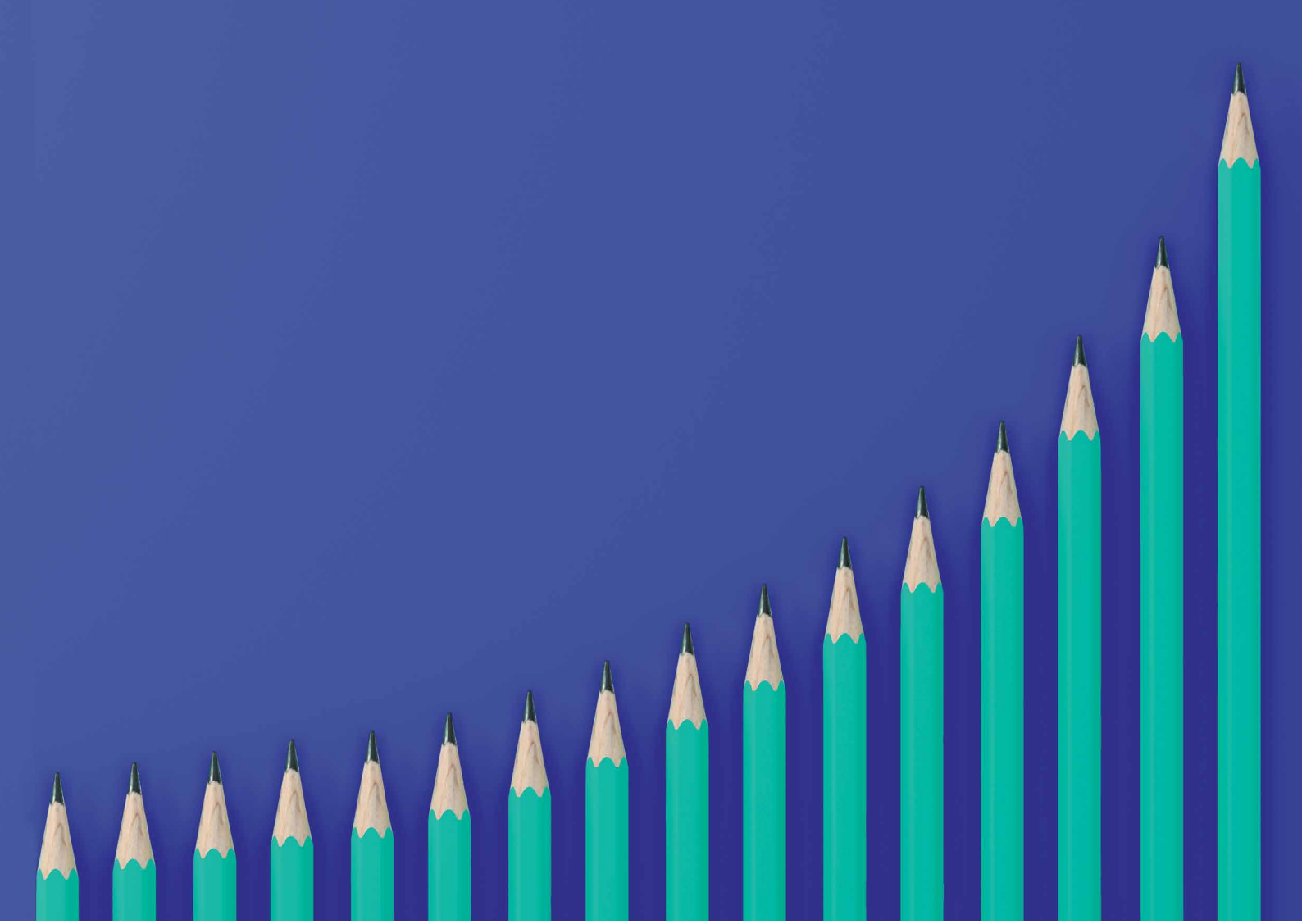


How businesses are losing money and saving costs amid cyberattacks

IT security economics in 2019

kaspersky BRING ON THE FUTURE

Contents

Methodology

4,958 interviews

23 countries

The Kaspersky Global Corporate IT Security Risks Survey (ITSRS) is a global survey of IT business decision makers, which is now in its 9th year. A total of 4,958 interviews were conducted across 23 countries. Respondents were asked about the state of IT security within their organizations, the types of threats they face and the costs they have to deal with when 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 SMBs (small & medium sized businesses with 50 to 999 employees), or Enterprises (businesses with over 1,000 employees). Not all survey results are included in this report.

All financial consequences and costs of cyberattacks mentioned in this report are only related to incidents that, according to the survey respondents, have led to data breaches.

Introduction

It's estimated that in the first half of 2019 alone there have been nearly 4,000 data breaches, putting more than four billion users' data at risk.

As business leaders strive to future-proof their organizations from cyberthreats, Kaspersky continues to work towards building a safer world. This involves understanding how enterprises and small and medium businesses can continue to identify vulnerabilities and protect themselves from sophisticated attacks.

It's estimated that in the first half of 2019 alone there have been nearly 4,000 data breaches, putting more than four billion users' data at risk. Organisations have continued to be hit by high-profile, and costly cybersecurity beaches throughout the last 12 months. This year, Gartner has revealed that IT security and infrastructure budget investment has continued to grow. Worldwide IT spending is projected to total $3.74 trillion in 2019 as businesses respond to number of growing threats to their systems, business operations and finances.

Given that businesses are still proving to be vulnerable to cyberattacks, it's clear that more needs to be done so they adapt to a fast-moving and ever-increasing threat landscape. As they strive to achieve this, we can see that businesses are continuing to invest in their IT security and systems. With the Financial Services Information Sharing and Analysis Center advising that businesses should be asking for greater budgets to tackle cybersecurity, it's clear that organizations need to bolster their businesses to mitigate long-term risks and protect from anticipated attacks in the future.

Building on our annual research into the economy of the IT security industry, this report reflects on survey results from the past 12 months to highlight how organizations are investing their IT security budget. It looks at how businesses are losing money and saving costs amid cyberattacks as well as how they are affected by the threat landscape and the ways they are responding to these incidents, both financially and operationally.

Key findings

More than a third (38%) feeling they lack sufficient insight on the threats facing their business

- Growing in confidence: more than half (55%) of organizations are completely confident that their network hasn't been hacked, despite more than a third (38%) feeling they lack sufficient insight on the threats facing their business
- Businesses are overlooking danger: only one-in-ten (12%) enterprises are concerned about malware infection, despite it being the costliest security incident for them, at $2.73m
- People power: 66% of both enterprises and SMBs are looking to increase their investment in specialist IT staff this year
- Forewarned but not forearmed: policies regulating third-party access aren't increasing enterprise protection, but simply treble the potential for compensation
- Play to your strengths: having an internal Security Operation Center nearly halves the financial impact of enterprise data breaches from $1.4 million to only $675k
- A DPO can save you money: more than a third (34%) of companies with a Data Protection Officer didn't lose money when they suffered a data breach

Businesses need to focus their attention on the costliest attacks

Increasingly, businesses of all sizes are feeling more confident that their network is safe.

Despite the fact that businesses are growing their IT security budgets, and the resources they put into monitoring threat incidents, many aren't aware of the attacks that are costing them the most money.

The number of businesses who say they feel "100% confident their network hasn't been hacked" is up more than 10% from 2016's report and a three percent growth year-on-year. However, despite this confidence, more than a third still believe they lack the sufficient insight or intelligence on the type of threats faced by their business.

This is reflected in the types of threats our respondents are most concerned are affecting their business. For enterprise businesses, malware infection on company-owned devices is actually the form of data breach with the biggest financial impact, costing $2.73 million this year, despite only a small percentage of enterprises feeling very concerned about malware infection as a threat.

SMBs too are ignoring their most expensive forms of attack. The costliest type of data breach for smaller businesses are incidents affecting IT infrastructure hosted by a third party, adding up to $162k. However, SMBs only ranked this as the fifth most important measure, and instead are most concerned about data protection issues, such as the loss of a physical device, or data loss though a targeted attack.

Investing in people, not systems

Last year's report saw many businesses embarking on digital transformation projects to overhaul systems and defend their systems from cyberattacks, particularly cloud-based breaches. This year's results however, reveal that businesses are increasingly investing in their people and resources to ready themselves for more attacks and prepare their IT departments for the future.

In 2019, enterprises have seen the highest rise of costs following incidents come from employing external professionals ($170k) and the hiring of new staff ($131k), which have increased by 35% and 24% respectively since 2018. At SMBs, new staff hiring costs remain unchanged at $11k, compared to spending falling elsewhere on different departments across the board. Yet, organisations face the challenge of being able to invest in expertise to build a more secure organization as the talent is not available to meet market demand.

Notably this is resulting in the bolstering of internal IT teams, rather than just the hiring of outsourced MSPs, bringing skills and expertise in-house.

Investing in dedicated resources, and trained experts in house, is also a way for businesses to save on costs in the long run following security attacks. As our research reveals, 34% of all companies with a dedicated, internal DPO (Data Protection Officer) didn't lose money when they suffered data breach. Our report makes clear that continual investment in people and internal expertise is becoming key for businesses to minimize financial losses and protect themselves from future incidents.

Security Operation Centers are becoming increasingly important

Interestingly, our study also found that maturity of IT systems pays in savings as a result of data breaches. Having an internal Security Operation Center nearly halves the financial impact of data breaches in enterprises, from $1.4 million to only $675k.

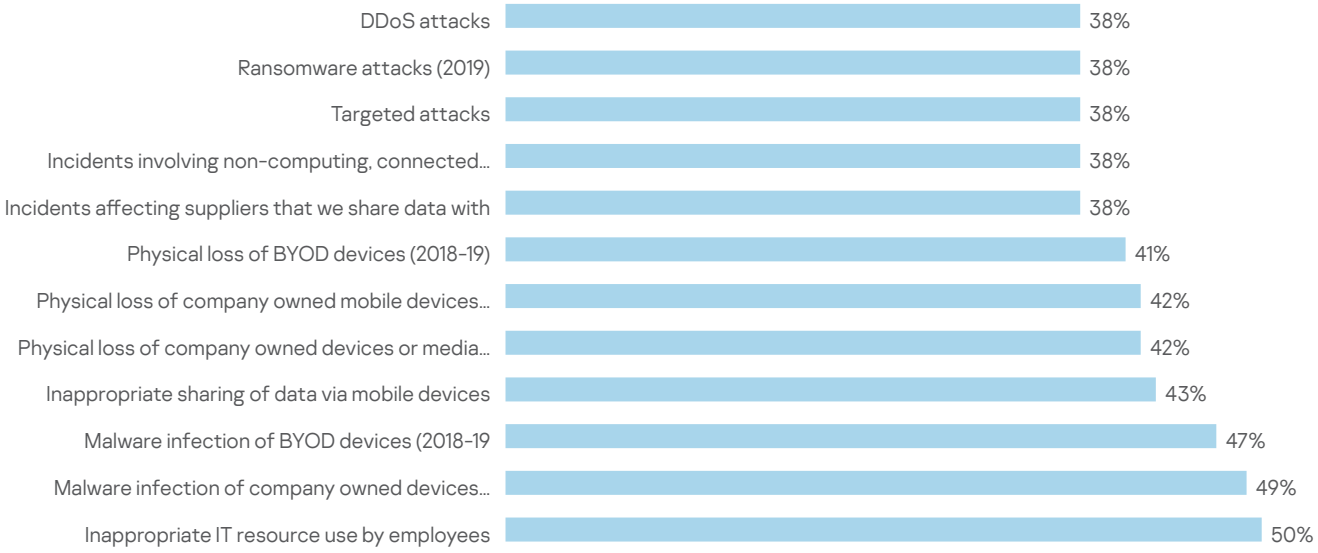
There are savings for upper SMBs who adopt an SOC as well, with the total financial impact of a data breach sitting at only $106k for those with an internal SOC, compared to $129k for SMBs overall. Although this saving isn't as pronounced, it still reduces costs by 22%, and this cost saving may be lower given that many SMB still use an external service for this function.

Read on, to find out more detail about the findings of the report.

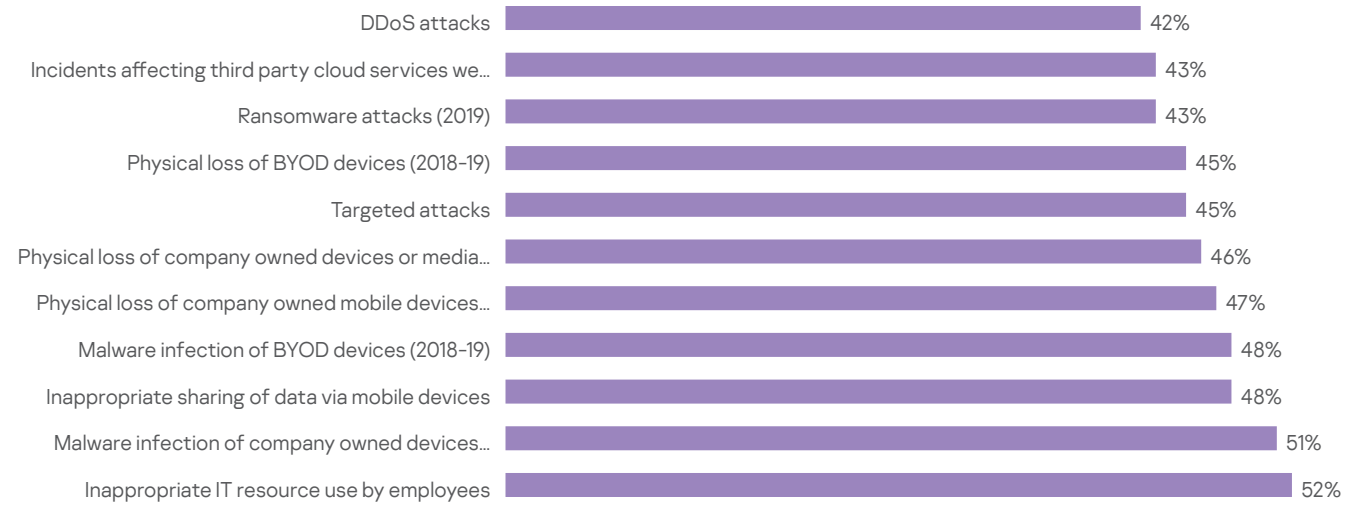
Inappropriate IT use leads to most frequent form of business data breach

Our 2019 report has revealed that both enterprises and SMBs were most frequently affected by incidents as a result of inappropriate IT resource use by employees (52% enterprise, 50% SMBs), followed by malware infection of company owned devices (51%, enterprise; 49% SMBs). This reflects that businesses could look at reducing the risk of data breaches with increased data security training for employees, to raise awareness of safe IT use.

The most frequent incidents targeting SMBs

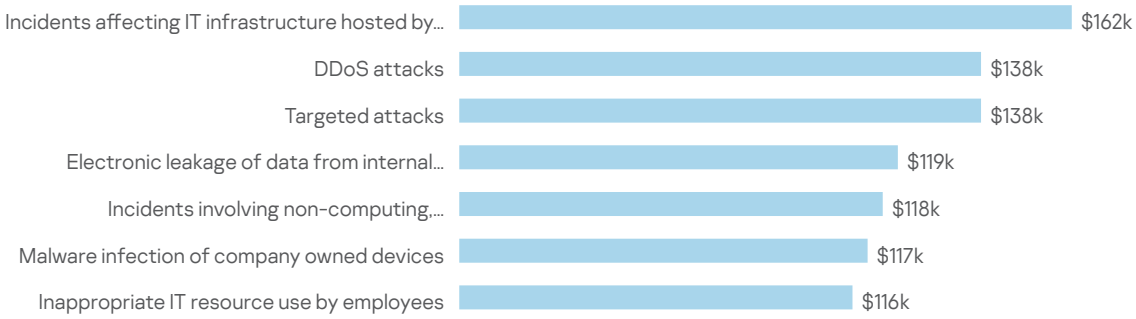


The most frequent incidents targeting enterprises



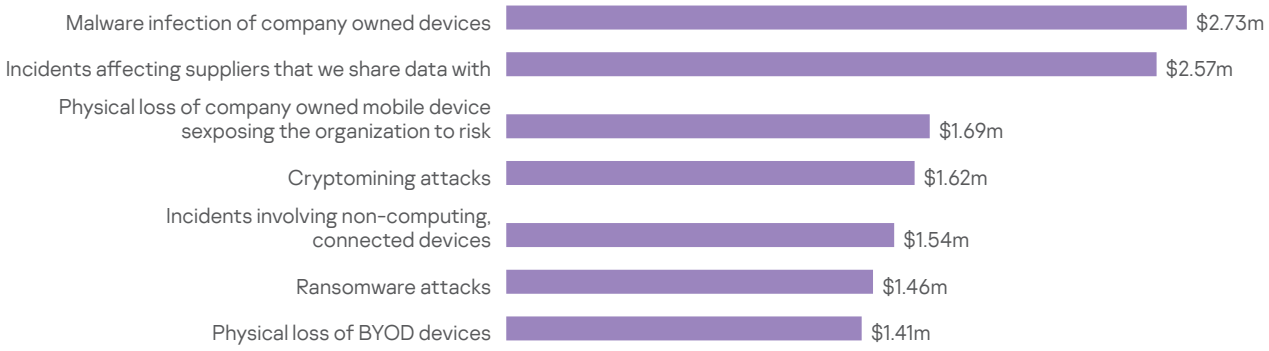
Surprisingly, in 2019, the most-costly data breaches for SMBs were actually not the most frequent forms if security incidents. The three most expensive attacks on SMBs this year were incidents affecting IT infrastructure hosted by a third party ($162k), DDoS attacks ($138k) and targeted attacks ($138k). However, in terms of frequency, these rank at only 16th, 12th and 10th places respectively in the list of security incidents most commonly targeting SMBs.

The average financial impact of data breaches by type for SMBs



Enterprises differ here, with the three most costly enterprise data breaches corresponding to their most frequent attacks: malware infection of company-owned devices ($2.73m), incidents affecting suppliers the company shared data with ($2.57m) and the physical loss of company-owned mobile devices ($1.69m) all feature in the top six in the list of most frequent security incidents. The costliest security incident for enterprises in 2019 was malware infection of company-owned devices. Notably, targeted attacks are only the fifth most expensive.

The average financial impact of data breaches by type for enterprises



However, when it comes to the incidents that worry businesses, enterprises are actually most concerned about losing data as a result of a targeted attack (23%) compared to viruses and malware (13%). Similarly, targeted attacks are the top concern of SMBs (23%), and the third most expensive form of data breach for SMBs at $138k.

This year, 47% of SMBs and 51% of enterprises agreed that it is becoming more difficult to tell the difference between a generic or a targeted security attack. This is making it harder for them to detect an incident among gray noise or evaluate the potential harm of the incident, which is possibly one reason why they are becoming susceptible to the growing levels of both moderate and advanced malware threats.

Overall, the cost for data breaches for enterprises has risen, with the financial impact of their average data breach reaching $1.41 million, up from $1.23 million the previous year. The greatest rises in costs stem from a growth in hiring external experts to secure a breach ($170k), and from the overall cost of lost business ($163k). Adding to this cost is the need for extra PR to repair brand damage after a breach ($161k).

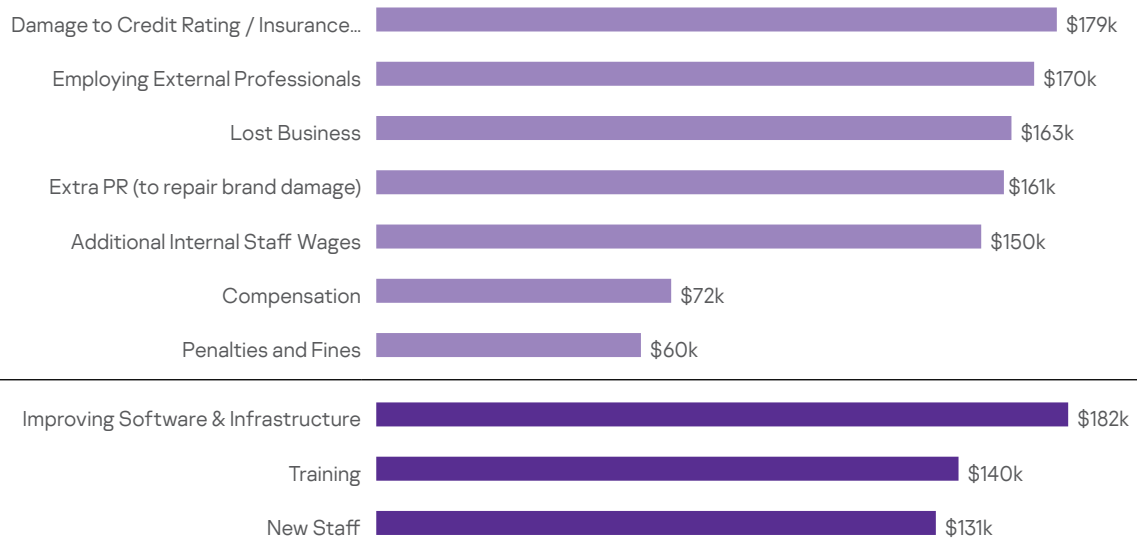
In comparison, SMBs have seen a total cost for data breaches of $108k, this is down from $120k in 2018[1], with less spent on compensation ($5k), lost business ($13k) and software and infrastructure ($13k).

1 The decrease in cost of data breaches for SMBs may be also influenced by the change of survey sample in 2019. Changing the sample structure in some verticals may introduce vertical specific needs.

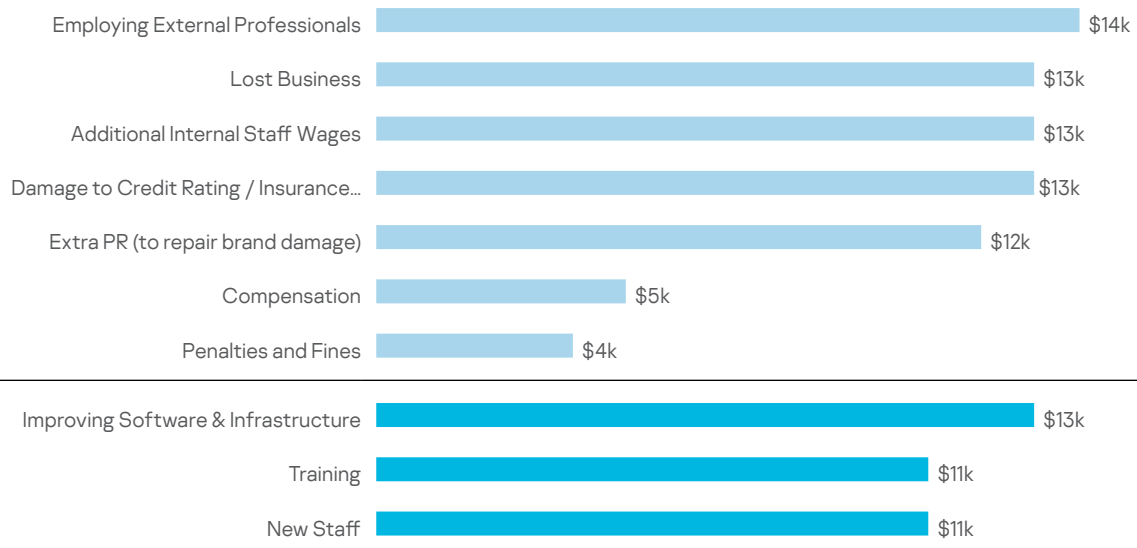
Companies pay for people, PR and lost business opportunities

When a business, whether an enterprise or an SMB, suffers a security attack, their increased business costs stem from a variety of fields, including penalties and fines, increased insurance premiums, new software and training. However, according to our research, external expertise and people power are the key drivers for the increase in business costs as a result of a cyberattack in 2019.

Breakdown of the average financial impact of a data breach for enterprises

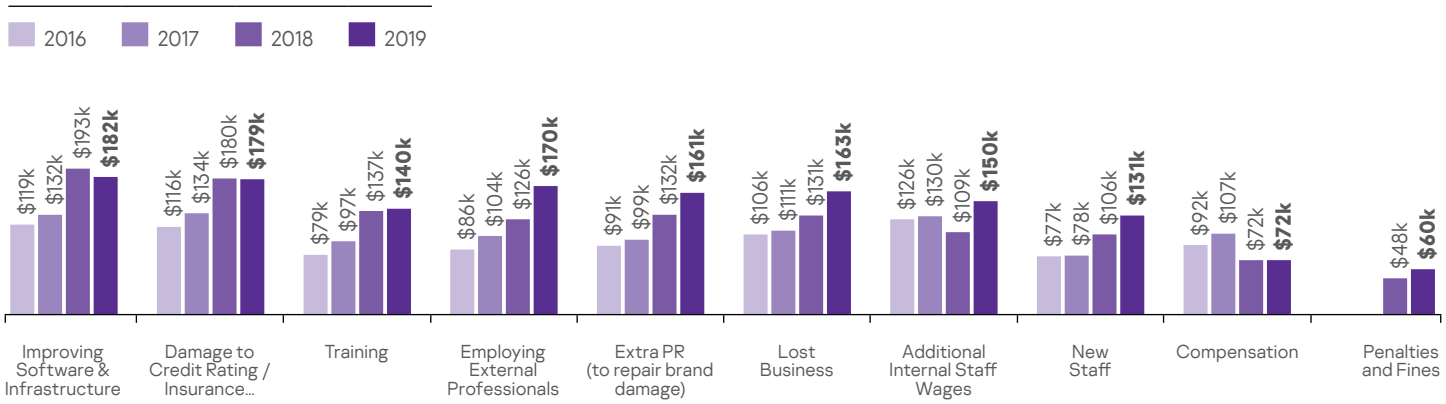


Breakdown of the financial impact of a data breach for SMBs



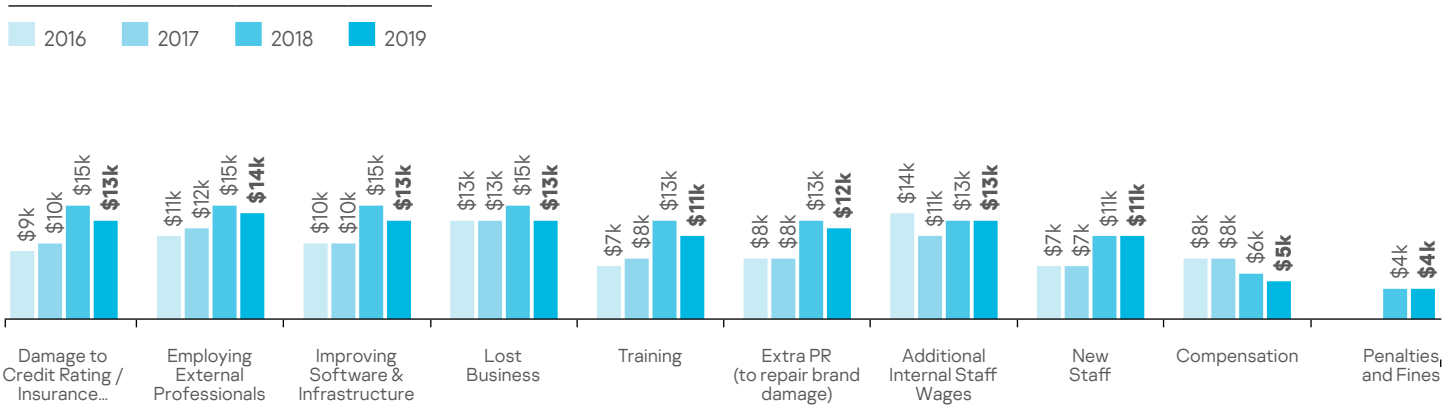
For enterprises, the most significant year-on-year increase in costs due to data breaches are in employing external professionals ($170k) and the hiring of new staff ($131k), which have increased by 35% and 24% respectively since 2018.

The average financial impact of a data breach for enterprises



Meanwhile for SMBs, their general levels of threat-related expenditure are falling. But spending for new staff remains unchanged at $11k, showing that SMBs are continuing to invest in team expertise to develop a higher state of security readiness.

The average financial impact of a data breach for SMBs

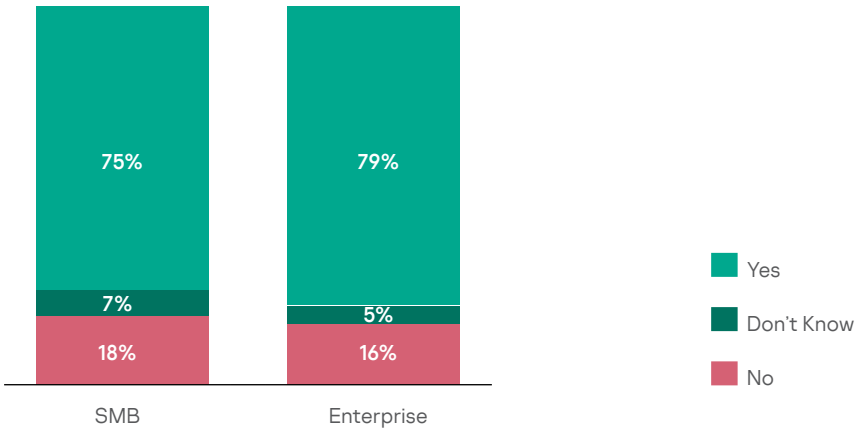


Losing new or existing business is also a notable cost point for businesses of all types who suffer an incident. This year, malware infection topped the list of the costliest financial breaches for enterprises, while SMBs were financially most affected by targeted attacks. In both of these cases the biggest costs for each industry came from lost business as a result of the attack, representing $331k of lost revenue for enterprises affected by a malware infection, and $22k for SMBs who experienced a targeted attack.

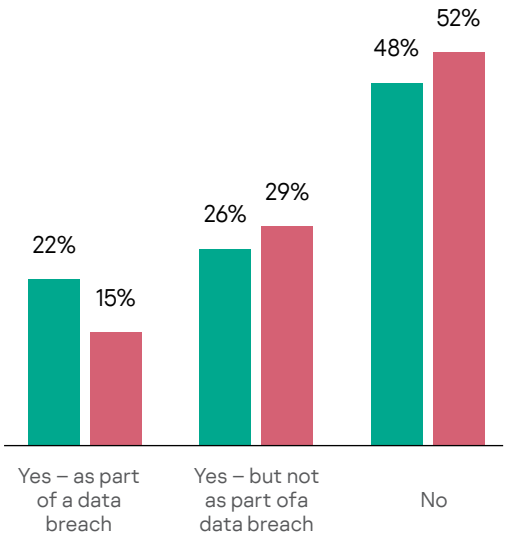
PR scandals and threat incidents: With corporate data breach scandals hitting the headlines more frequently, the public has become increasingly aware of incidents involving the security of their data. This can lead to a lack of trust and public confidence in companies, requiring businesses to invest in PR and crisis management to restore customer confidence in their brand. Our survey found that 31% of SMBs and 36% of enterprises experienced PR-related issues in 2019 because of data breaches, incurring additional financial impact as a result.

Increasingly businesses are introducing third party access policies, using them to mitigate the risks of security incidents, but do these policies actually make data breaches less likely? According to our research, 79% of enterprises and 75% of SMBs have put in place special policies to regulate the access of suppliers to their data.

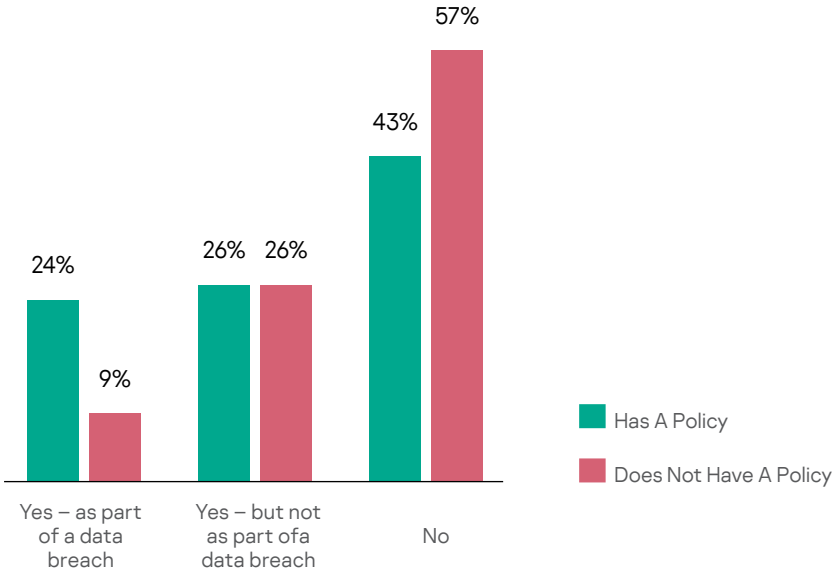
Are third parties subject to IT security policies?



Third party access policies and data breaches for SMBs

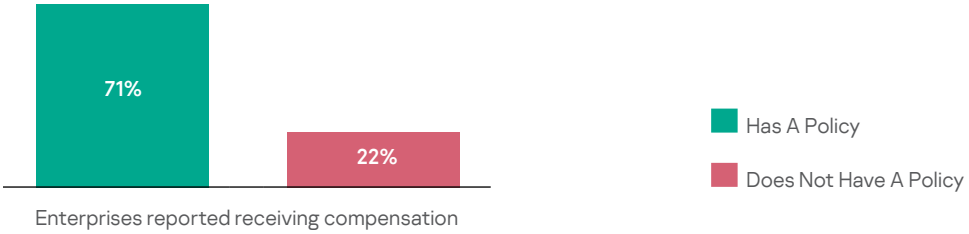


Third party access policies and data breaches for enterprises



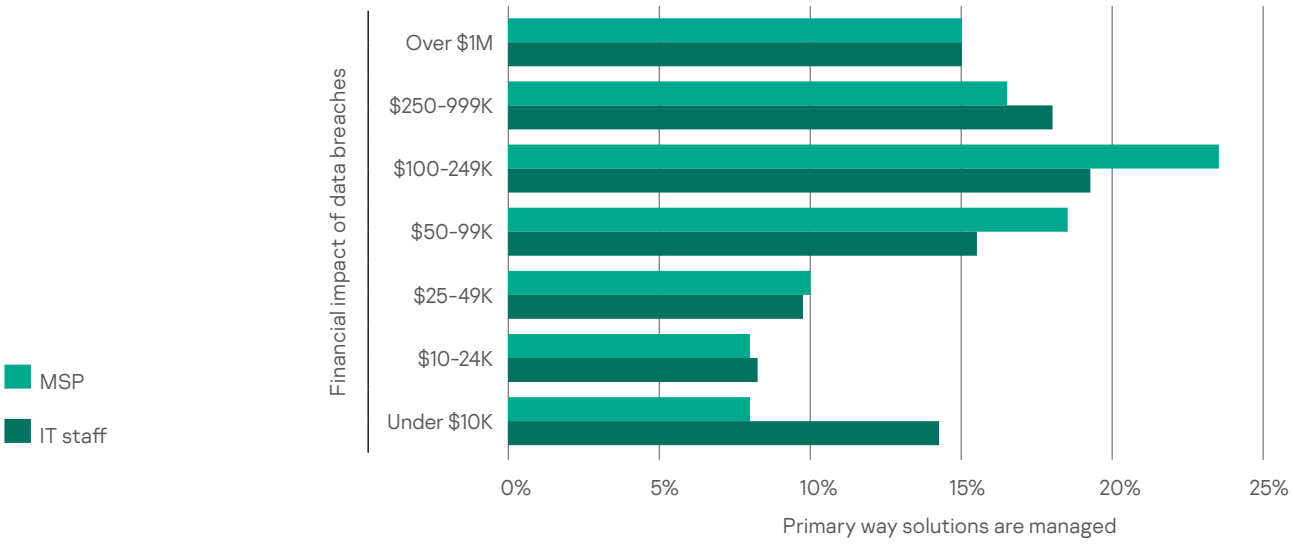
As the charts above reveal, it is clear these policies haven't made such incidents less frequent, they have boosted the likelihood of a company receiving compensation following a data breach involving a third-party. As the graph below shows, 71% of enterprises with a third-party policy reported they received compensation in 2019, compared to only 22% of companies who did not have a policy in place.

Third party access policies and compensation for Enterprises



When faced with growing costs for IT security, many organisations feel that outsourcing their IT teams can help save them money. However, careless or under-qualified cybersecurity service providers may actually increase a company's bill in the case of an incident. Of all companies that experienced a data breach with a financial impact of between $100k-249k, 23% were companies that use an outsourced MSP for security, while only 19% were businesses with in-house IT staff.

Total financial impact of data breaches: outsourcing vs internal management of IT security



Maturity leads to savings: Businesses with DPOs and SOCs minimize the costs of a breach
Organizations with a dedicated Data Protection Officer (DPO) are less likely to suffer financial loss. 34% of companies with a DPO didn't see a loss in revenue following their attack, compared to 20% of business who don't have this function. But of course, while it may help reduce losses, having this devoted role won't provide protection from data breaches.

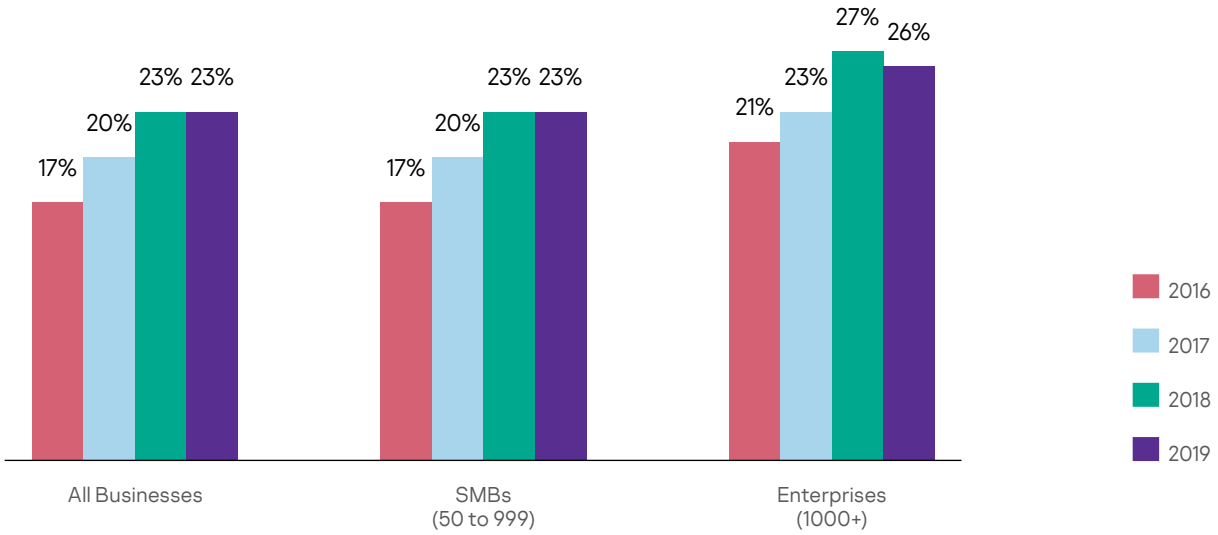
For enterprises, having an internal Security Operation Center can help to reduce the cost of data breaches significantly. In 2019, this was only $675k for SOC enterprises, compared to an average of $1.41m for businesses over all.

However, simply naming your company's current security team an SOC doesn't bring the same effect: our survey showed that if an SOC carries out general IT security functions, it doesn't affect the financial impact of a data breach. Dedicated training, expertise and systems are needed to see this cost saving after a breach.

How are IT security budgets changing?

According to Gartner, overall security spending in businesses is on the rise. This is confirmed in this year's survey with SMB spending reaching $267k compared to $256k in 2018. This is even more pronounced in enterprises where their security budget has more than doubled, reaching $18.9m, up from $8.9m last year. This is expected to grow by a further 11% over the next three years.

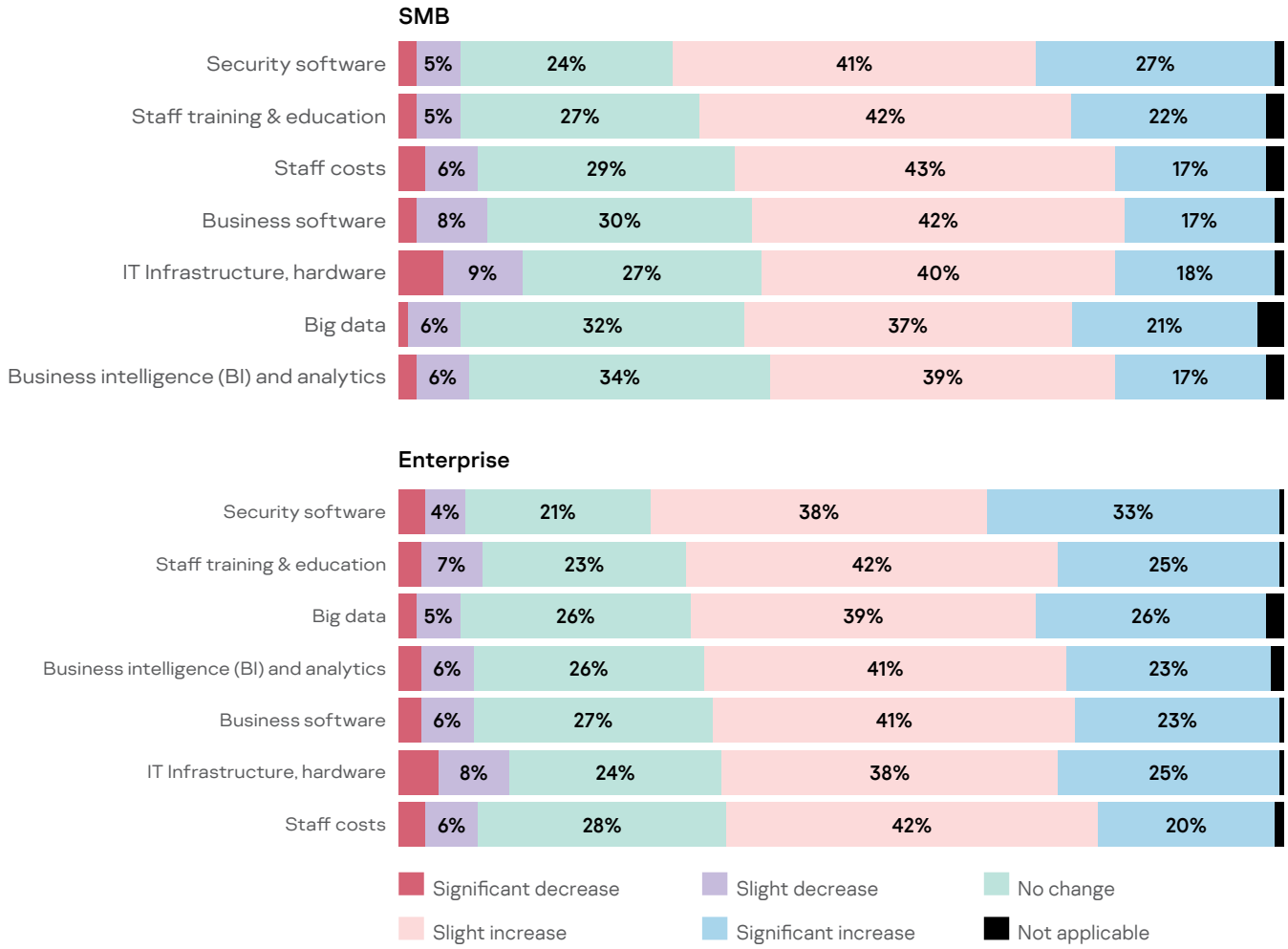
The proportion of IT budget allocated to IT security



Despite this rise, IT security budgets aren't taking up a larger percentage of companies' wider IT budgets. This year, the overall proportion of IT security as a percentage of overall IT spending has stayed even at SMBs with a steady 23% in both 2018 and 2019, and has even slightly decreased for enterprises, with a 27% share of the total budget in 2018 to 26% in 2019.

This could be explained by large investments made in previous years. Several big data breaches – such as the Capital One credit card database breach, which revealed 106 million customer details, or the Facebook incident seeing hundreds of millions of user records exposed on an Amazon cloud server - the rollout of GDPR and all-around digital transformations catalyzed big investments in business cybersecurity over the past few years. Now it appears companies have reached a relatively stable threshold of around 25% and could be starting to re-evaluate the profit of these previous investments before they further improve their cybersecurity.

Where SMBs and enterprise businesses are investing their IT budget

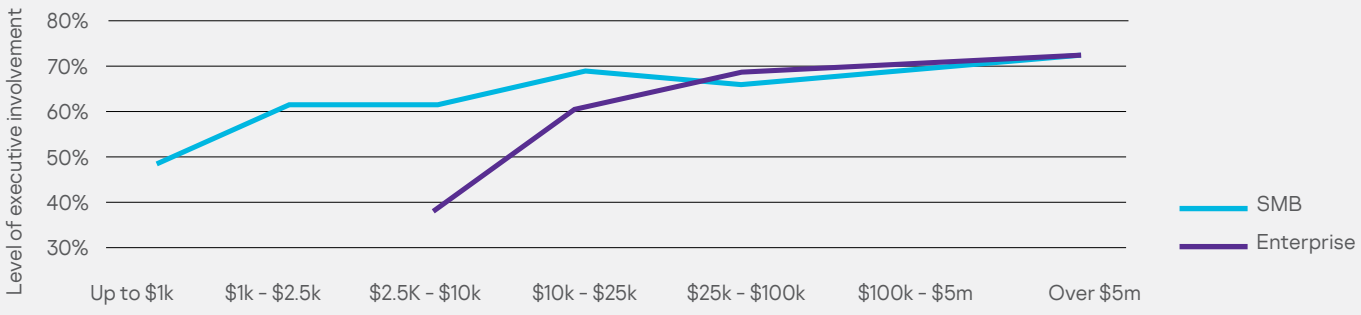


When it comes to investing for the future, companies are mainly using their IT budget to increase their investments in cybersecurity software staff training and education. As the chart above shows, 33% of enterprises and 27% of SMBs have seen a significant increase in security software spending. Both enterprises and SMBs have also seen significant investment in big data programs (26% enterprise, 21% SMB) and staff training and education (25% enterprise, 22% SMB).

Buy-in from C-level executives leads to an increase in cybersecurity budgets

In companies where C-level executives are strongly involved in the IT decision making process, the average IT security budget reaches more than $5 million for both enterprises and SMBs. This is in comparison to an average budget of $10k - $12k in companies where executive management is only partially involved.

IT security spending and C-level involvement



Conclusion

It's vital that businesses keep investing and rethinking their IT security processes in order to stay one step ahead of the growing rates of cyberattacks, and to limit any financial losses incurred.

Our report highlights that when a business invests in its people, resources and processes, they are better able to cope with the outcomes and financial losses of cybersecurity incidents.

Businesses who have installed an expert DPO, built an internal SOC or introduced regulation for third parties who have access to company data, all see a decrease in financial losses, or the ability to recoup some costs, following a data breach.

Increasingly, business leaders are also getting involved in the IT security decision-making process. This is resulting in higher IT security budgets and greater preparation for incident management. Therefore, for both SMBs and enterprises looking to get greater investment in their cybersecurity activities, it's key to get the executive level interested.

However, not all businesses are as prepared as they could be for the threat of attack. Overall, the general perception among businesses is that the number of threats to their networks are decreasing, despite incidents of all types continuing to rise in 2019. Given that only one-in-ten (12%) enterprises are concerned about malware infection, despite it being their costliest security incident, it's clear that businesses need to increase their awareness of how much these attacks are costing their company, regardless of frequency.

Similarly, the percentage of budget dedicated to IT security has stayed static compared to last year, possibly showing that investment in IT security has started to stall while businesses consider their next approach. Giving the continued risk of attack, instead of waiting, enterprises and SMBs should continue to invest in their future now so they are ready for the next generation of security incidents. It's vital that businesses keep investing and rethinking their IT security processes in order to stay one step ahead of the growing rates of cyberattacks, and to limit any financial losses incurred.

Clearly, for many businesses when it comes to protecting themselves from cybersecurity threats, there are challenges in sourcing the right expertise. That's why, either internally or externally through a vendor, prioritizing and investing in cybersecurity knowledge is essential to staying secure.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

kaspersky BRING ON THE FUTURE

www.kaspersky.com

2019 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.