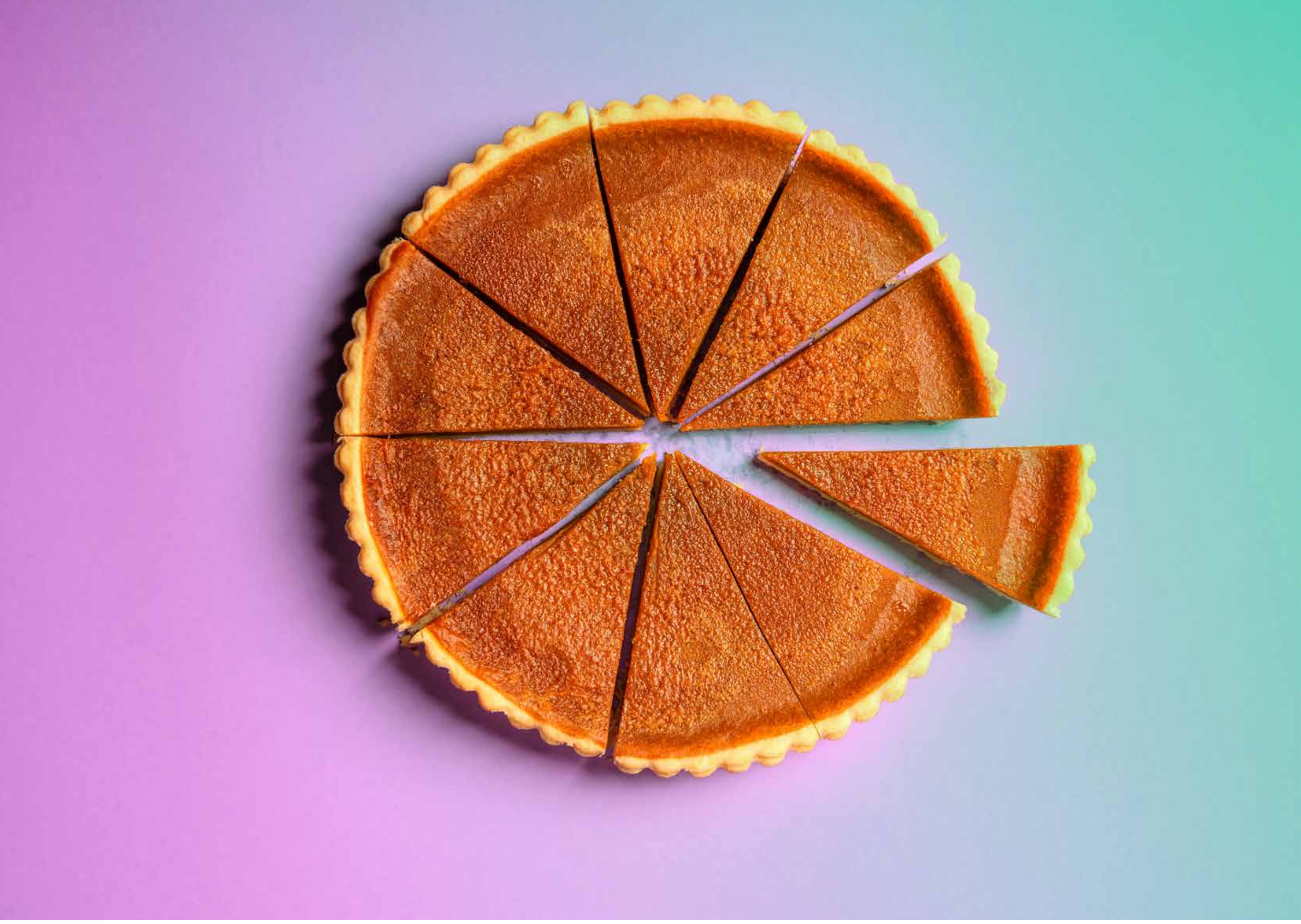


Investment adjustment: aligning IT budgets with changing security priorities

IT security economics 2020: executive summary

kaspersky BRING ON THE FUTURE

Learn more at kaspersky.com

Contents

Introduction 2

The changing cost of data breaches 4

Cementing top cybersecurity challenges 8

Realigning IT security budgets 9

Conclusion 11

Introduction

Risk versus reward is a fine line for every business to tread. No more so when it comes to the security of its people and the valuable data it holds.

With 2020 being a year of immense change and uncertainty for all organizations – large and small – it has never been more important for business leaders to review IT security priorities and ensure procedures and budgets are aligned, to yield future prosperity and growth. **Recent research from Gartner** supports this trend, predicting that 75% of CEOs will be personally liable for cyber-physical security incidents by 2024.

Over the past decade, through Kaspersky's ongoing research into the economy of IT security, we have seen great change in priorities when it comes to protecting businesses, along with huge strides in cybersecurity solutions, intelligence and education. But what impact has an increased reliance on technology and online collaboration over the past year alone had on today's security spend and outlook?

This first report in a series of several looks at the economics of IT security, delving into the headline findings of this year's research, and setting the scene for the costs, challenges and changes affecting IT security decision-makers today. Interestingly, the size of IT security budgets remains fairly flat compared to the 2019 data, but its share within overall IT spend is growing. This suggests an elevated position for cybersecurity measures around the decision-making table, when it comes to keeping mission critical systems online, and people and data protected.

Methodology

The Kaspersky Global Corporate IT Security Risks Survey (ITSRS) is now in its 10th year

A total of 5,266 IT business decision-makers were interviewed across 31 countries in June 2020. 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.

Throughout the report, businesses are referred to as either SMBs (small and 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.

Please note that while every effort has been made to make the results comparable year-on-year, the research has undergone some revisions in 2020 meaning that not all results are directly comparable. The target audience has remained the same, but screening questions have been revised to more reliably identify people with the most relevant experience and insights. This has significantly increased the proportion of respondents in IT and IT security specialist roles from 33% in 2019 to 62% in 2020.

In addition, while the scope of the study has remained global, fewer countries were included in 2019 (most notably China was absent). The 2020 research features a broader country base (as per 2018 and 2017), and also adds Poland and Kazakhstan to the list.

Key findings

Cost of data breaches

$101k
for SMBs

$1.09m
for enterprises

IT security budget

$275k
for SMBs

$14m
for enterprises

- Average cost of data breaches decreased to $101k for SMBs and $1.09m for enterprises in 2020, compared to $108k and $1.41m respectively in 2019
- Share of IT security in overall IT budgets has grown from 23% in 2019 to 26% in 2020 within SMBs, and from 26% in 2019 to 29% in 2020 for enterprises
- This is despite decreased spend by $4.9m for enterprises (from $18.9m in 2019 to $14m in 2020) and a slight rise in SMB spend by $8k (from $267k in 2019 to $275k in 2020)
- Three years ago, a third of decision-makers (33% of SMBs and 35% of enterprises) admitted that it took several months to detect a data breach. In 2020, that reduced drastically to only 13% of businesses
- The main challenges worrying IT security teams this year are very specific: phishing attacks on customers (50% of SMBs and 48% of enterprises) and attacks on branch offices (44% of SMBs and 42% of enterprises)
- Top drivers to reduce spend on IT security include a third (32%) of senior management within enterprises seeing no reason to invest so much in the future, and 29% of SMBs cutting overall company expenses and optimizing budgets

The changing cost of data breaches

One of the key drivers and motivators for spending on IT security is ultimately the cost to the business if you don't, and a data breach happens. There is no shortage of examples of companies putting customers and their own reputation at risk by suffering a data breach.

The **hack in May 2020 which targeted Blackbaud** – one of the world's largest providers of education administration, fundraising, and financial management software – affected over 10 universities in the UK, US and Canada who had student and alumni data stolen after hackers attacked a cloud computing provider. The hotel chain **Marriot was again subject to a security breach in March 2020**, which saw the data of more than 5.2 million hotel guests obtained by hackers over the period of a month before the breach was discovered.

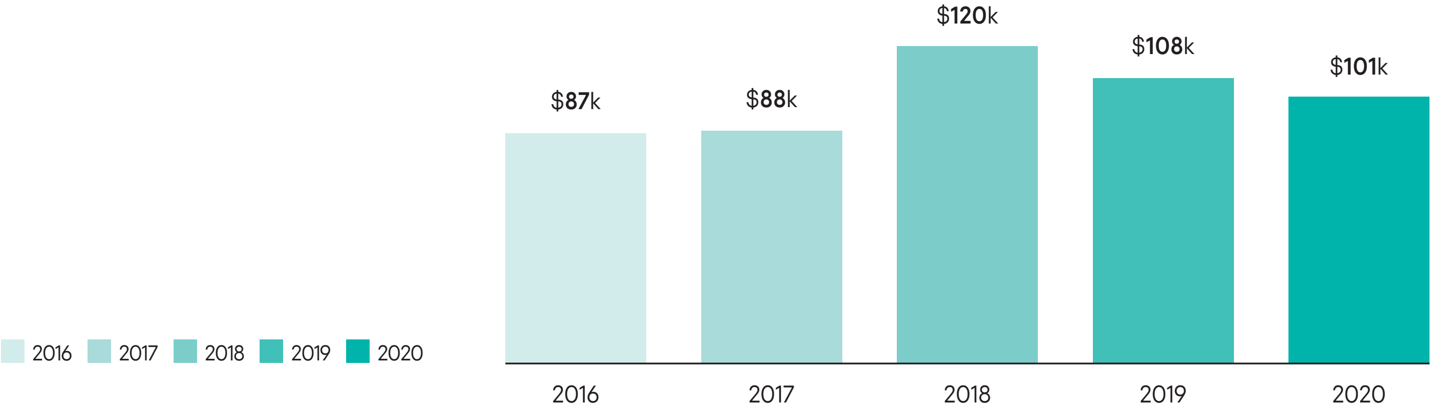
In addition to having a damaging effect on consumer confidence and tarnishing reputations, these companies and many others like them will have suffered huge financial costs and implications associated with a security breach, that can make it even harder to recover from – especially for a small business with smaller budgets and limited resources.

The good news is that our research found that the costs of a data breach are falling for both SMBs and enterprises, although the financial impact is still rising in the financial services industry, perhaps due to the highly regulated nature of the sector and more wide reaching consequences of non-compliance.

The average financial impact of a data breach for SMBs who have experienced at least one data breach stands at $101k (compared to $108k in 2019), and for enterprises it amounts to $1.09m (compared to $1.41m in 2019). The top three costs which make up this overall figure for all businesses are cited as additional internal staff wages, loss of business and the need to employ external professionals to sort out a data breach once it has happened.

Chart 1: Average total financial impact of a data breach for SMBs

Total financial impact



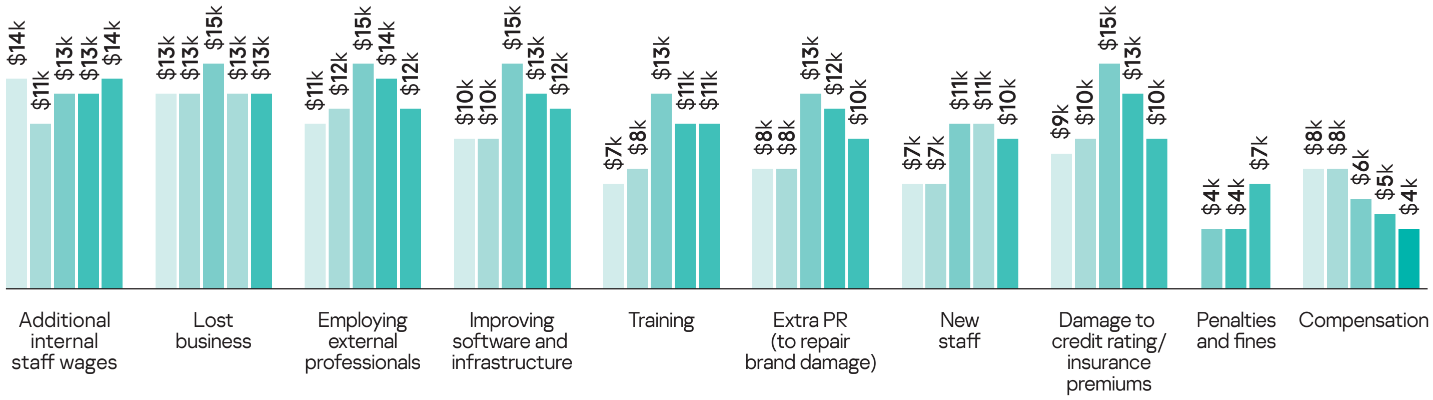
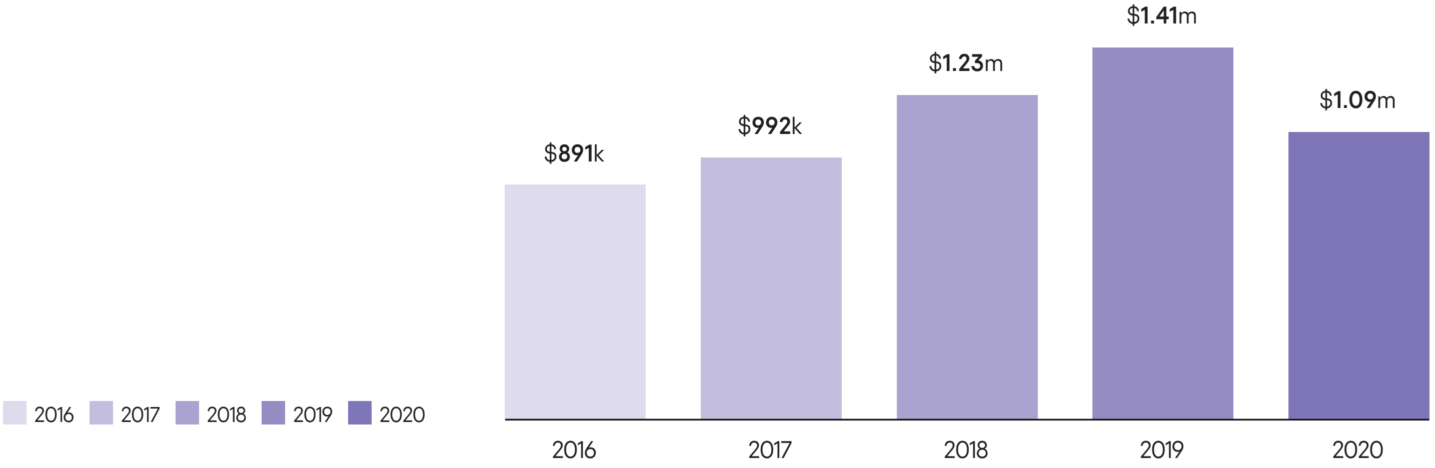
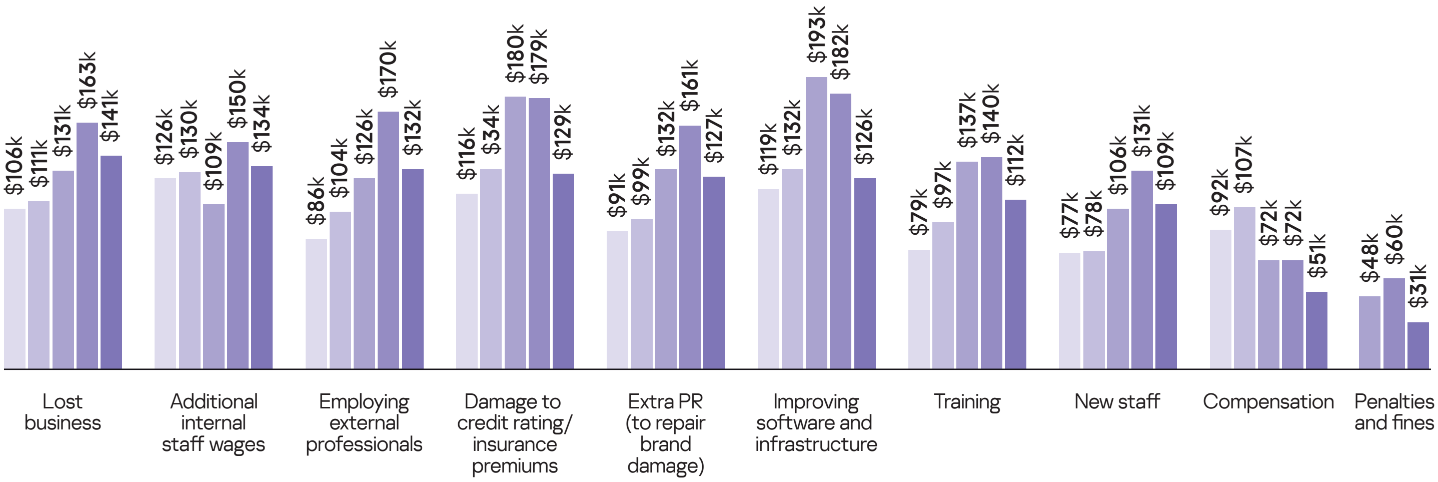


Chart 2: Average total financial impact of a data breach for enterprises

Total financial impact



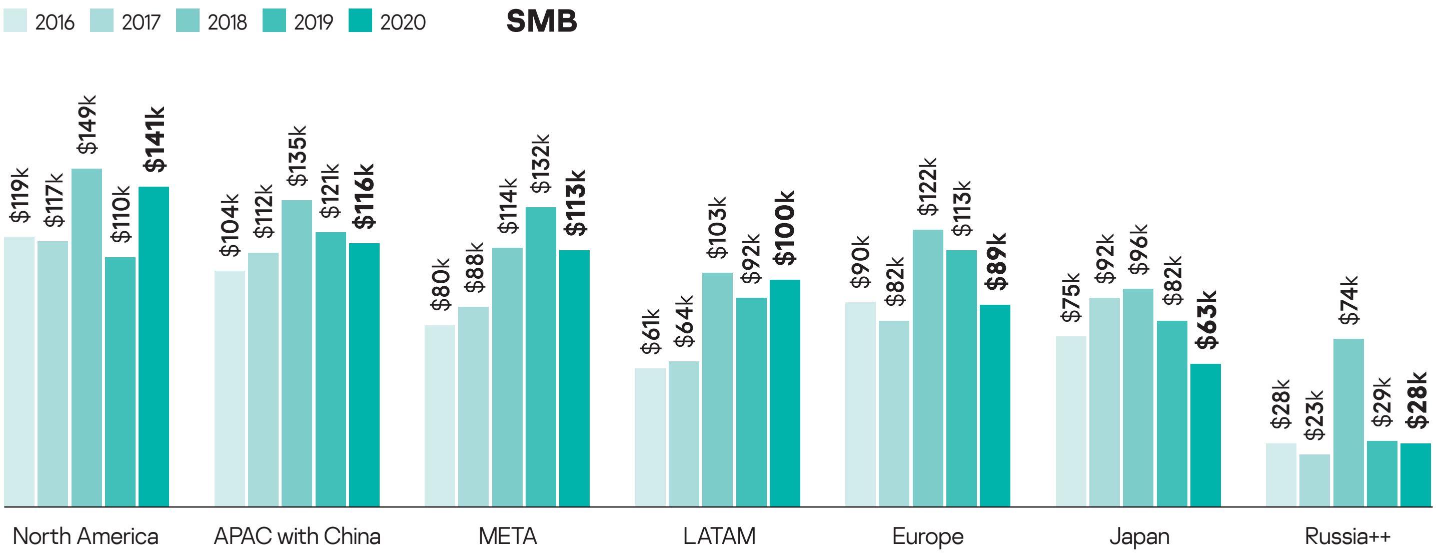


Regional variations

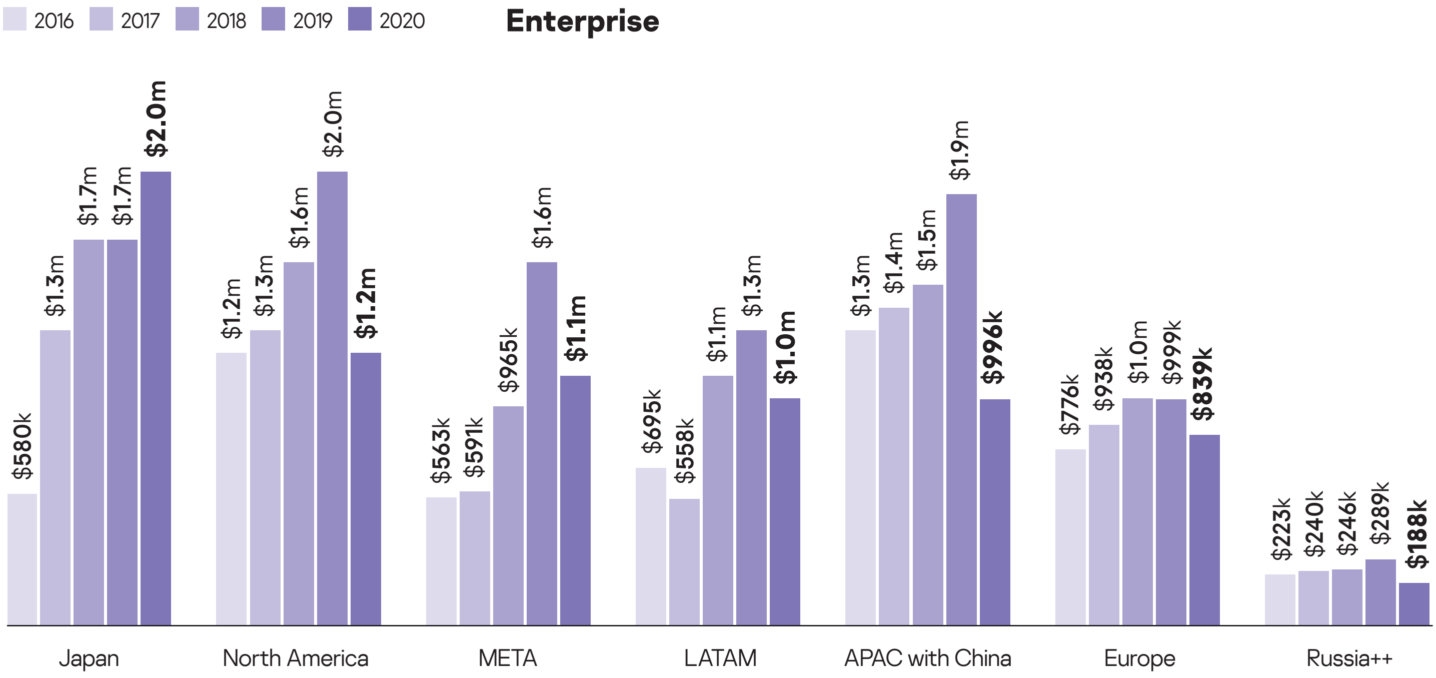
Most regions across the world follow a similar pattern when it comes to the declining costs associated with a data breach in 2020, with the exception of North America and LATAM, where costs among SMBs have risen, and in Japan, where the financial impact has increased for enterprises.

Chart 3: The average financial impact of a data breach across the regions

SMB

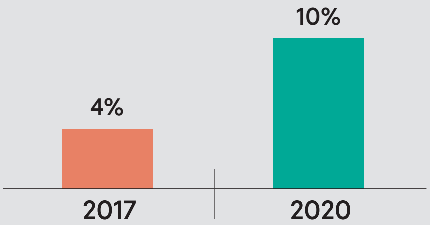


Enterprise



The value of quick reactions

Businesses that detect attacks almost instantly



One of the key reasons for this steady decline in costs across the globe could be due to improvements made in detecting attacks and therefore minimizing the impact upon businesses of a breach. Our research found that both the SMB and enterprise sectors have seen the amount of time taken to detect and respond to data breaches shorten significantly over the past few years.

In 2017, only 4% of businesses had a system in place – such as endpoint detection and response or network intrusion prevention – that could alert them to a breach almost instantly. Today that figure has risen to one in ten (10%). In 2017, a third of decision-makers (33% of SMBs and 35% of enterprises) admitted that it took several months to detect a breach. In 2020, that has reduced drastically to only 13% of businesses.

Over the past three years, businesses have changed the way they respond and react to data security and realized the value of investing budgets in solutions for detection and response, rather than reacting and paying a financial premium, once a breach has occurred.

Cementing top cybersecurity challenges

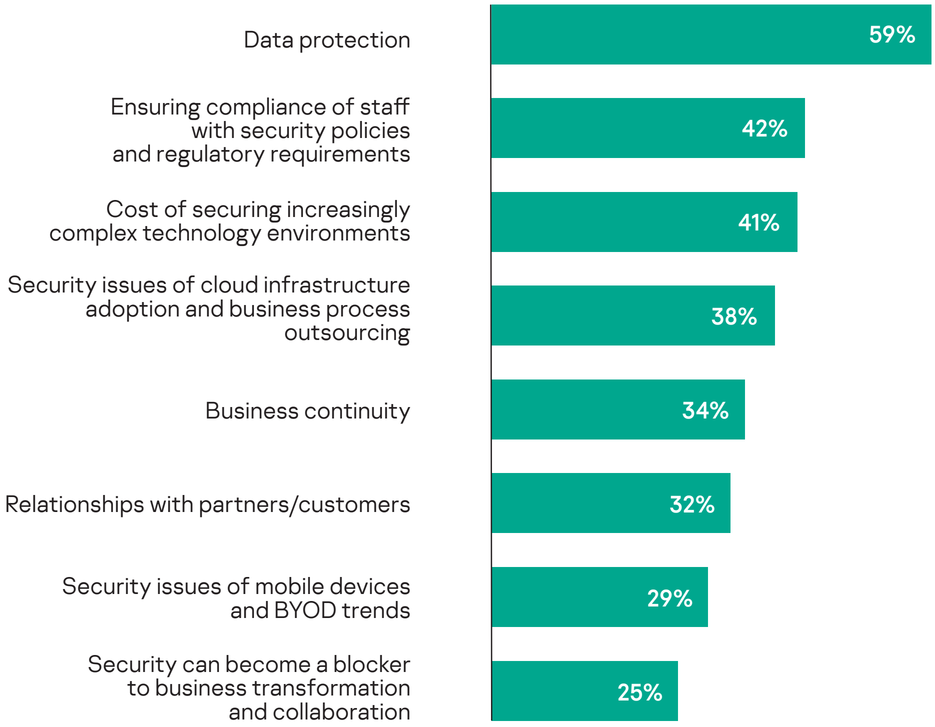
For all businesses, the top three most concerning IT security issues remain unchanged in the past 12 months. Data protection (59%), ensuring compliance with security policies and industry regulations (42%), and the cost of securing increasingly complex technology environments (41%) are the main worries for decision-makers.

In the current COVID-19 climate, it is no surprise to see these concerns continue to top the worry list. Businesses across the globe have shifted their operating models and moved entire workforces to homeworking, which has put an additional strain on businesses to ensure their systems are protected and compliant, and that their sprawling IT environments remain secure. With more people working remotely and outside the relative comfort and security of an office environment, this also puts the onus on individuals to continue to act responsibly when using work and personal devices.

When we drill down into specific cybersecurity concerns, we gain some very significant insights into how worries have changed. Phishing and social engineering attacks on customer accounts is the top challenge cited by half of SMBs (50%) and enterprises (48%). This is closely followed by concerns around attacks on branch offices (44% for SMBs and 42% for enterprises).

The pandemic has undoubtedly had a role to play in elevating and indeed substantiating these fears, with our own experts finding that phishing attacks have become more targeted and diverse in their approach over the period of the pandemic.

Chart 4: Top IT security concerns for all businesses



Rank of concern

2017	2018	2019	2020
1st	1st	1st	1st
5th	3rd	2nd	2nd
4th	6th	3rd	3rd
2nd	2nd	5th	4th
3rd	5th	4th	5th
6th	4th	6th	6th
7th	7th	7th	7th
N/A	N/A	8th	8th

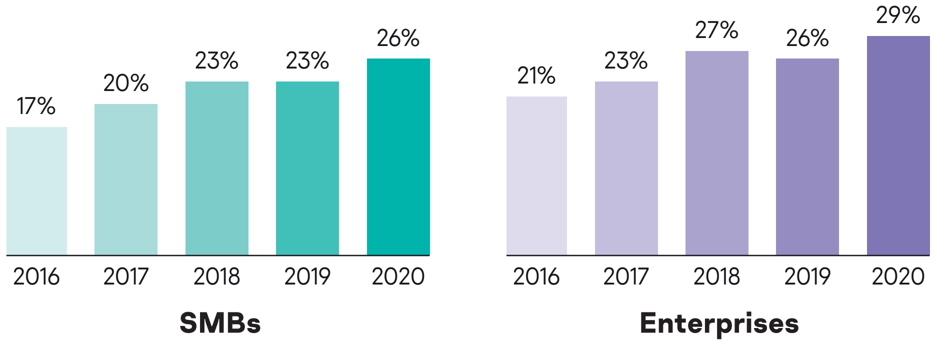
Realigning IT security budgets

Planning a budget can be a pain point for many businesses, with changing priorities and parameters all having a part to play. When it comes to allocating IT spend, business leaders already indicated digital and technology disruption as their top priorities for 2020 according to Gartner, even before the pandemic took hold and technology became the primary lynchpin for almost every business.

2020 has seen organizations make significant and fast-moving changes to day-to-day operations, to enable them to keep running and remain resilient in the face of evolving challenges. As such we have seen the goalposts for IT security spend shift over the past 12 months, as business priorities change and available budgets become even more squeezed and scrutinized.

Interestingly the 'value' of IT security budgets continues to grow – but not in monetary terms. As a share of overall IT spend, the proportion allocated to security is increasing in size. In 2019, 23% of IT budget within SMBs was allocated to security, compared to 26% in 2020. Within enterprises, the percentage rose from 26% to 29% over the past 12 months. When we look at the specific figures though, budgets remain largely static (within SMBs) or decrease (for enterprises). These findings are very much in line with recent figures from **Gartner** which suggest that global IT spending will decline by 8% in 2020 due to the impact of the COVID-19 pandemic.

Chart 5: IT security budget as a share of overall IT budget



	2018	2019	2020	2018	2019	2020
Average IT budget	$1.1m	$1.2m	$1.1m	$42.1m	$74.1m	$54.3m
Average IT security budget	$256k	$267k	$275k	$10.2m	$18.9m	$14.0m
Expected growth of IT security budget (over three years)	+14%	+11%	+12%	+15%	+11%	+11%

Investment priorities

More than two thirds (71%) of SMBs and enterprises plan to increase investment into IT security over the next three years while 17% plan to keep it unchanged. For those SMBs looking to increase their security spend, one of the top three drivers was cited as wanting to increase security spend in response to increased complexity of IT infrastructure (43% compared to 36% the previous year). In line with findings highlighted earlier in the report, this is followed by the need to improve internal specialist security expertise (39%) and for a third (34%) of SMBs, senior level management wants to increase budgets to improve company defenses.

Enterprises' desire to increase security budgets shows a similar trend. 43% state key reasons being increased IT infrastructure complexity, the improvement of internal expertise (41%), and top management wanting more robust defenses (34%).

For those investing in technology in response to a data breach, network (46% of enterprises and SMBs) and endpoint (45% of enterprises and 41% of SMBs) detection technologies are closely followed by threat intelligence for both enterprise and SMB organizations – 41% and 39% respectively. This suggests that businesses understand the value in not only being able to respond quickly, but having the necessary insights and information to react to ever-changing threats, as the cyber-landscape continues to evolve.

In contrast to those looking to put more investment into IT security, 9% of SMBs and 11% of enterprises indicated they plan to decrease their budgets in this area in the next three years. The overriding reason for this, especially visible across enterprises, is the feeling that enough investment has been made to secure an organization and that current levels of investment do not need to be maintained.

For example, a third (32%) of enterprises' senior level management sees no reason to invest so much in IT security – the top reason given for reducing budgets. For SMBs, a quarter (25%) believe that they are secure enough and do not need to spend further money in this area, but the top reason for reducing investment is due to overall cuts to company expenses and general budget optimization (29%).

Chart 6: Top reasons to decrease investments in IT security

Reasons given for expecting to reduce IT security spending over the next three years	SMB		Enterprise	
	%	Rank	%	Rank
Overall cuts to company expenses/general budget optimization	29%	1	26%	5
Large investments in past years solved key problems – now only maintenance is needed	25%	3	30%	2
Top management sees no reason to invest so much in IT security	23%	5	32%	1
We are secure enough and there is no need to invest more in IT security	25%	2	22%	7
Outsourcing some IT security functions allows us to cut costs	22%	7	26%	4
IT budget re-allocated to other needs in the company	19%	8	27%	3
Due to a decrease in business	23%	4	20%	10
There were no security incidents experienced in the last 12 months	22%	6	21%	8
Switched to a cheaper endpoint protection solution/vendor	19%	8	23%	6
Demand from our shareholders and investors	15%	10	21%	9

Conclusion

Despite the unique events of 2020, our research has identified a number of recurring trends and suggests a positive outlook for IT security prioritization and increased spend in this area within both the SMB and enterprise communities.

The falling financial impact on companies of a data breach is undoubtedly good news, suggesting that mitigating measures are working for the most part and budgets are being spent in the right places.

The figures should not however signal complacency but instead act as the proof point that strong and robust IT security measures work and are crucial to potentially save costs in the long-term. The growing share of IT security within overall IT spend points to the value placed on cybersecurity measures and is certainly an area that businesses should continue to build on, to maintain the highest levels of security and protection in the midst of an ever-changing threat landscape.

It is clear that senior management buy-in and understanding are key to securing and indeed increasing investment, particularly within enterprise companies. Even where respondents alluded to reduced budgets in the years to come, the development of cybersecurity infrastructures and spend, up to this point, have been largely positive. The acknowledgement, intelligence and ultimate reaction to threats have evolved, in tandem with the desire to upskill and bolster internal security teams.

As a form of proactive vigilance, there should be heightened awareness around how remote working and more dispersed teams increase levels of vulnerability among businesses. We only need to look at the fast-moving evolution of social engineering tactics including phishing, to see how cybercriminals are continuing to enhance their attack arsenal and keep IT teams on their toes.

To help businesses address these ongoing challenges and ensure budgets and measures are aligned with current priorities and evolving threats, Kaspersky suggests the following measures:

- Use a risk-based approach when planning your cybersecurity budget. Look at the threats most relevant to your industry and company size, then consider the cost to the company and the probability of risk occurrence when prioritizing what to address first
- Outsourcing can be a good option for organizations that don't have the necessary internal expertise or risk assessment processes. Agreeing a guaranteed service level agreement (SLA) with any third-party and moving expenses from CapEx to OpEx is a way to keep security spending under control
- Provide all your staff with **basic cybersecurity hygiene training**. Always improve the skills of your IT security workers so they can defend against even sophisticated attacks. For example, Kaspersky provides **online training on threat hunting with YARA rules**
- Despite the cost of data breaches falling year-on-year, businesses need to stay vigilant and always use a dedicated cybersecurity solution that combines endpoint protection with detection capabilities. Kaspersky's **Integrated Endpoint Security** solution provides instant visibility and insight on incidents, along with immediate investigation and automated response options
- Security solutions that can be managed from the cloud should simplify protection of remote offices and branches which was another key concern for cybersecurity specialists this year
- Ensure protection from spam and phishing so that malicious actors cannot profit from the credulity of employees – whether linked to COVID-19 or any other event or trend. This is also relevant for SaaS mail services such as **Microsoft Office 365**
- To protect customers from phishing, educate them on possible tricks malefactors may use. Regularly send them information on how to identify fraud and what actions to take in this situation. In the case of a customer account being taken over, an **anti-fraud solution** that can detect anomalies and suspicious user behavior will be of huge value

For further insight into the changing costs associated with IT security and how to keep your business protected from evolving threats and data breaches, follow **#securityeconomics** for our series of reports on the topic.

Cyberthreat news: securelist.com
IT security news: business.kaspersky.com

kaspersky.com

kaspersky