, with the average cost of a data breach having grown from \$87.8k in 2017 to \$120k in 2018. SMBs are facing many of the same costs as enterprises, with employing external professionals, damage to credit ratings and lost business (all \$15k) having the joint biggest impact, all of which could make up a large chunk of an SMB's revenue.

Following prominent expensive incidents last year it seems that Enterprises are investing heavily in improving protection and strengthening insurance coverage

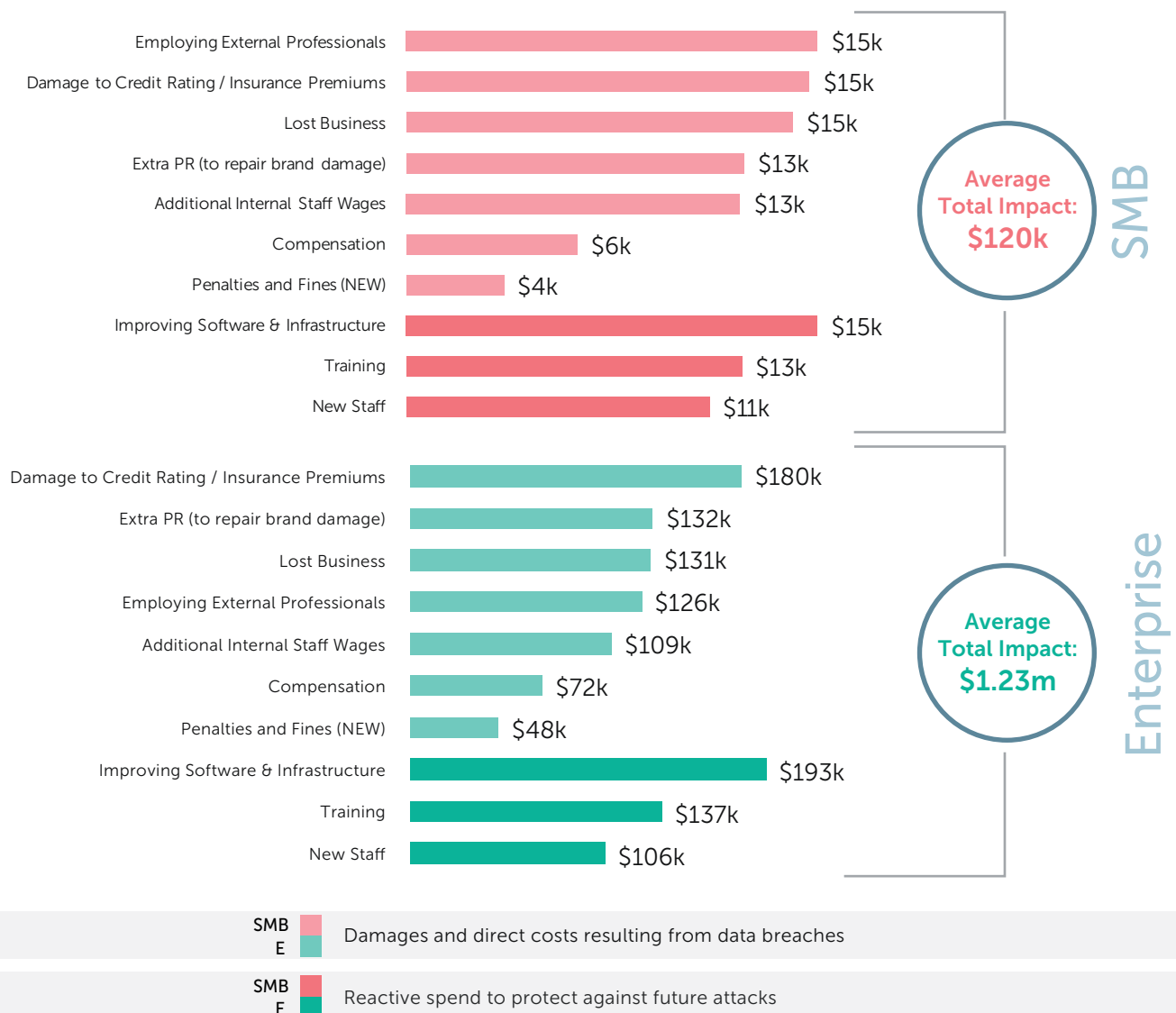
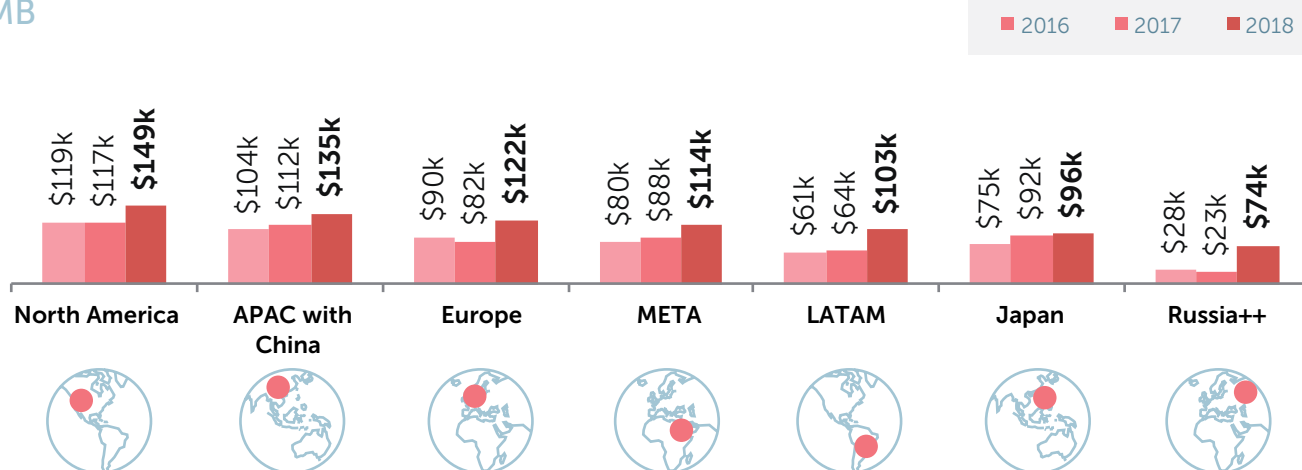


Figure 1: The average financial impact of a data breach globally

Interestingly, the costs associated with recovering from a data breach vary significantly between regions. For SMBs, the average costs have increased across all seven regions included in the study, with North America (\$149k) and APAC with China (\$135k) being the most expensive and Russia (\$74k) coming in as the least costly.

And the same is true for enterprises. The average cost of suffering a data breach now stands at \$1.7m for enterprises in Japan, \$1.6m in North America and \$1.5m in APAC with China. As with SMBs, data breaches have the lowest financial impact for enterprises in Russia (\$246k), just a \$6k increase from 2017.

SMB



Enterprise

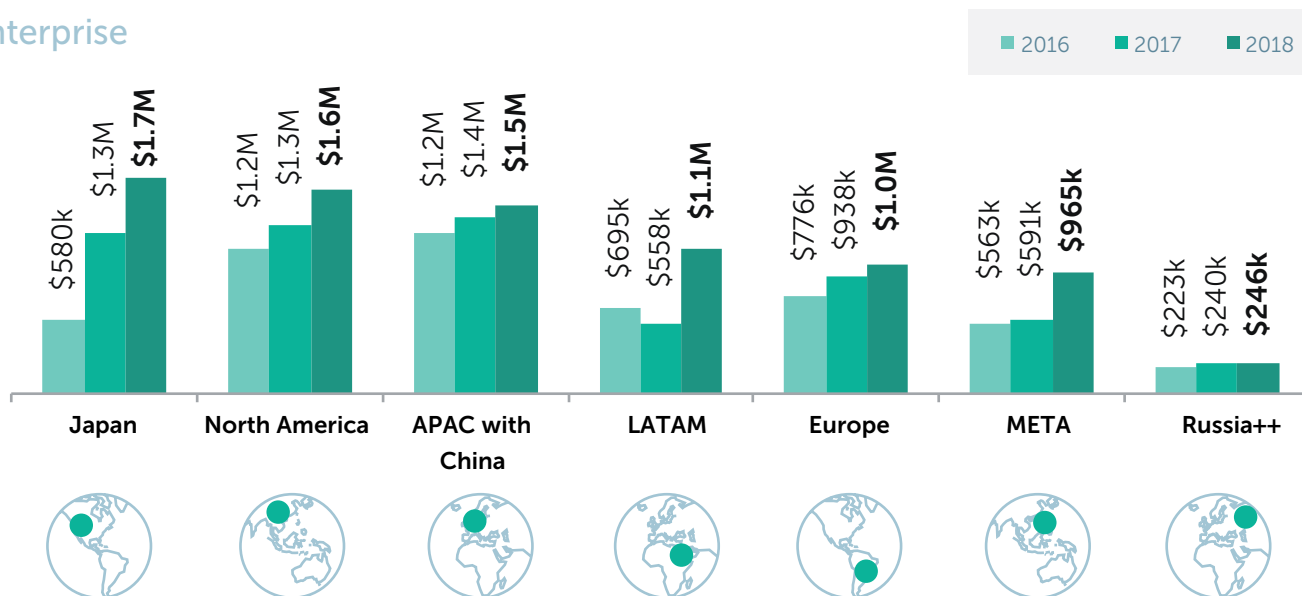


Figure 2: Average financial impact of a data breach by region

Whatever the reason, the costs are clearly growing across the board, placing serious financial pressures on businesses large and small and illustrating why security is becoming such a prominent issue as businesses continue to transform. But, just where is all this extra money being spent?

Why are the costs growing?

With the costs incurred from suffering a data breach stemming from so many different areas, it can be hard for businesses to identify exactly where their money is being spent. Our study found that making technical enhancements following an incident now carries an especially heavy financial burden for enterprises and SMBs alike, along with damage to insurance premiums and activities to improve internal expertise.

For enterprises, improving software and infrastructure represents the biggest costs following a data breach at \$193k, coming in ahead of damage to credit ratings/insurance premiums (\$180k) and training investments (\$137k). The pattern is similar for SMBs, where four different costs share the top spot – infrastructure improvements, employing external professionals, damage to credit ratings and lost business all costs SMBs \$15k on average.

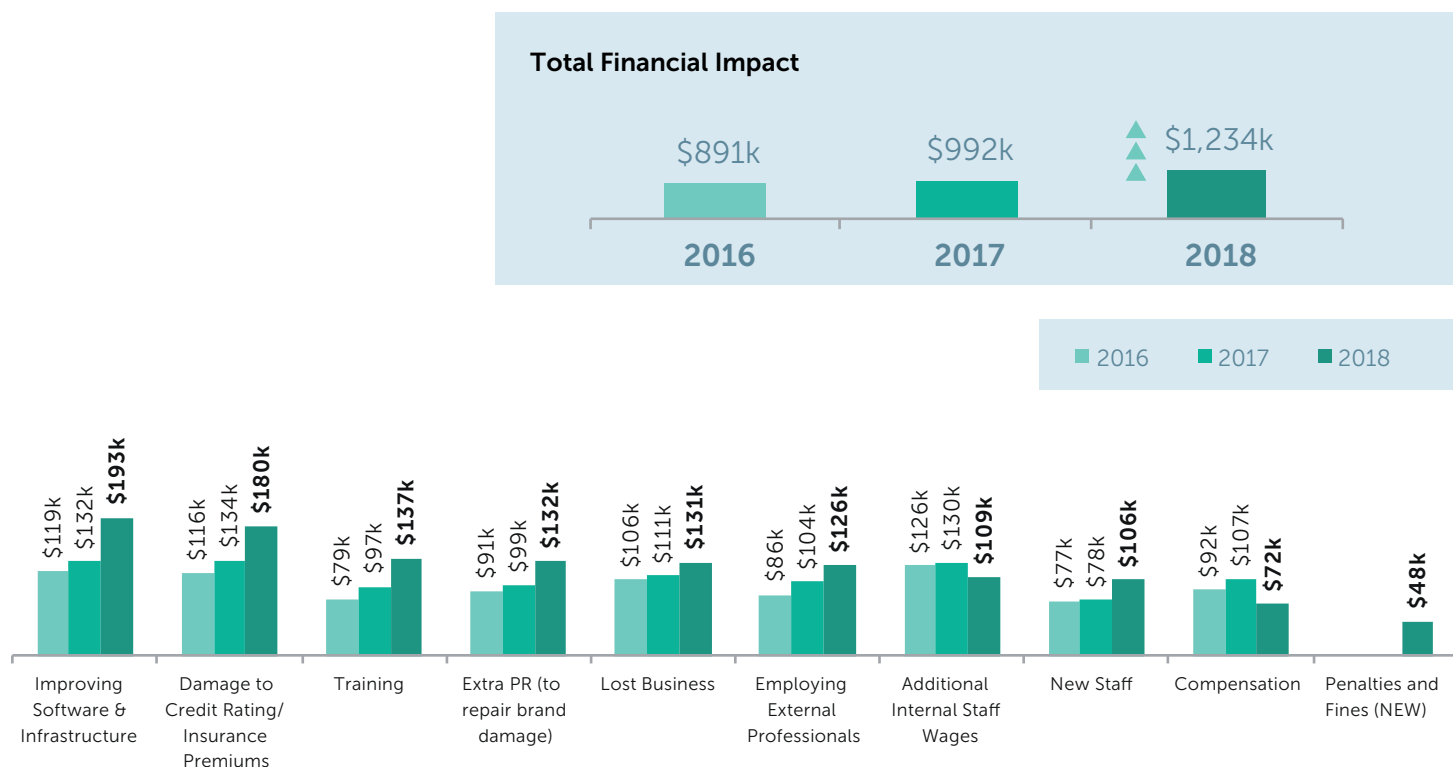


Figure 1: Tracking the financial impact of a data breach for enterprises

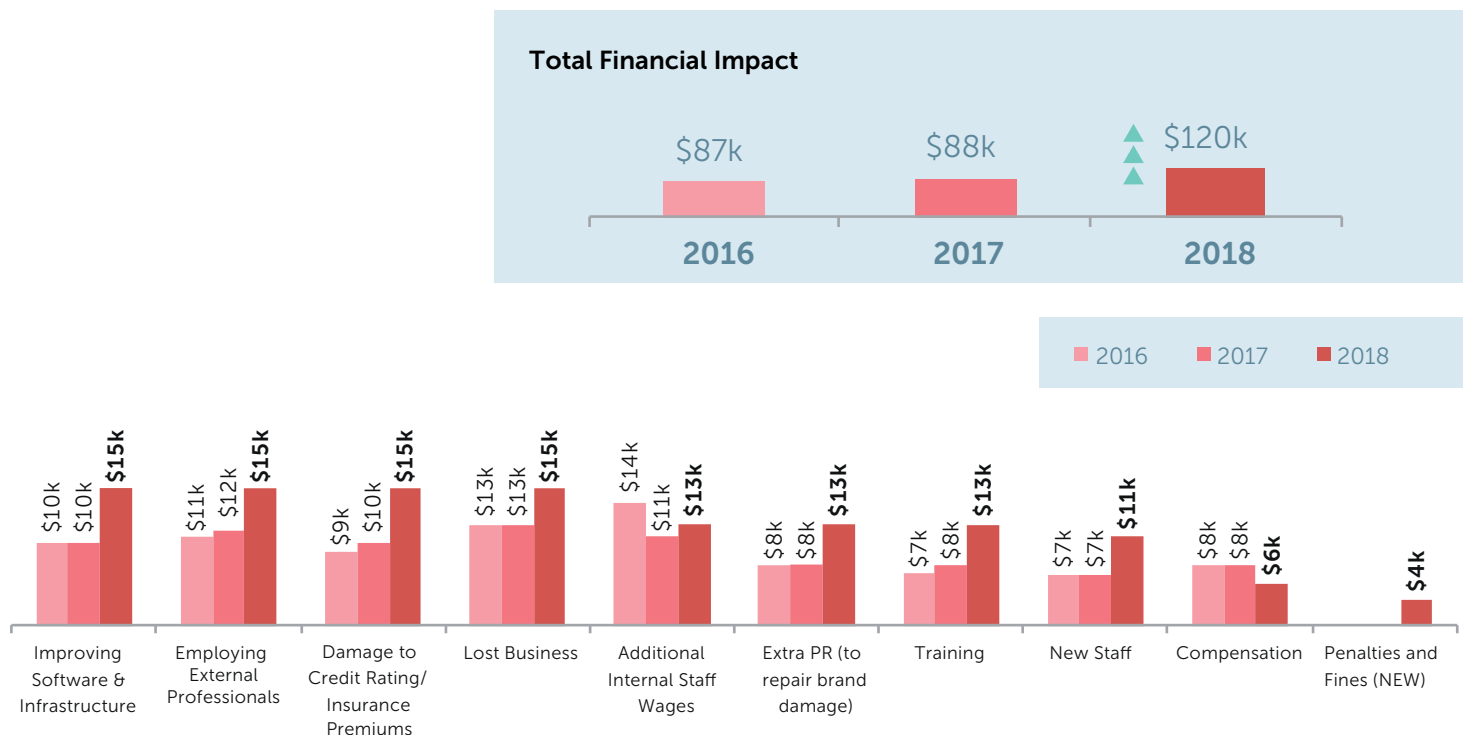


Figure 2: Tracking the financial impact of a data breach for SMBs

There are also some interesting regional variations that are worthy of mention. For example, employing external professionals is one of the costliest outcomes of a security breach for SMBs in North America, Latin America and Europe, suggesting that businesses in these regions are more in need of additional expertise.

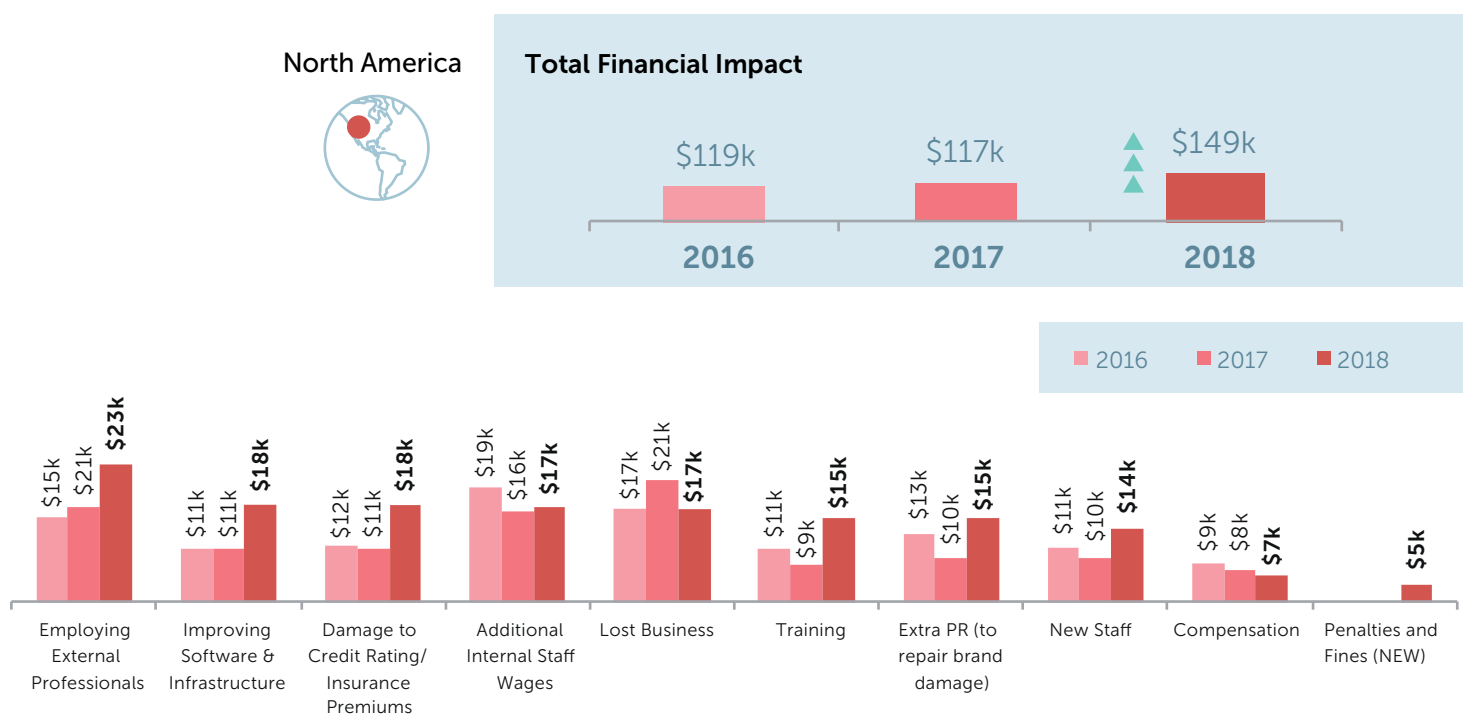


Figure 3: The financial impact of a data breach for SMBs in North America

LATAM



Total Financial Impact

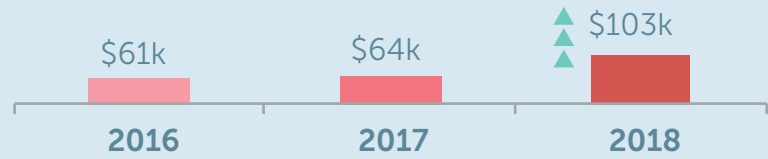


Figure 4: The financial impact of a data breach for SMBs in LATAM

Europe



Total Financial Impact

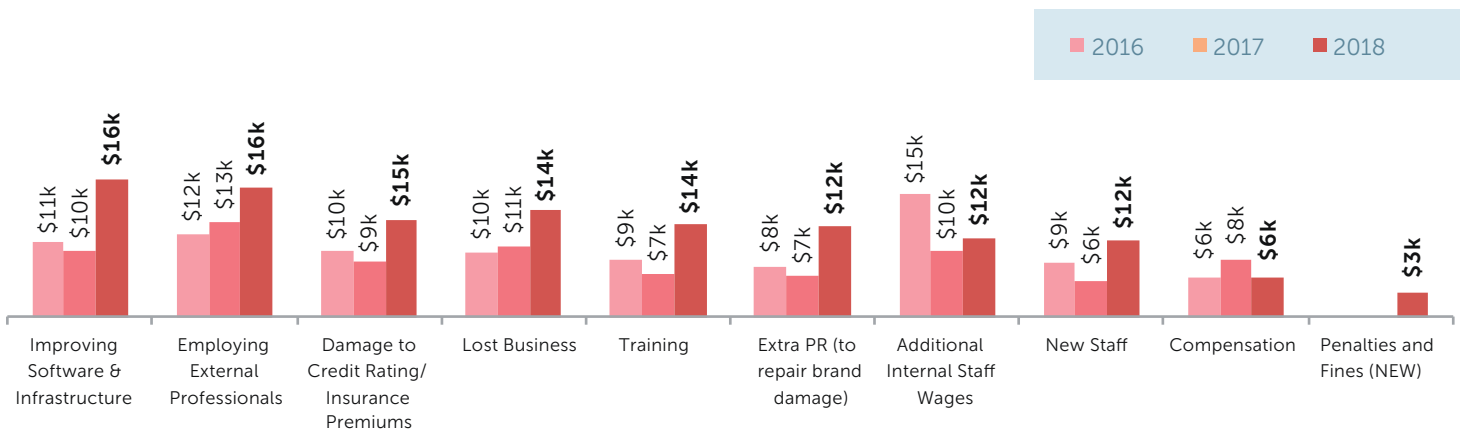
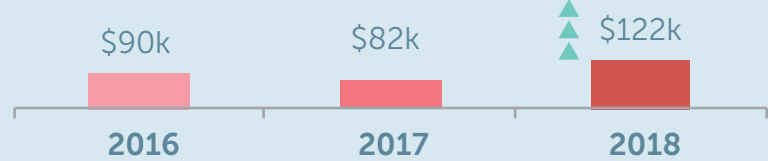


Figure 5: The financial impact of a data breach for SMBs in Europe

Furthermore, there are certain regions where minimizing or repairing reputational damage is much more of a priority. Extra PR to repair brand damage ranked as the second-most costly factor for SMBs in Japan (\$13k) and the third-most costly factor for enterprises in the META region (\$113k) and SMBs in Russia (\$8k).

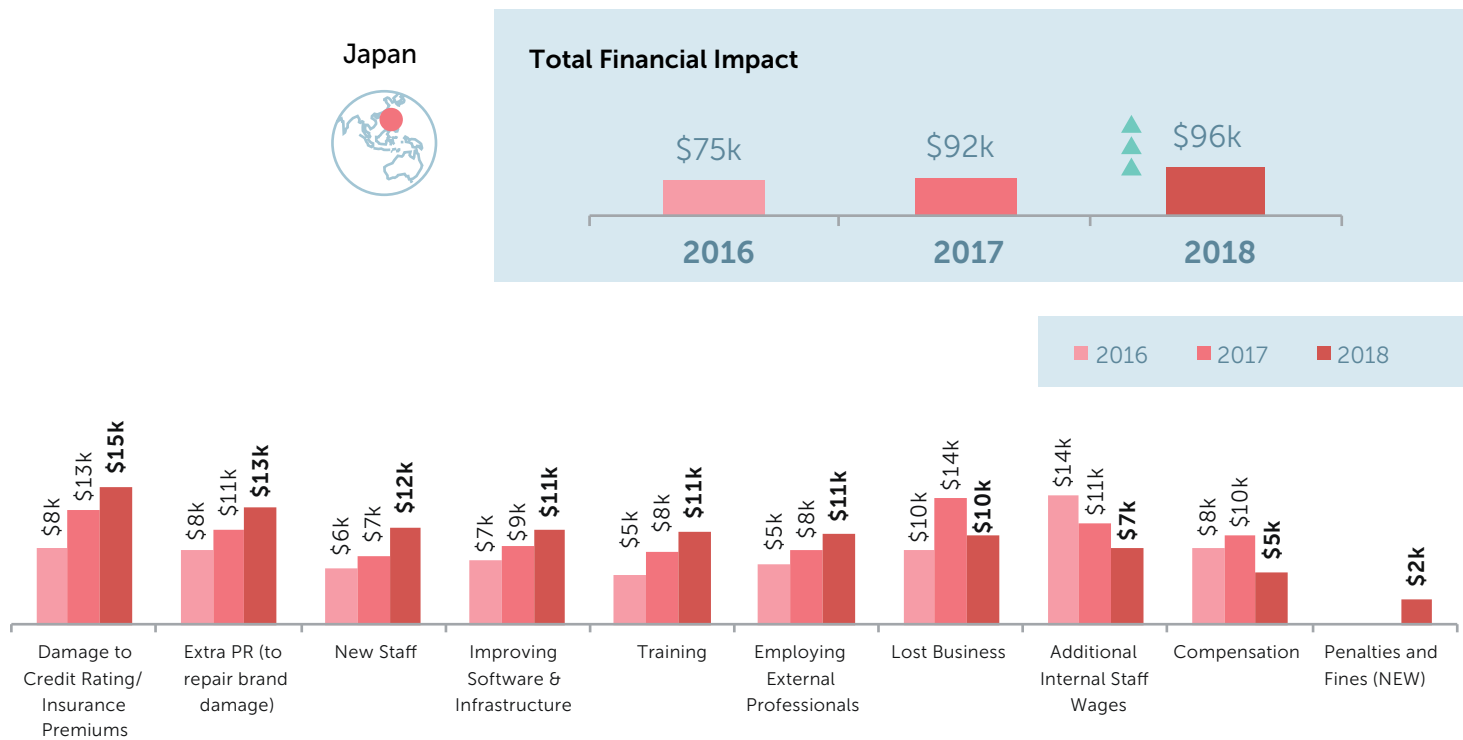


Figure 6: The financial impact of a data breach for SMBs in Japan

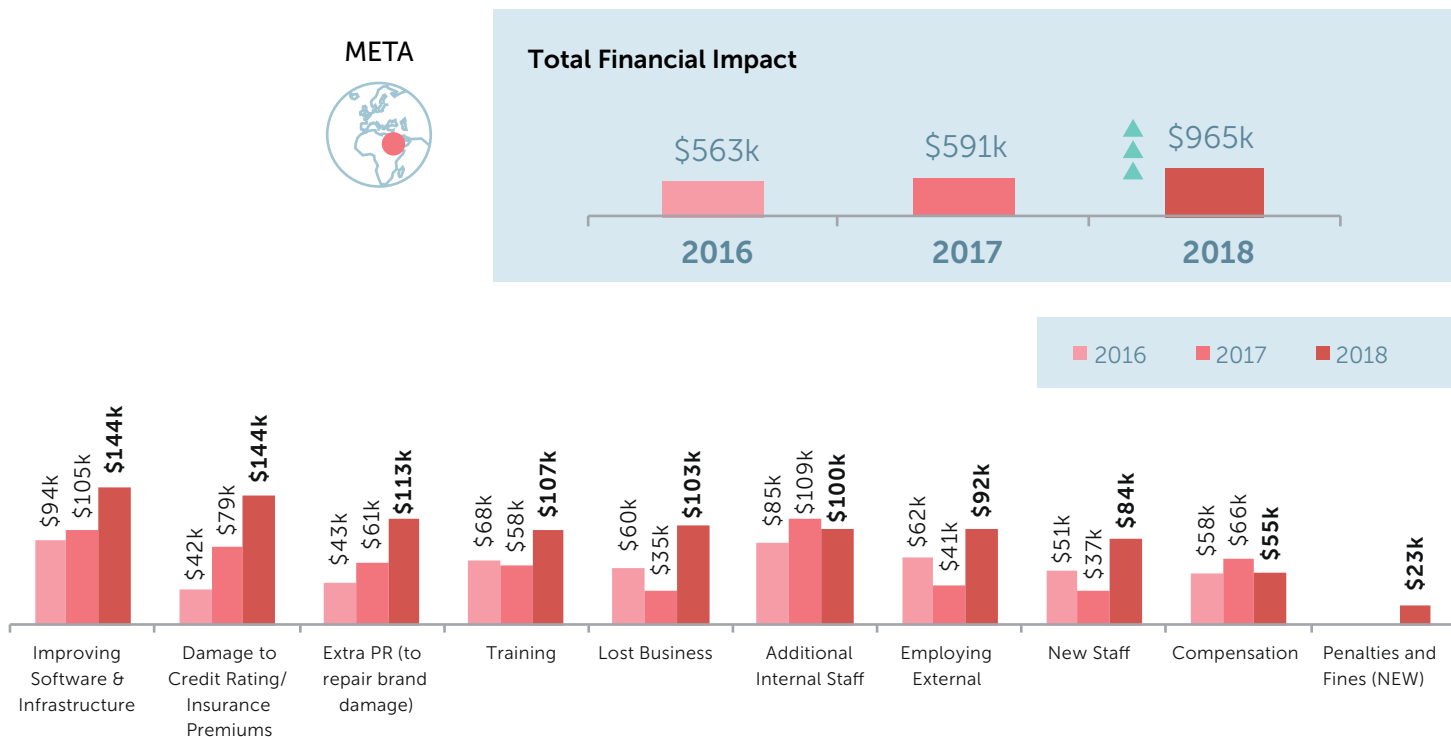


Figure 7: The financial impact of a data breach for enterprises in META

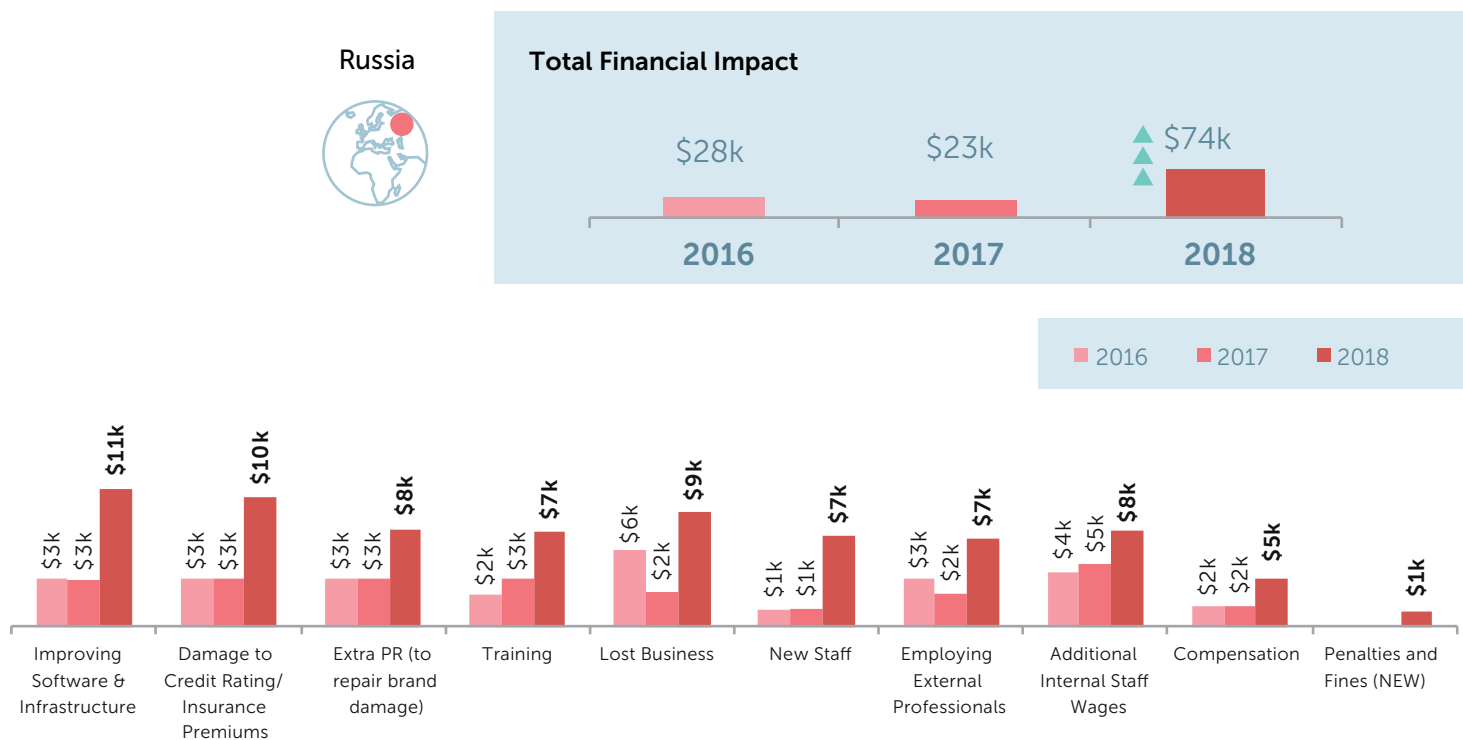


Figure 8: The financial impact of a data breach for SMBs in Russia

Finally, SMBs in APAC with China have to contend with loss business following a data breach, costing them an average of \$17k and suggesting that local customers are particularly unforgiving towards those businesses that suffer a breach.

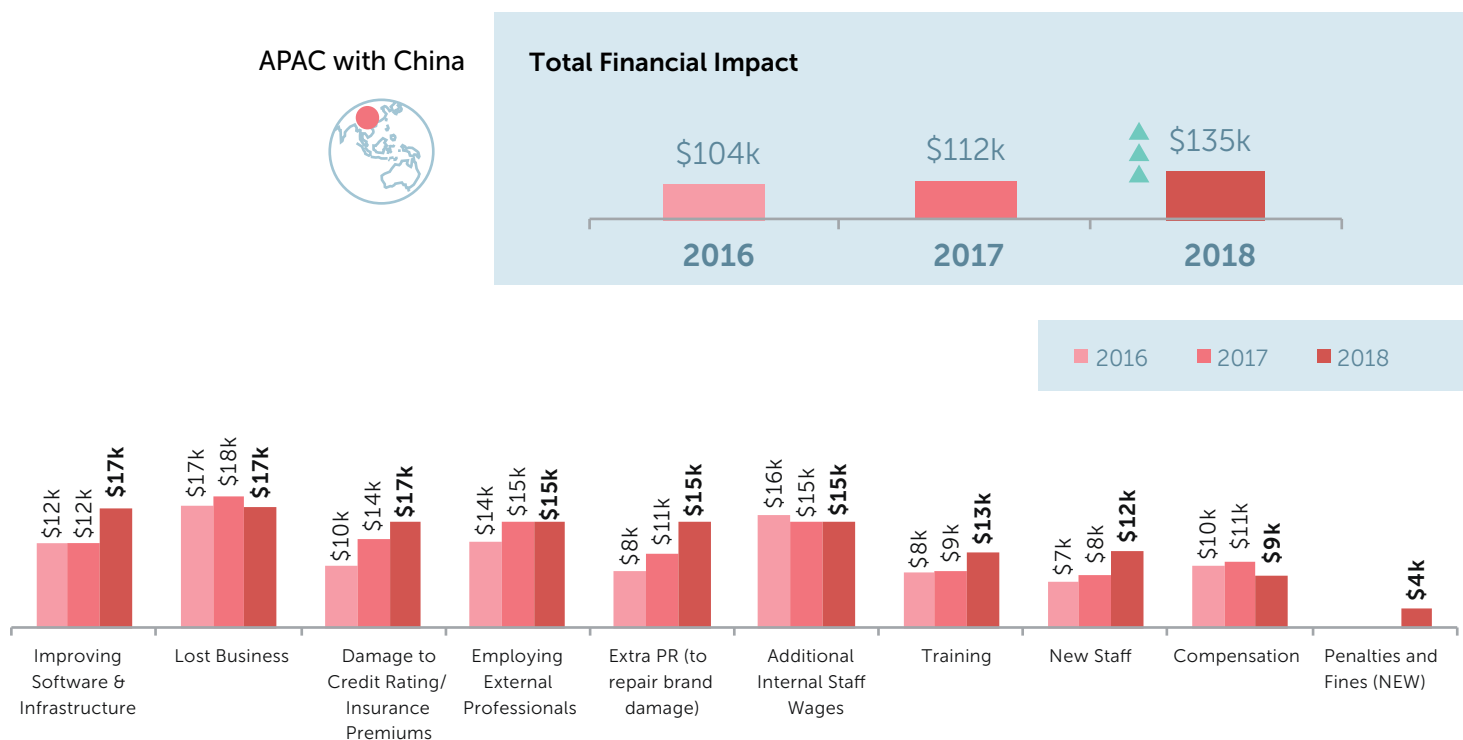


Figure 9: The financial impact of a data breach for SMBs in APAC with China

The costliest attacks: All about data on the go



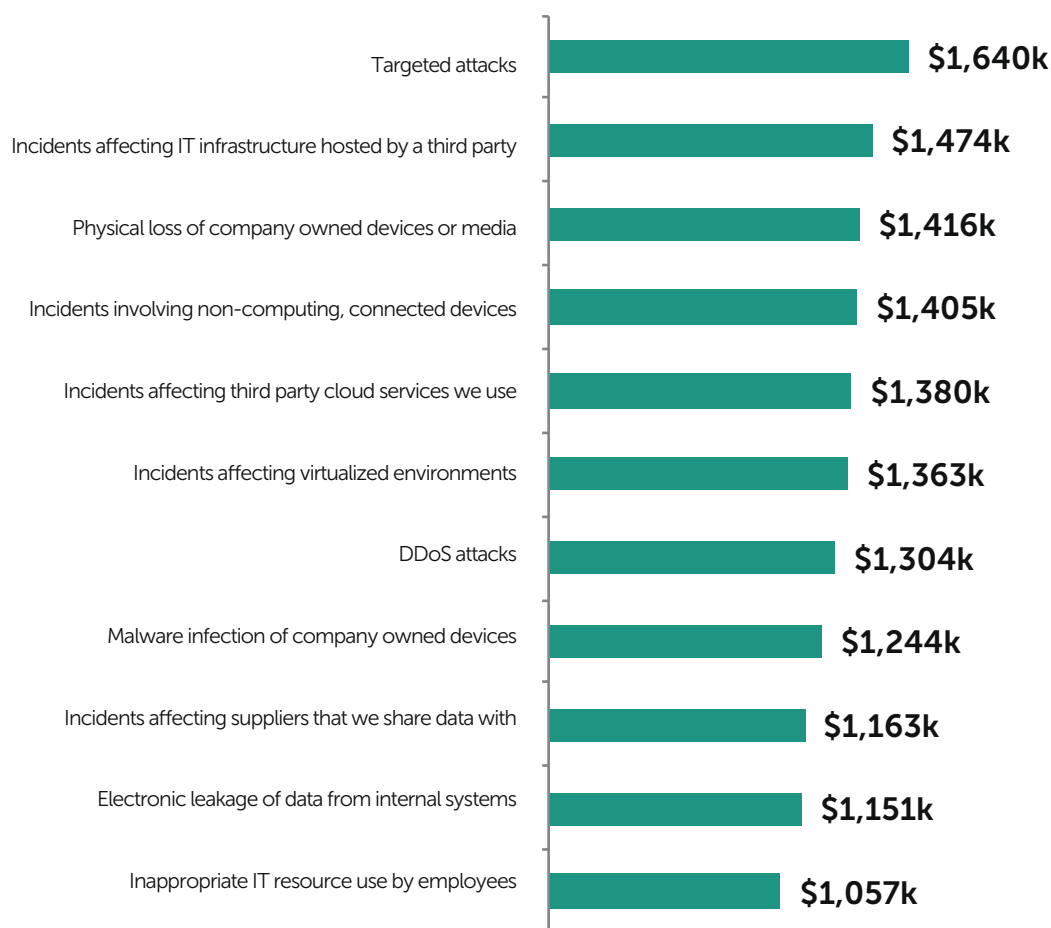
It's not just enough to know how much a data breach costs. Additional insight can come from understanding the different types of threats businesses are facing and which – if successful – are the most expensive to recover from. **The top five types of data breaches with the biggest financial impact for enterprises were:**

- 🎯 Targeted attacks - **\$1.64m**
- 🖥️ Incidents affecting IT infrastructure hosted by a third party - **\$1.47m**
- 📱 Physical loss of company owned devices or media - **\$1.42m**
- 🖨️ Incidents involving non-computing connected devices - **\$1.41m**
- ☁️ Incidents affecting third party cloud services we use - **\$1.38**

In comparison, the top five for SMBs were:

- 🖥️ Incidents affecting IT infrastructure hosted by a third party - **\$179k**
- 🖨️ Incidents involving non-computing connected devices - **\$148k**
- 🤖 Incidents affecting virtualized environments - **\$146k**
- ☁️ Incidents affecting third party cloud services we use - **\$130k**
- 🔒 Incidents affecting suppliers that we share data with - **\$130k**

Enterprise



SMB

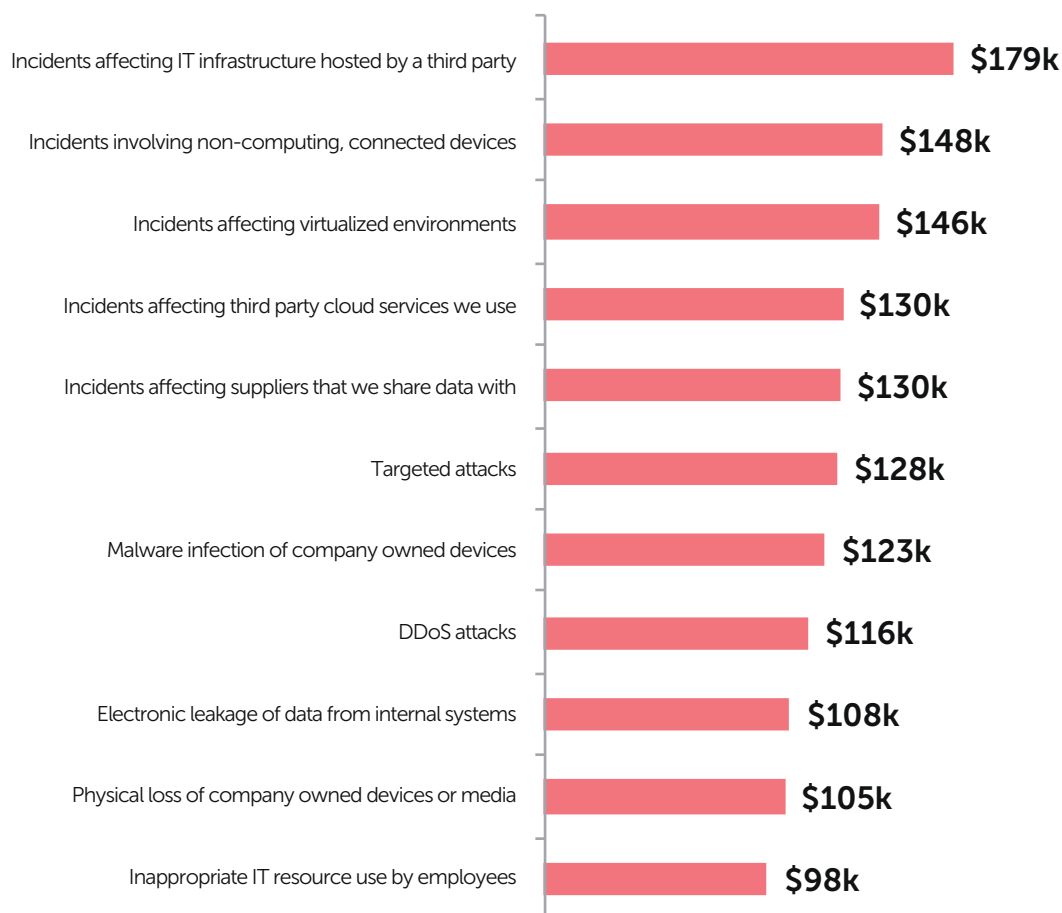


Figure 10: Types of data breaches and their financial impact

When undergoing digital transformation strategies, businesses often work with third parties to migrate data or change the access to their infrastructure. Businesses have to trust that their external providers are taking the necessary security precautions.

However, the costly nature of data breaches stemming from third parties shows that this trust is often misplaced, as any failings on the provider's side will also directly impact the customer.

When it comes to all cybersecurity incidents, the picture is very similar, with third parties being the source of the most costly types of incidents. **The top five affecting enterprises were:**

 Targeted attacks - **\$1.11m**

 Incidents affecting IT infrastructure hosted by a third party – **\$1.09m**

 Incidents involving non-computing connected devices - **\$993k**

 Incidents affecting third party cloud services we use - **\$942k**

 Electronic leakage of data from internal systems - **\$909k**

For SMBs, the top five were:

 Incidents affecting IT infrastructure hosted by a third party - **\$118k**

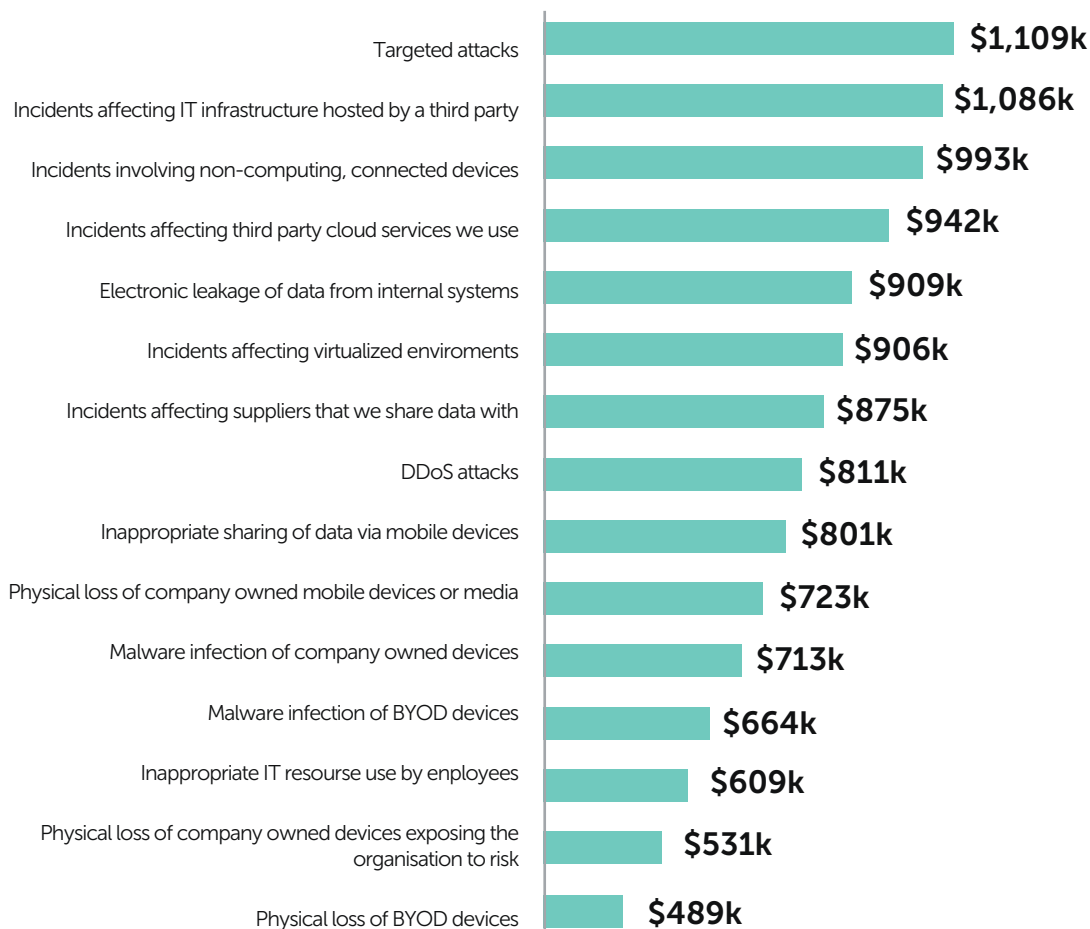
 Incidents involving non-computing connected devices - **\$98k**

 Incidents affecting third party cloud services we use - **\$89k**

 Targeted attacks - **\$87k**

 Incidents affecting suppliers that we share data with - **\$83k**

Enterprise



SMB

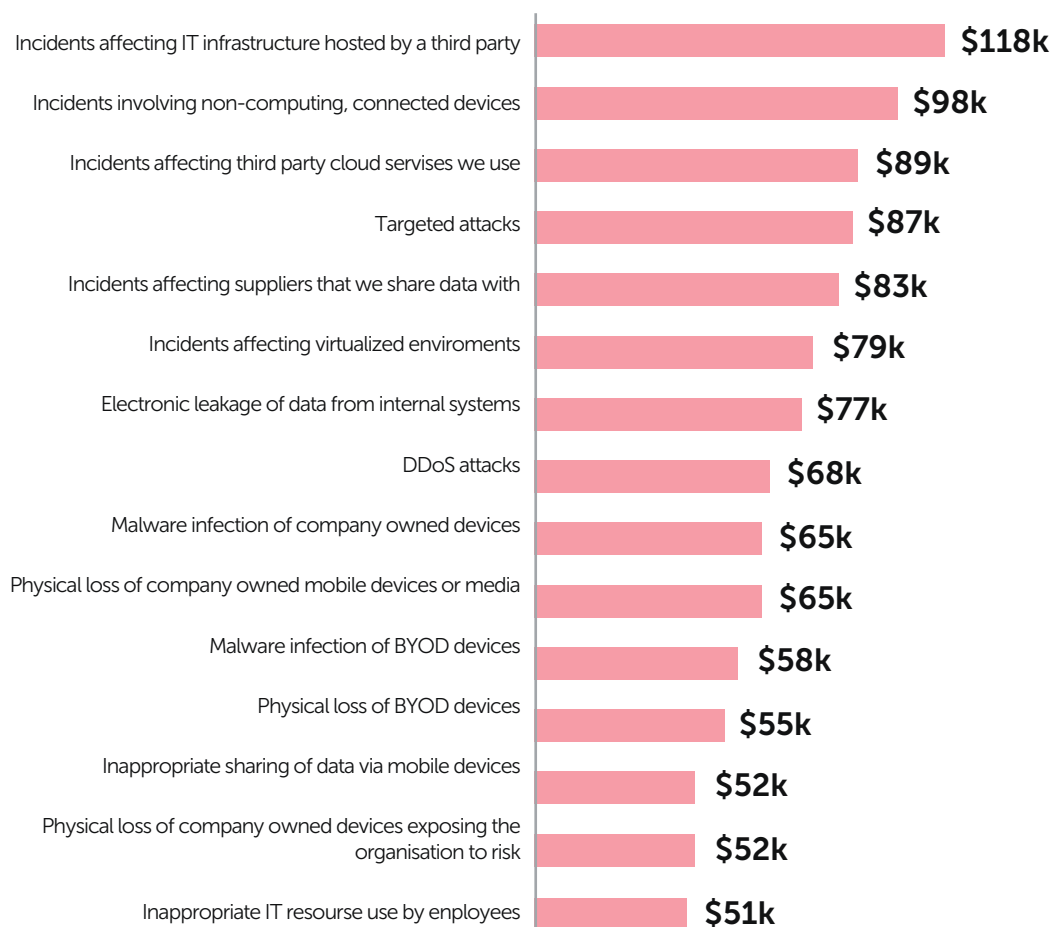


Figure 11: Types of cybersecurity incidents and their financial impact

IT security has a place on the boardroom agenda

With data breaches and security incidents costing businesses more and more every year, the importance of putting tools and processes in place to defend against cybercriminal activity is becoming ever-more important. This trend is reflected in the amount of money enterprises and SMBs are spending on IT security.

Indeed, IT security budgets have increased across all company sizes over the last 12 months. In enterprises, the percentage of the overall IT budget being spent on security has risen from 23% in 2017 to over a quarter (26%) in 2018, equating to an average of \$8.9 million.

A similar pattern can also be seen in both SMBs and VSBs. SMBs now spend an average of \$246k a year on IT security, comprising 23% of the overall IT budget as opposed to 20% in 2017. VSBs show the largest percentage increase, with security budgets rising from 16% (\$2k) to 20% (\$4k) of the total IT spend.

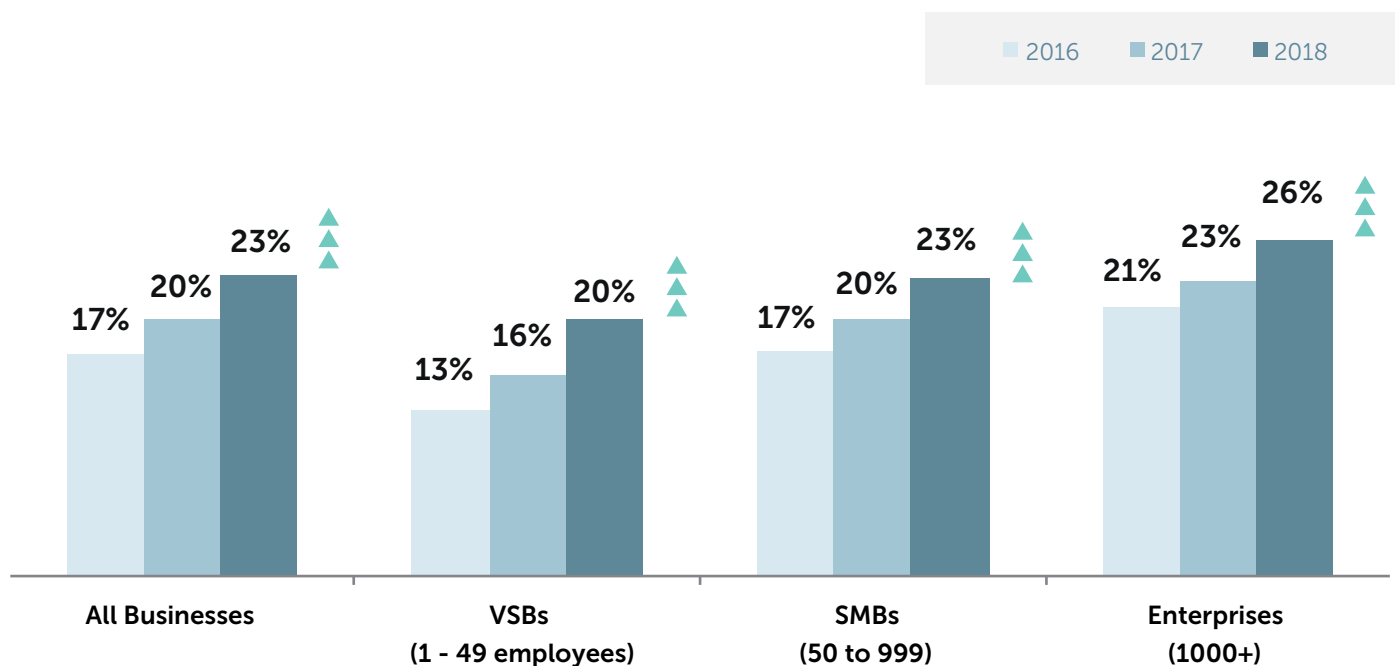


Figure 12: Tracking the percentage of IT budgets being spent on security

These findings are consistent across virtually all regions, but it's interesting to note that there are a few anomalies, particularly among enterprises in North America and the META region where proportions of the IT budget being spend on security showed the biggest increases from 2017. Enterprise budgets in North America grew by 9 percentage points to 28% of the total IT budget, while those in META showed an 8 percentage point increase to 27%.

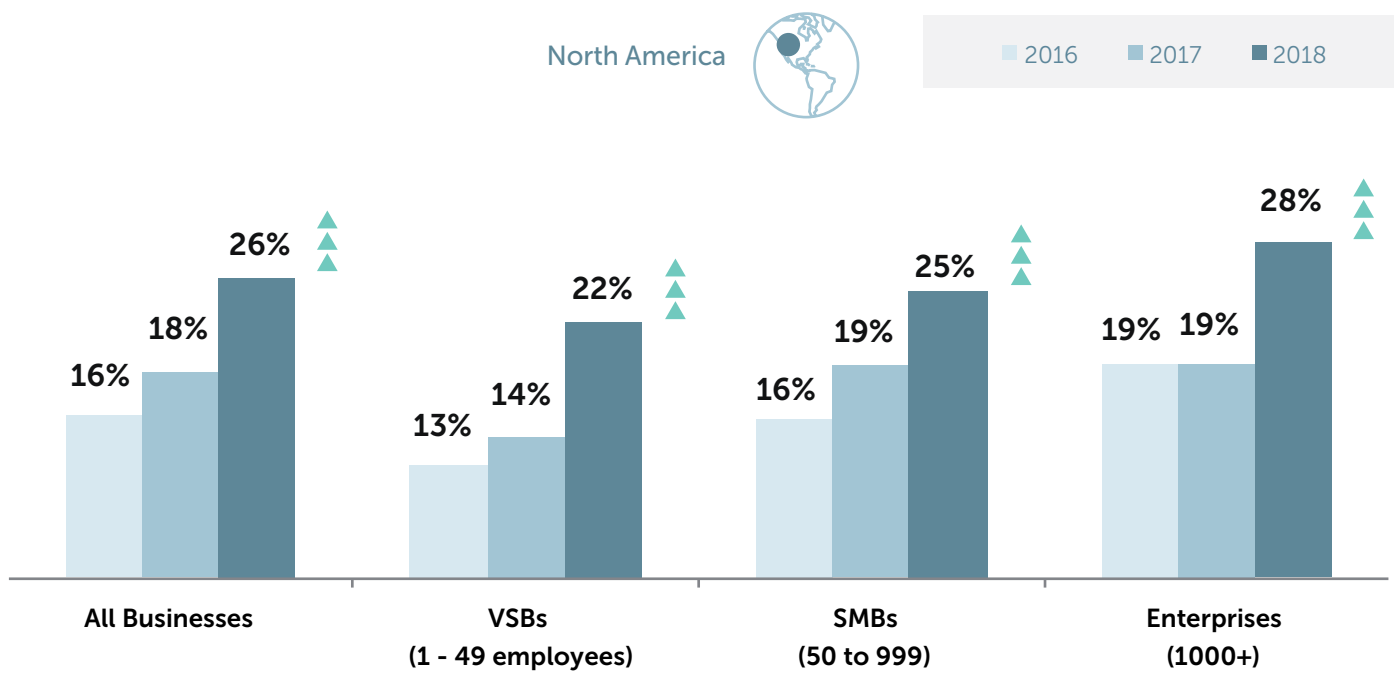


Figure 13: Tracking the percentage of IT budgets being spent on security in North America

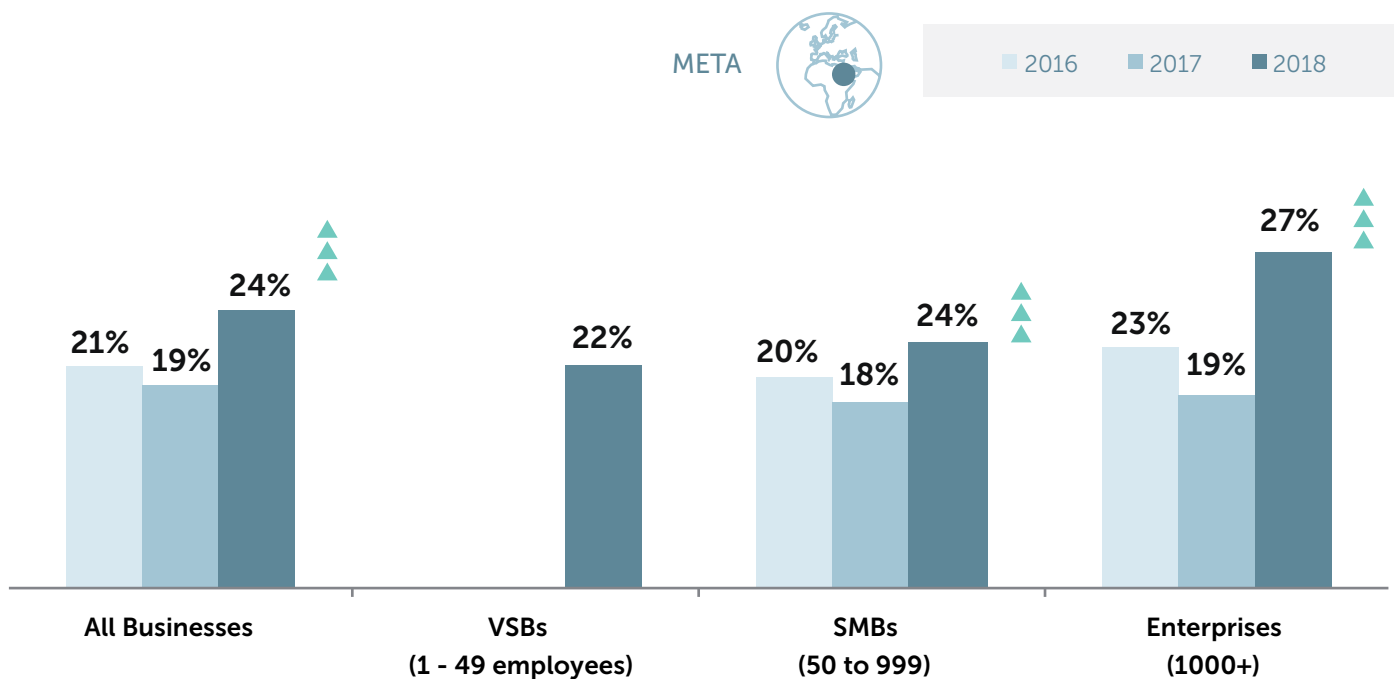


Figure 14: Tracking the percentage of IT budgets being spent on security in META

In comparison, the percentage of IT security budgets remained the same for both SMBs and enterprises in APAC with China (23% and 26% respectively), and enterprises in Japan (26%). This lack of movement could be explained by the fact that Japanese enterprises are spending an average of \$31.1m, which is significantly greater than any other region.

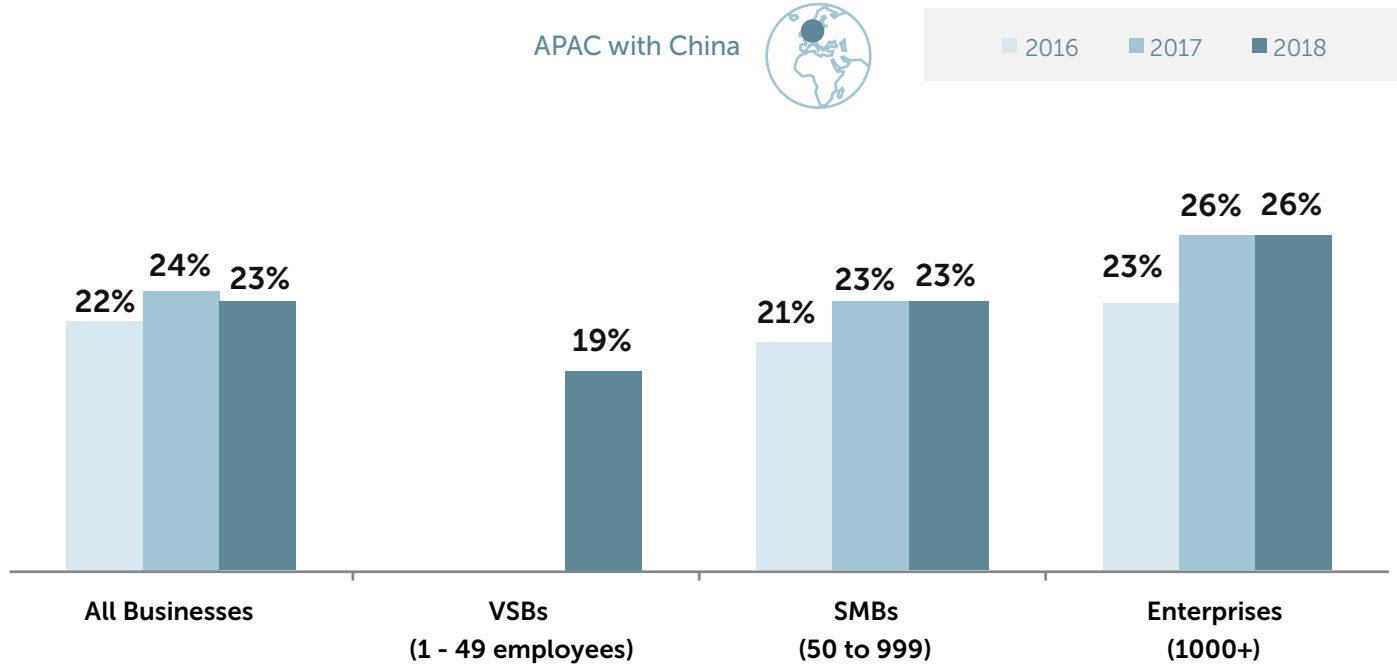


Figure 15: Tracking the percentage of IT budgets being spent on security in APAC with China

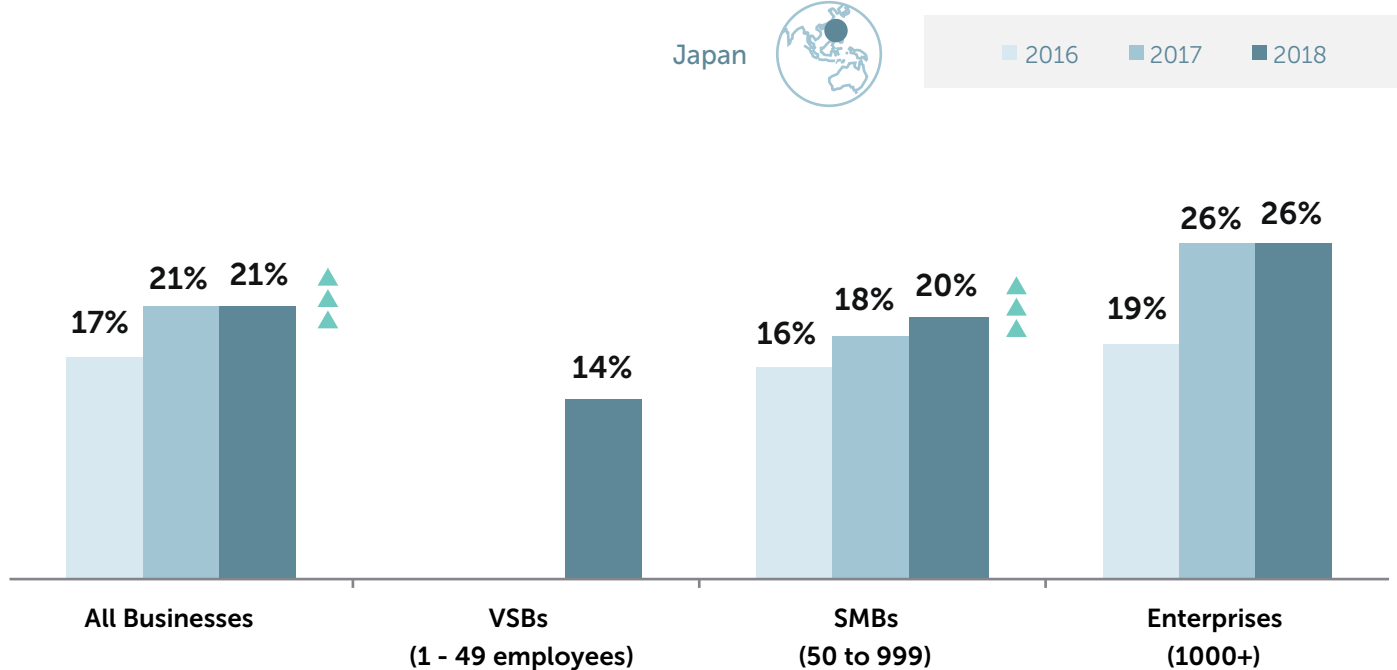


Figure 16: Tracking the percentage of IT budgets being spent on security in Japan

What's more, businesses still expect their IT security budgets to grow in the future. Globally, both VSBs and enterprises predict that the amount of money they spend on cybersecurity will increase by 15% over the next three years, while SMBs predict a 14% increase.

Again, there are some regional differences, such as SMBs in Japan predicting the smallest increase (7%) in their IT security budgets. At the other end of the scale, VSBs in LATAM predict their security budgets to increase by 22%, ahead of enterprises and SMBs in META (19%) and Russia (18%).

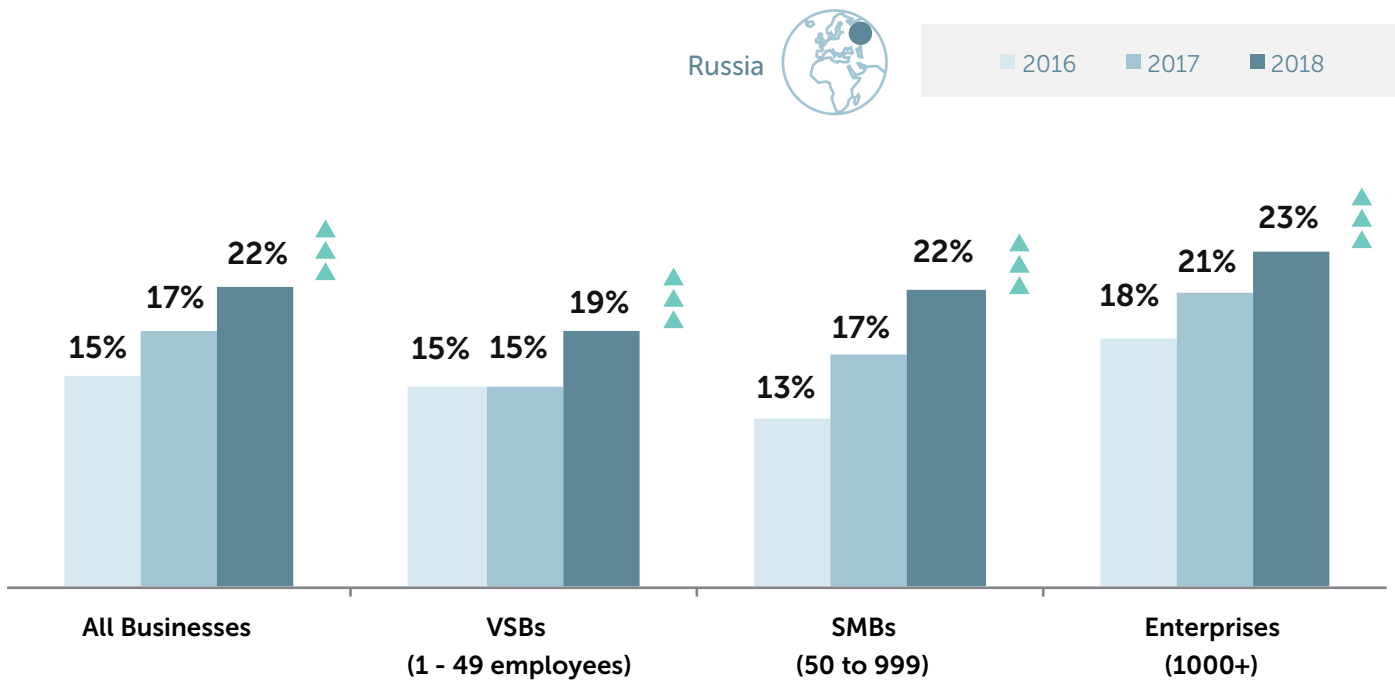


Figure 17: Tracking the percentage of IT budgets being spent on security in Russia

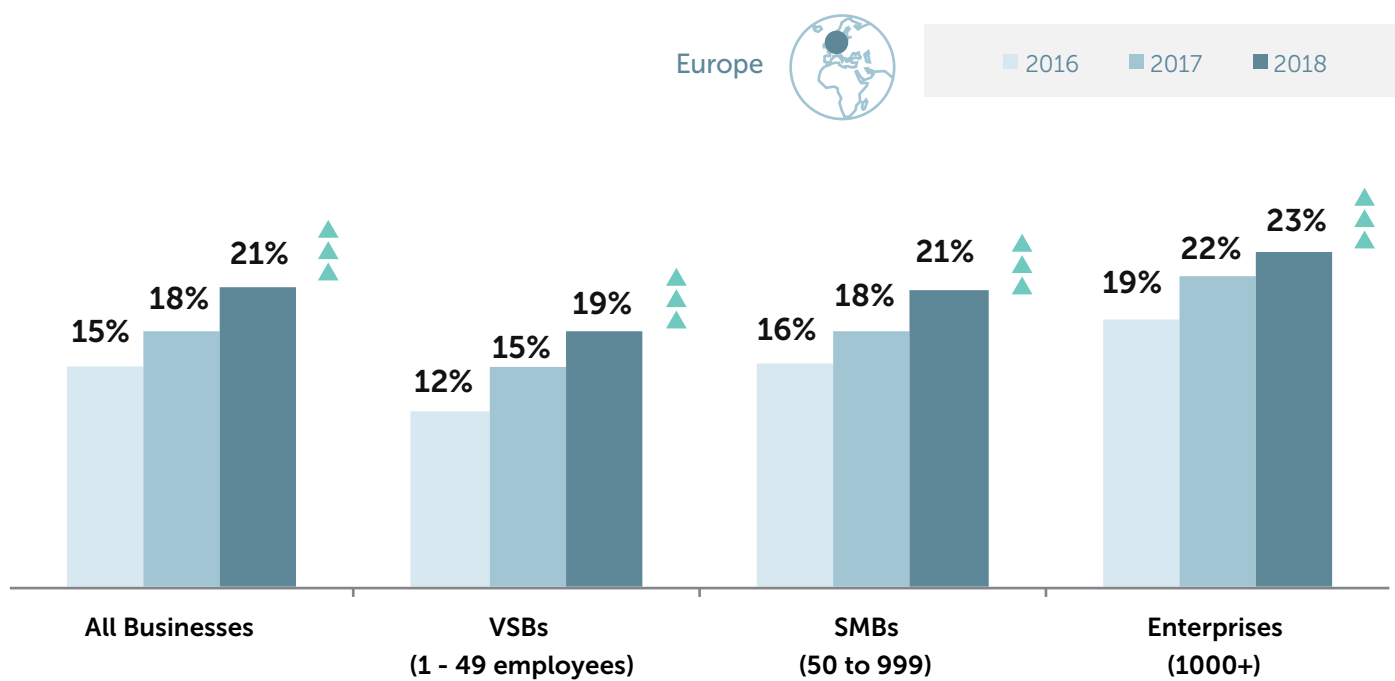


Figure 18: Tracking the percentage of IT budgets being spent on security in Europe

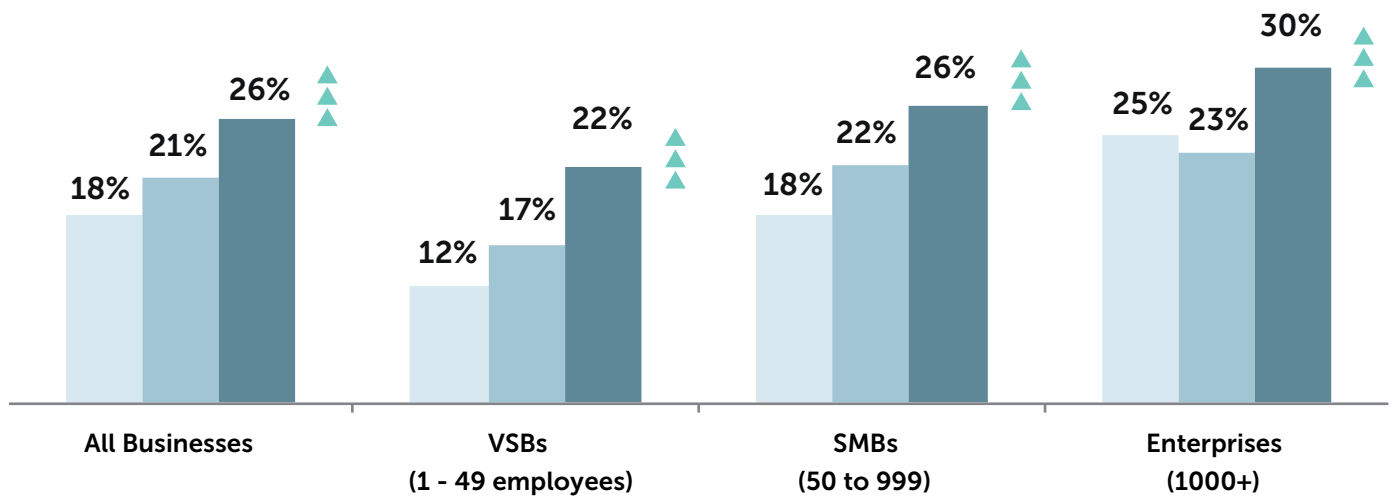


Figure 19: Tracking the percentage of IT budgets being spent on security in LATAM

Motivations for investing in IT security



With different company sizes, different industries and diverse needs to take into consideration, the key question we wanted to ask businesses was exactly what motivates them to invest in cybersecurity?

With IT budgets widely expected to continue growing over the next three years, businesses are clearly aware that there is a definite need to invest in IT security both now and in the future. As our survey discovered, there are some clear factors that are motivating businesses to put their money where it is needed.

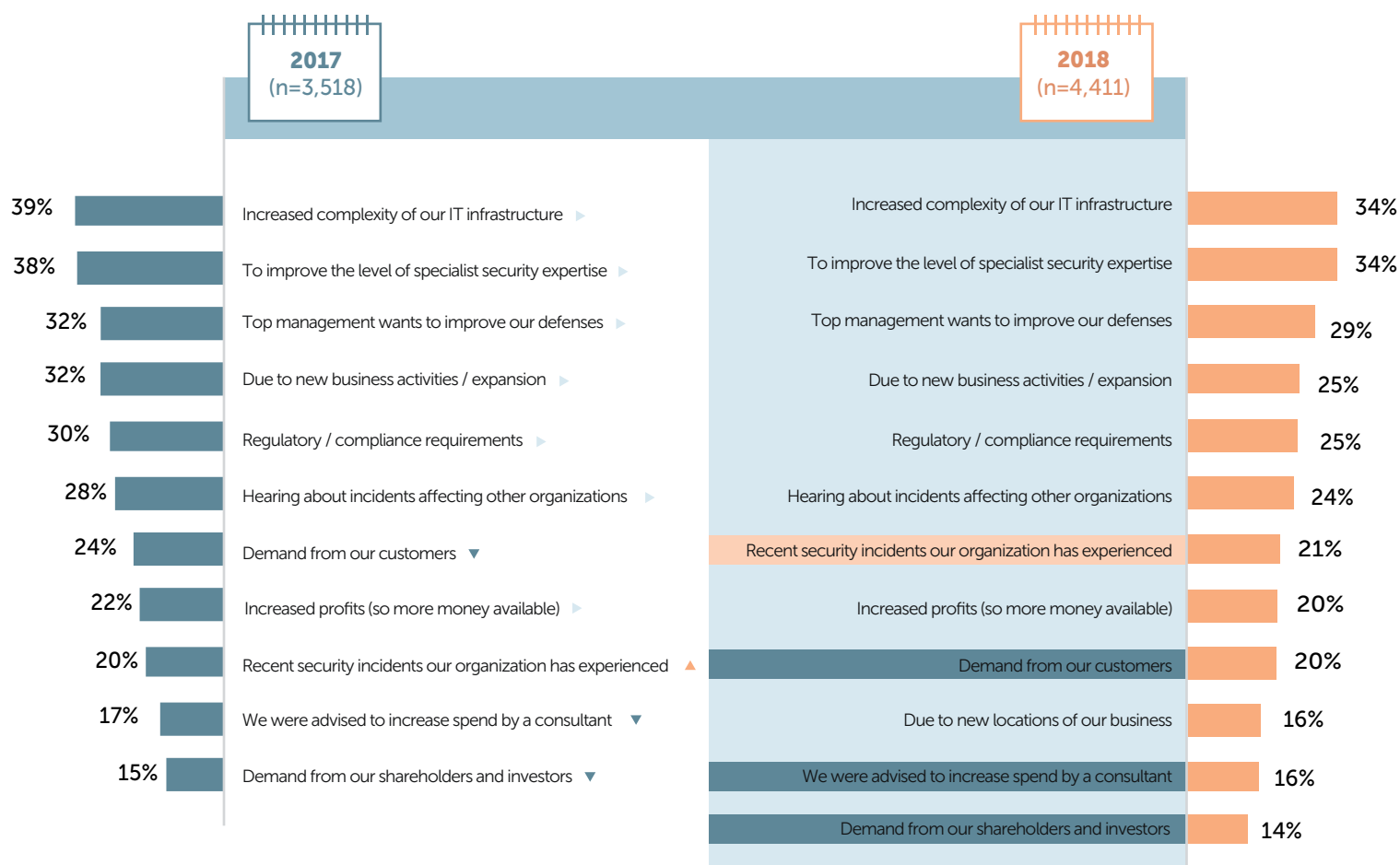


Figure 20: Top three motivations to invest in IT security across regions

As the figure above shows, the increased complexity of IT infrastructure retained its position at the top and jointly ranked with improving the level of specialist security expertise (both 34%) as the biggest motivators for investing in IT security across all regions. They are closely followed by pressures from top management (29%) – suggesting that business leaders are taking a greater interest in cybersecurity – and the impact of new business activities as well as compliance requirements (both 25%).

Demand from shareholders and investors (14%) was identified as the smallest motivator of IT security investment, just behind those businesses that were advised to increase their security spend by a consultant (16%).

As this is an area where regional factors can have a significant influence, we also looked at the top three motivators for each region to identify the similarities or differences that could go towards explaining how different businesses perceive the importance of cybersecurity.

Unsurprisingly, the increased complexity of IT infrastructure appeared in the top three motivators across all regions, being the number one motivator in North America (34%), LATAM (33%) and Europe (29%).

Improving the level of specialist security expertise was equally as prevalent and the biggest motivator of investment in four of the regions included in the study – Japan (48%), APAC with China (41%), META (37%) and Russia (36%). This is likely to be down to the widely-discussed skills gap in the cybersecurity industry. Security experts are still in short supply, meaning businesses in all sectors are struggling to find people with the skills to be able to counter today's most sophisticated cyberattacks.

	Russia ++	North America	META	ACAP with China	Japan	LATAM	Europe
TOP-1 	To improve the level of specialist security expertise (36%)	Increased complexity of our IT infrastructure (34%)	To improve the level of specialist security expertise (37%)	To improve the level of specialist security expertise (41%)	To improve the level of specialist security expertise (48%)	Increased complexity of our IT infrastructure (33%)	Increased complexity of our IT infrastructure (29%)
TOP-2 	Increased complexity of our IT infrastructure (33%)	To improve the level of specialist security expertise (31%)	Top management wants to improve our defenses (29%)	Increased complexity of our IT infrastructure (41%)	Increased complexity of our IT infrastructure (34%)	To improve the level of specialist security expertise (28%)	To improve the level of specialist security expertise (27%)
TOP-3/4 	Top management wants to improve our defenses (29%)	Top management wants to improve our defenses (30%)	Increased complexity of our IT infrastructure (29%) Hearing about incidents affecting other organizations (28%)	Top management wants to improve our defenses (35%)	Regulatory / compliance requirements (26%)	Due to new business activities / expansion (26%) Top management wants to improve our defenses (25%)	Regulatory / compliance requirements (25%) Top management wants to improve our defenses (24%)

Figure 21: Tracking the percentage of IT budgets being spent on security in META

The growing role IT security is having in the boardroom is also clearly evident. Pressures from upper management came in as the second-biggest motivator for businesses in the META region (29%) and the third or fourth-biggest motivator in five other regions – APAC with China (35%), North America (30%), Russia (29%), LATAM (25%) and Europe (24%).

The findings also indicate that regulatory changes are having a financial effect for businesses in certain regions. A quarter (25%) of European businesses identified regulatory/compliance requirements as being a key driver of cybersecurity investment, which is not surprising given the attention around GDPR, which comes into force in May 2018.

Businesses in Europe are likely taking a long-term view when it comes to achieving compliance. With GDPR fines able to reach a maximum of **€20 million** or 4% of the company's global annual turnover, investing in IT security now could actually save firms a huge amount of money in the long run.

The same is true for businesses in Japan. The Japanese government recently updated its Act on the Protection of Personal Information – one of Asia's oldest data protection laws – and established a new Personal Information Protection Commission (PPC) to govern business compliance.

Conclusion

Resoundingly, our study has shown that IT security is gaining a more strategic role in the modern business landscape.

One of the reasons for this is that the costs incurred from data breaches and security incidents are still on the rise – the highest they have ever been at **\$1.23m** for enterprises and **\$120k** for SMBs. This alone should be enough to make any firm see the financial value of getting cybersecurity tools in place.

But, our research clearly shows that the threat of costs isn't the only factor driving security onto the boardroom agenda. IT is also playing an ever more important role in business, with businesses increasingly looking toward digital transformation strategies to keep up with competition and consumer expectations. In this environment, a system glitch or IT incident could have a swift and direct impact on revenue streams.

Business leaders are increasingly understanding that if their digital transformation strategy – ie, their move to the cloud, their migration to a new platform or their upheaval of existing working practices - is put at risk, so too is the business itself.

Ultimately, for many businesses, it comes down to one simple question: will making IT security a more strategic investment, actually end up paying the company dividends in the long run?

The answer, it appears, is a resounding 'yes'.