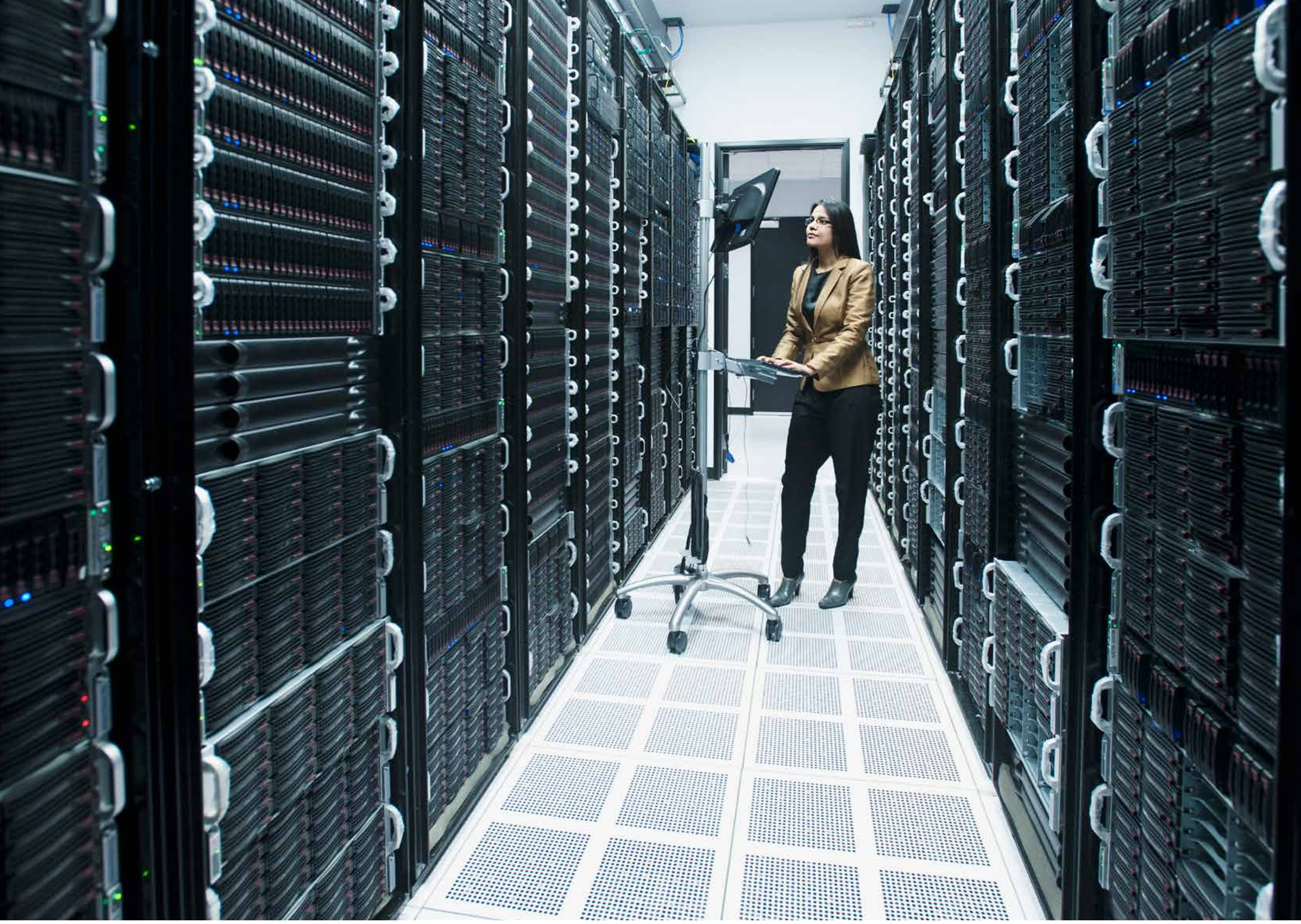


Managing the trend of growing IT complexity

IT security economics 2021: executive summary

kaspersky BRING ON THE FUTURE

Learn more at kaspersky.com

Contents

Introduction

In last year's IT Security Economics report , we described 2020 as a year of great change. That change has continued, or perhaps even increased this year, with working patterns and the way businesses operate shifting forever.

In 2021, businesses have embraced the hybrid working model, with staff sometimes in the office, or sometimes at home. That has required companies to secure networks across new staff laptops or tablets, set up Virtual Private Networks (VPNs), transition to cloud servers and quickly approve new collaboration software.

That rapid, widespread adoption of working-from-home tools has put considerable strain on security teams, who must safeguard business networks without making it harder for employees to work.

Our research highlights a growing cybersecurity trend for 2021: IT teams, in businesses both large and small, are facing increasingly complex IT infrastructure and operating environments. Today they are required to not only protect their organizations from cyberthreats, as they have always done, but do it across a more remote, hybrid and challenging IT infrastructure.

In the current crisis management-led environment, IT security specialists are also focused on optimizing security budgets. This year, effective use of resources became one of the most important topics on their agenda for a long time.

Despite these challenges, our data reveals that businesses have actually coped well throughout the last year and are improving their data breach resilience. In fact, small and medium-sized businesses (SMBs) report only a slight increase in the cost of data attacks, while the costs for enterprises is decreasing.

This report highlights the economics of IT security, laying out the key findings of this year's research and unpicking the changes in the budgets, breaches and business challenges affecting IT security decision makers in 2021.

Methodology

The Kaspersky Corporate IT Security Risks Survey (ITSRS) is a global survey of IT business decision makers

A total of 4,303 interviews from businesses with more than 50 employees were conducted across 31 countries in May-June 2021. 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.

Key findings

Cost of data breaches

$105k
for SMBs

$101k	▲	$105k
2020		2021

$927k
for enterprises

$1.09m	▼	$927k
2020		2021

IT security budget

$267k
for SMBs

$275k	▼	$267k
2020		2021

$11.4m
for enterprises

$14m	▼	$11.4m
2020		2021

- The cost of data breaches for SMBs increased slightly ($105k in 2021, compared to $101k in 2020, but still does not achieve the 2018 high point ($120k). The cost of a data breach for enterprises fell to $927k, below the previous low of $992k in 2017.
- Incidents involving shared data with suppliers was the costliest breach for enterprises, with a total impact of $1.4m in 2021.
- Enterprises were less likely to report data breaches this year, with 34% avoiding doing so, compared to 28% in 2020.
- Cybersecurity budgets, planned in the midst of the pandemic at the end of 2020, decreased dramatically for enterprises, falling by 19% to $11.4m. That's compared to $14m in 2020. Meanwhile, SMB security budgets only decreased slightly, down to $267k in 2021, compared to $275k last year (a 3% decrease).
- The number one cybersecurity concern for businesses in 2021 is the need for bigger budgets to secure increasingly complex environments (44%), that's up from third place last year (41%) and sixth place in 2018.

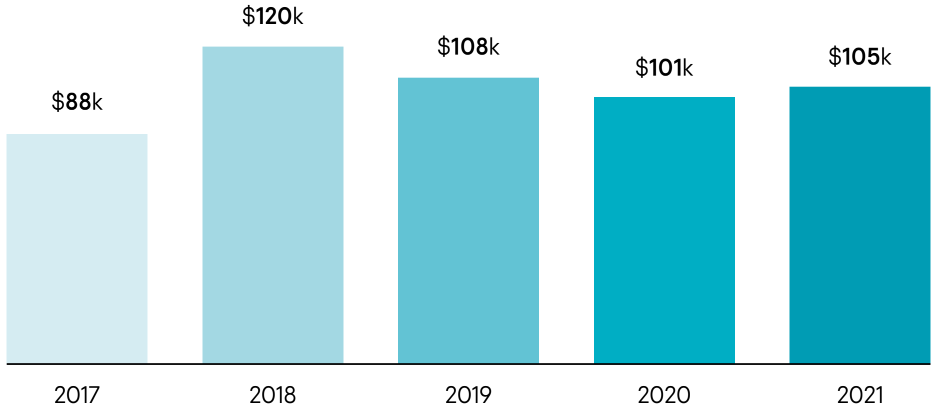
Old threats, same costs, new challenges

This year, cybersecurity risks continued to be a big concern for enterprises and small businesses, with new threats emerging during the pandemic and the extended period of remote work it introduced.

However, our research shows that, despite those new threats, the costs of data breaches didn't grow excessively in 2021.

In fact, there was only a small 4% increase in the financial impact of data breaches for SMBs ($105k in 2021, compared to $101k in 2020), and a notable 15% decrease for enterprises. That impact for those larger organizations fell to $927k from $1.09 million in 2020, below the previous lowest figure from 2017 ($992k).

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



Total financial impact

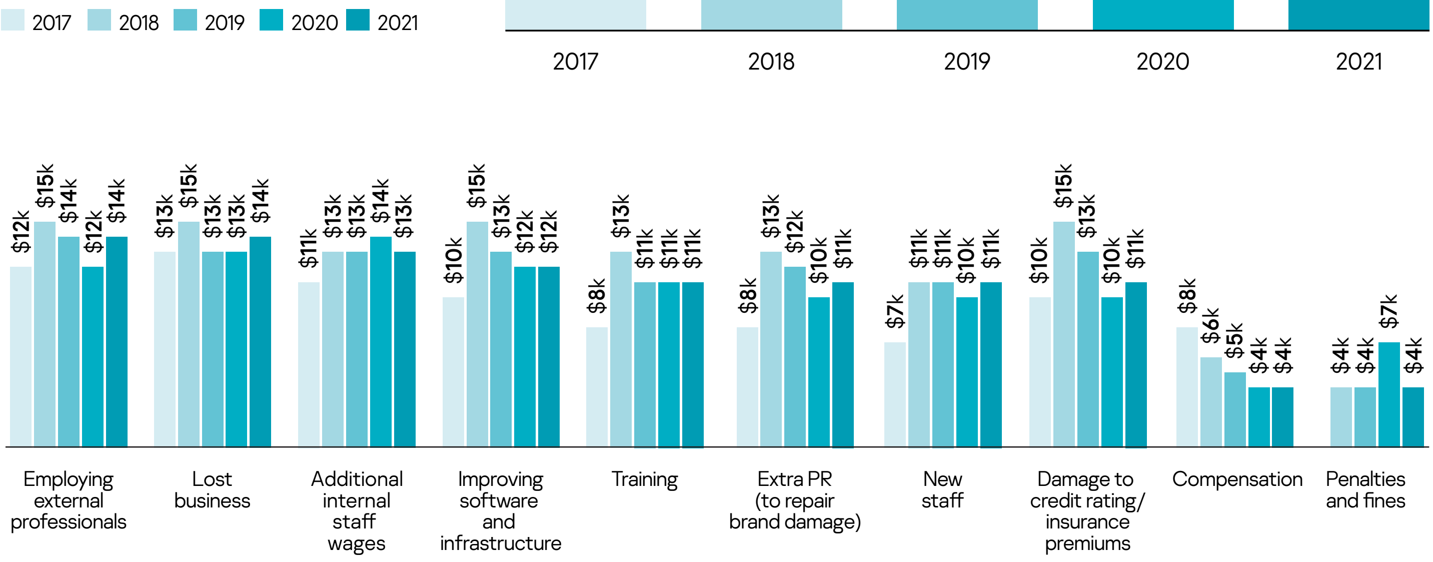
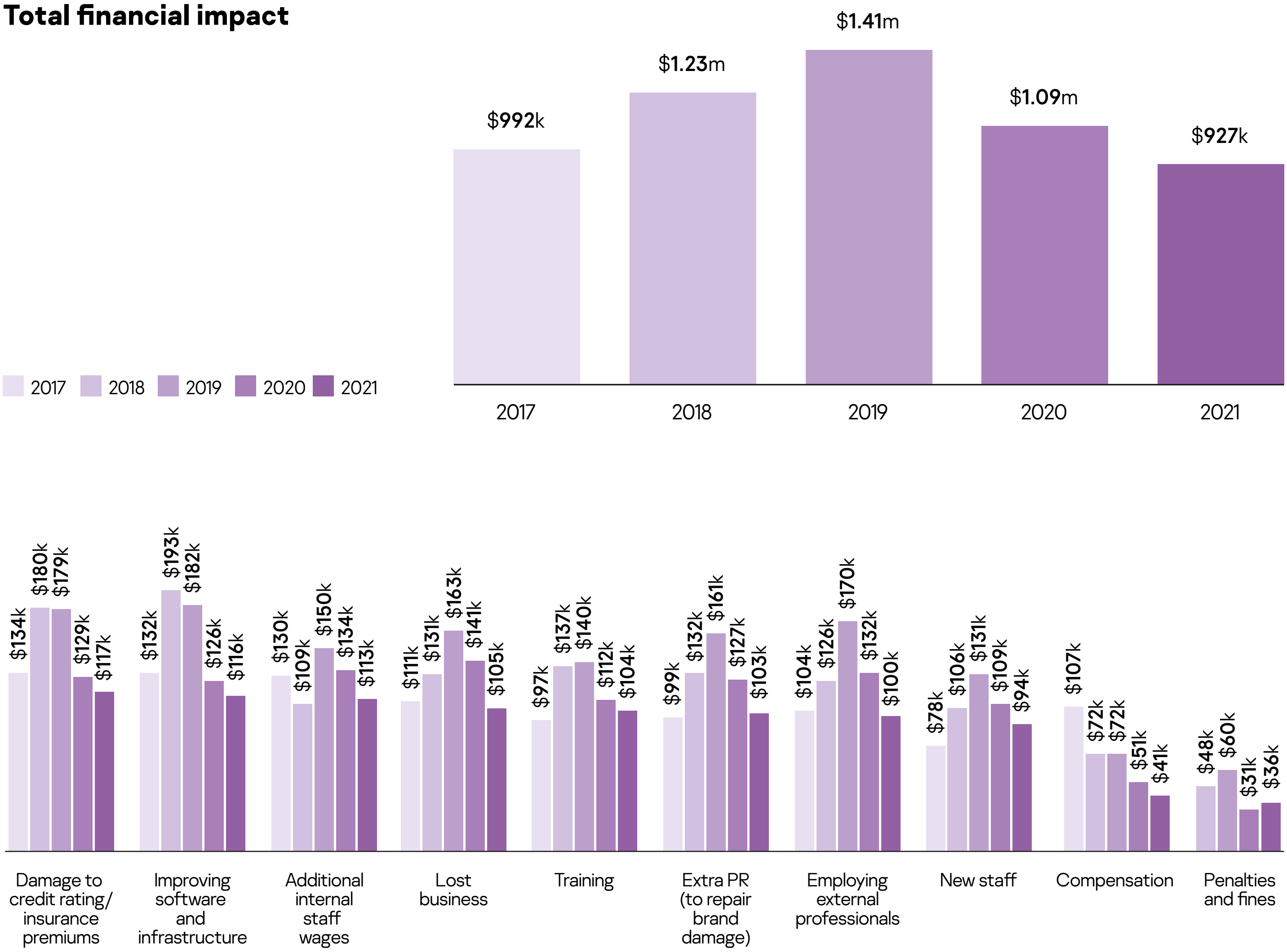


Chart 2: Average total financial impact of a data breach for enterprises

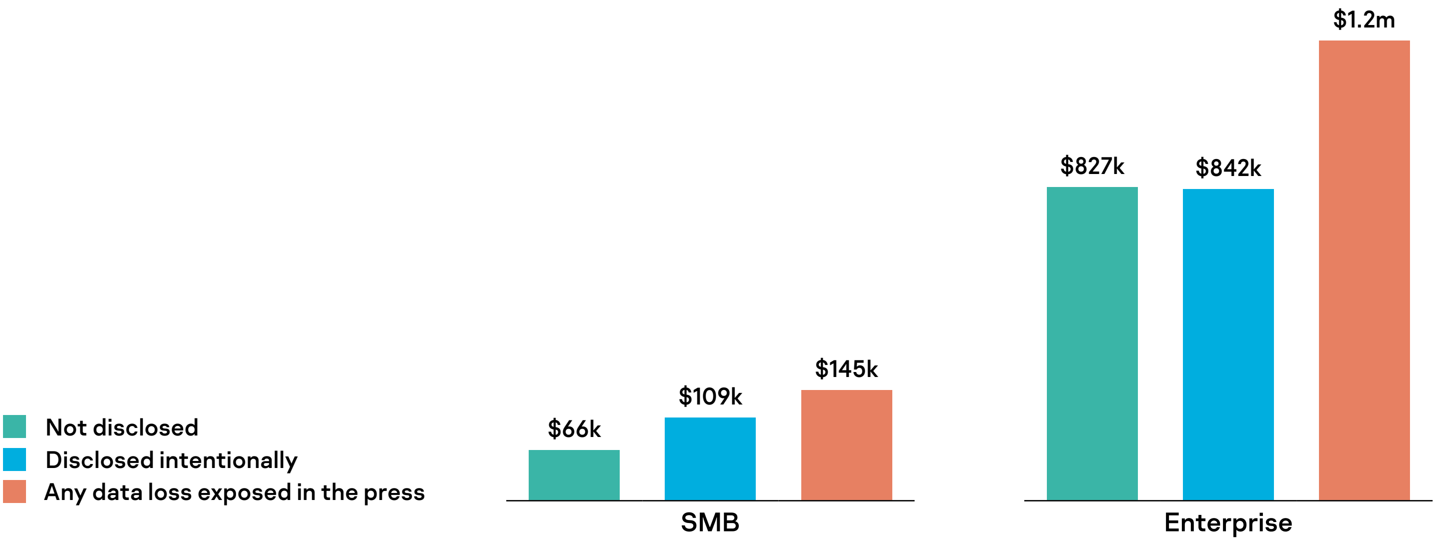


One of the key reasons we may be seeing this drop in the financial impact of a data breach in businesses could be due to improvements made in detecting attacks, therefore minimizing the impact of a breach. However, our research also found that enterprises were less likely to report data breaches this year, with 34% managing to avoid doing so, compared to just 28% in 2020.

One explanation for this reduction in reporting could be that businesses are becoming more proactive in eliminating the consequences of a data breach and avoided a lot of the impact from a leak, leading to less need to disclose it. Of course, sometimes the fact of an attack cannot be hidden, for example, if the victim is a public authority or organization providing state services, as it was with Italian COVID-19 vaccination booking system **attacked by ransomware in summer 2021**. In such cases, when the attack is exposed to the press, the financial impact rises significantly.

However, the higher number of companies avoiding disclosure of breaches could also reflect that some financially vulnerable companies are reluctant to commit time and expense to a criminal investigation or risk reputational damage if a breach becomes public knowledge.

Chart 3: Average cost of data breaches



Changing tactics in response to data breaches

A security breach became less likely to be a sackable offence in 2021, with just 21% of all enterprises firing employees as a result of one in 2021, compared to 24% in 2020.

Our research found senior security executives (in both IT and non-IT roles) were least likely to be fired. C-level executives are 4% likely to be let go, compared to 8% for those with a functional role in IT. Meanwhile, the number of senior IT security staff being laid off decreased by almost half from 14% in 2018 to 8% in 2021.

One possible reason for this change is that, amid a challenging cybersecurity environment, businesses have realized they need to keep their cybersecurity experts to boost skills and knowledge rather than swiftly letting them go following an incident.

"The transfer to remote work and processes has put increased pressure on the information security sector. With cybersecurity jobs in such high demand and skilled professionals in low supply, companies are realizing the value of senior security executives, and the need to plug the talent gap," comments Evgeniya Naumova, Executive VP, Corporate Business at Kaspersky.

This year, the research also found that companies were less likely to recruit more IT security analysts or specialists in response to incidents, with a decrease from 47% last year to 45% in 2021. There was also a notable decrease in the number of establishing new teams or departments dedicated to IT security, down from 42% in 2020 to 39% this year.

Instead, more than a third of organizations (36%) tend to hire non-IT security specialists with legal, compliance and risk management competencies who could help them address the consequences of a breach or prepare a crisis plan if another incident happens. This figure is supported by the Gartner 2020 Board of Directors Survey, which predicts that by 2025, 40% of boards of directors will have a dedicated cybersecurity committee overseen by a qualified board director.

Chart 4: Changes in response to data breaches in enterprises

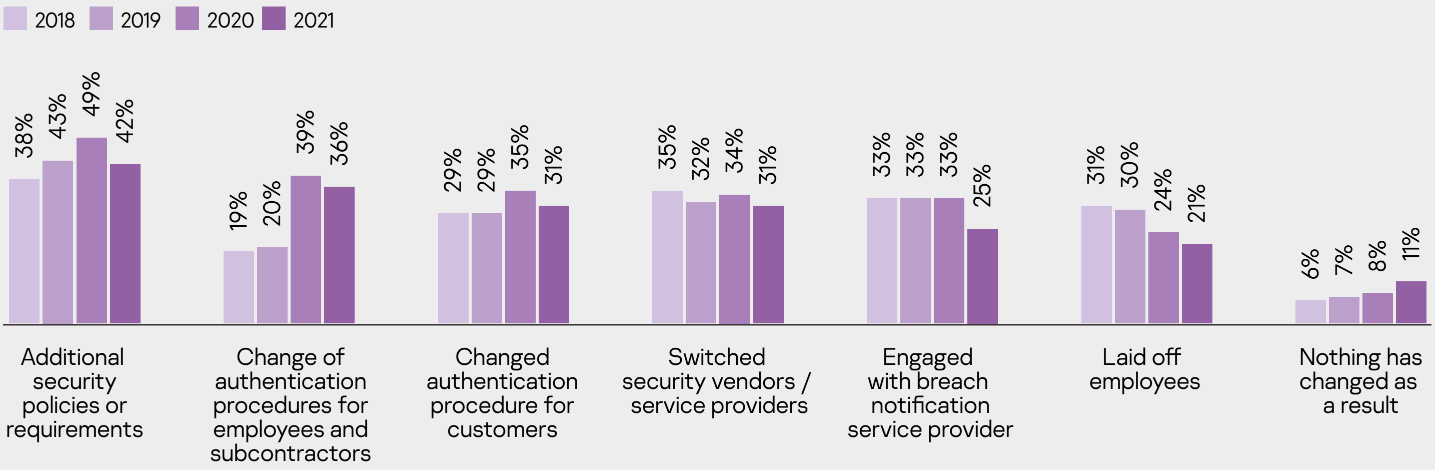


Chart 5: Enterprise employees laid off following a security breach

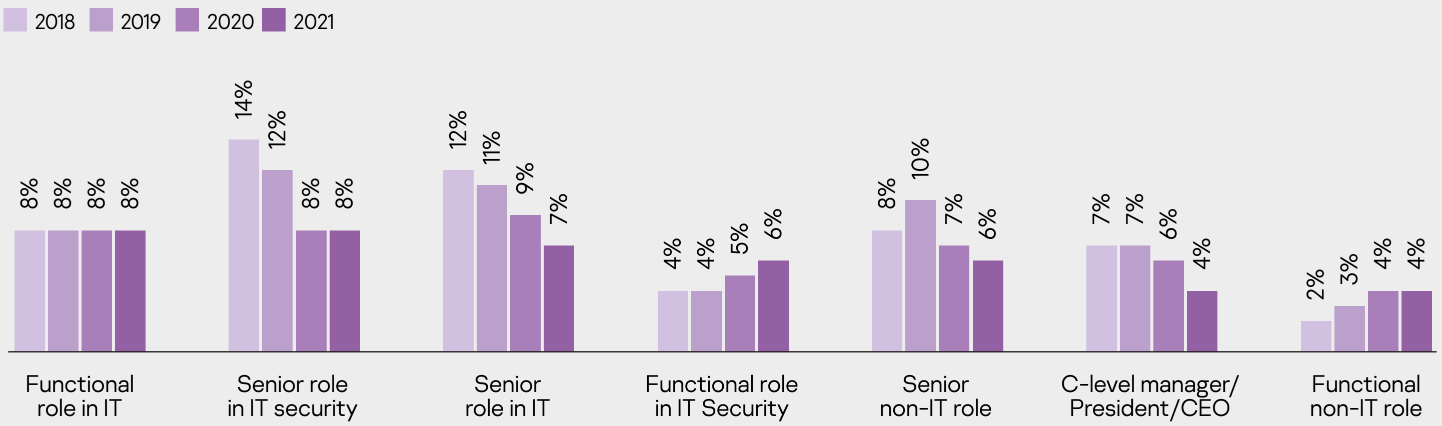


Chart 6: Changes in response to data breaches in SMBs

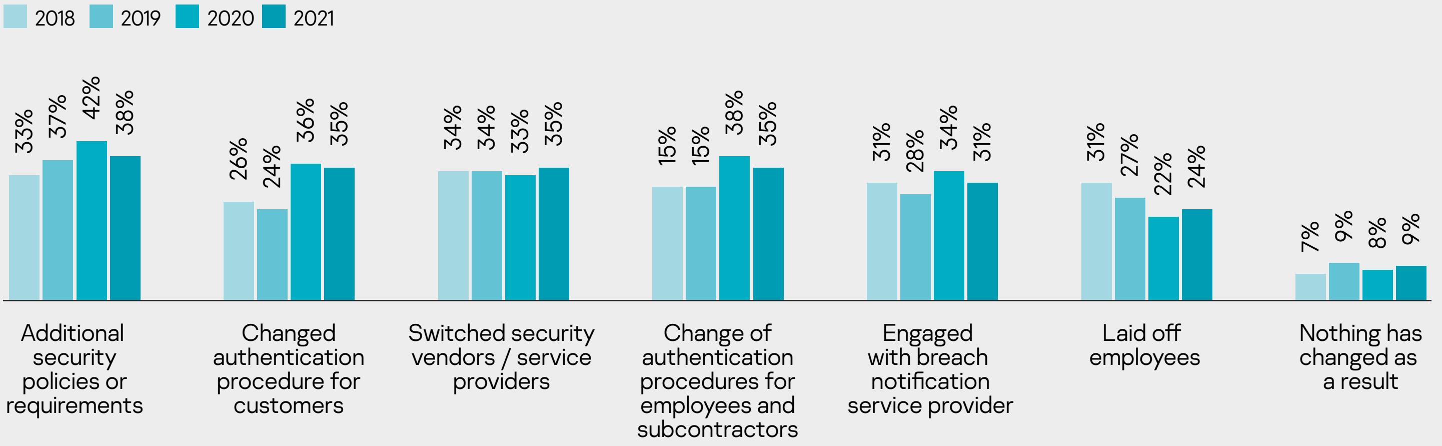
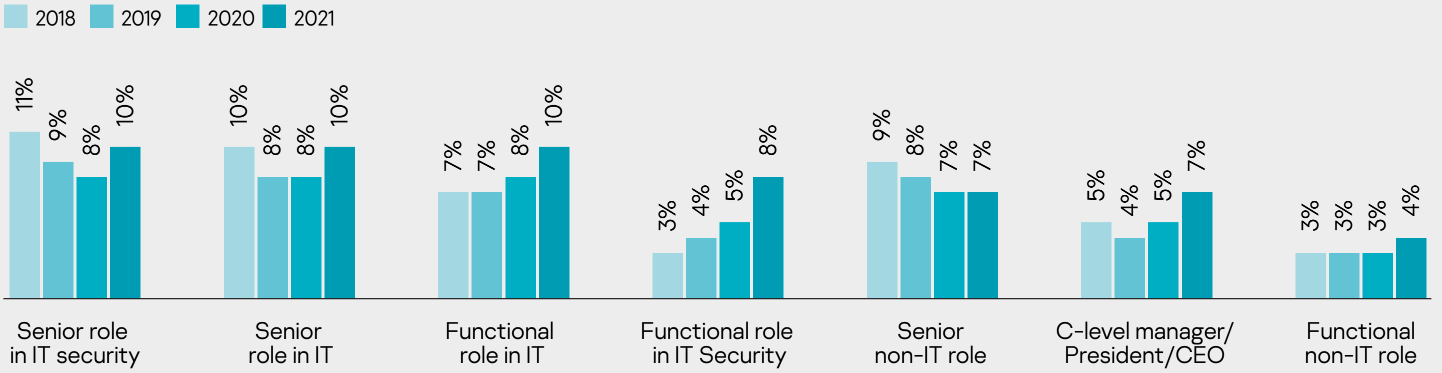


Chart 7: SMB employees laid off following a security breach



The costliest data breaches start with third parties

While companies focused on securing their increasingly complex networks this year, third-party software and data suppliers became a cybersecurity blind spot for many organizations. The research highlights a rise in data breaches when partners and third parties were involved – something which businesses are unable to directly control.

In 2021, incidents involving shared data with suppliers were the costliest data breach for enterprises ($1.4 million), an expense that did not even reach the top five last year, showing how quickly it has become a leading concern among the many other types of incidents.

For SMBs, incidents affecting suppliers' were the costliest form of all cybersecurity incidents (not just data breaches), costing SMBs $212,000 this year.

Chart 8: The average financial impact of a data breach

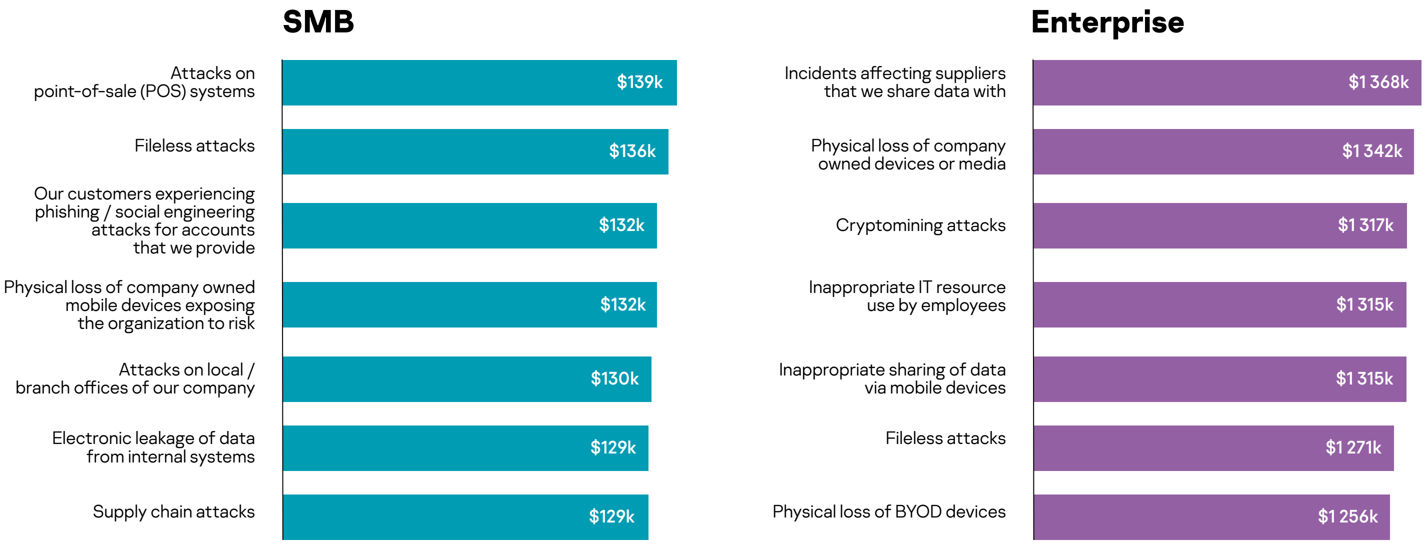
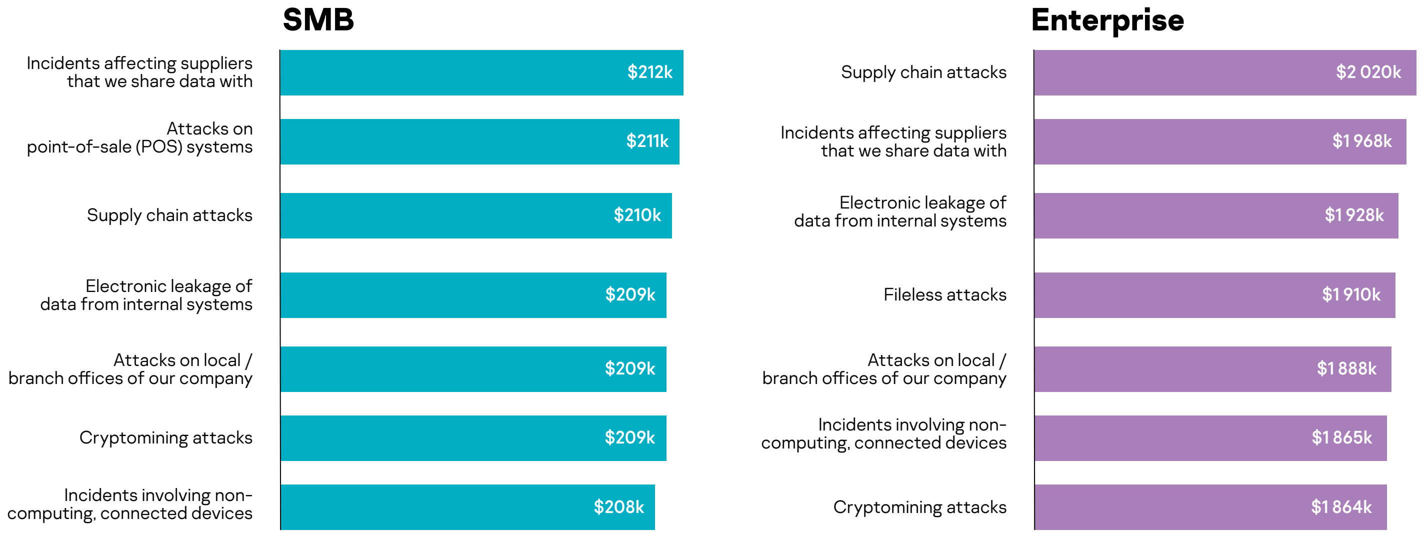


Chart 9: The average financial impact of any cybersecurity incident (not just data breaches)



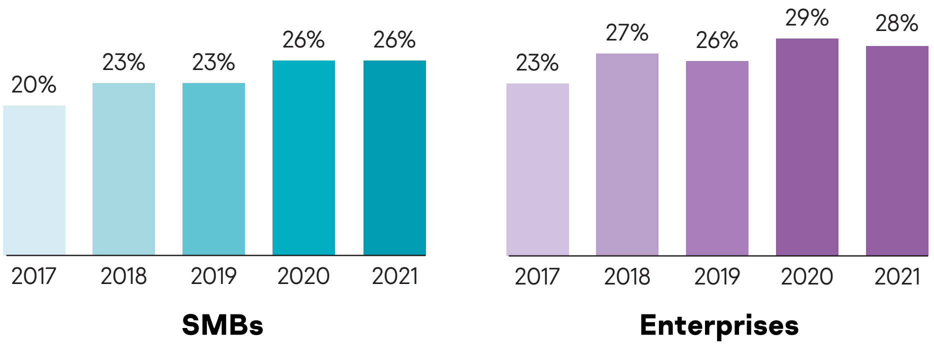
What is driving IT security investments?

External conditions and events can influence IT priorities for businesses. The pandemic and the world economic recession has proven that. As a result, during the new budget planning period at the end of 2020, organizations have had to adjust plans to meet changing business needs as the crisis continued. The survey revealed the impact this has had on IT security budgets.

According to estimations of organizations themselves, among SMBs, their average IT budget has fallen from $1.1m in 2020 to $1m in 2021. We also see a drop from $54.1m to $42.9m for enterprises.

When it comes to cybersecurity budgets, at enterprises, they decreased dramatically by 19%, to $11.4m in 2021, compared to $14m in 2020. SMB cybersecurity budgets remained at a similar level – $267k in 2021, compared to $275k last year[1].

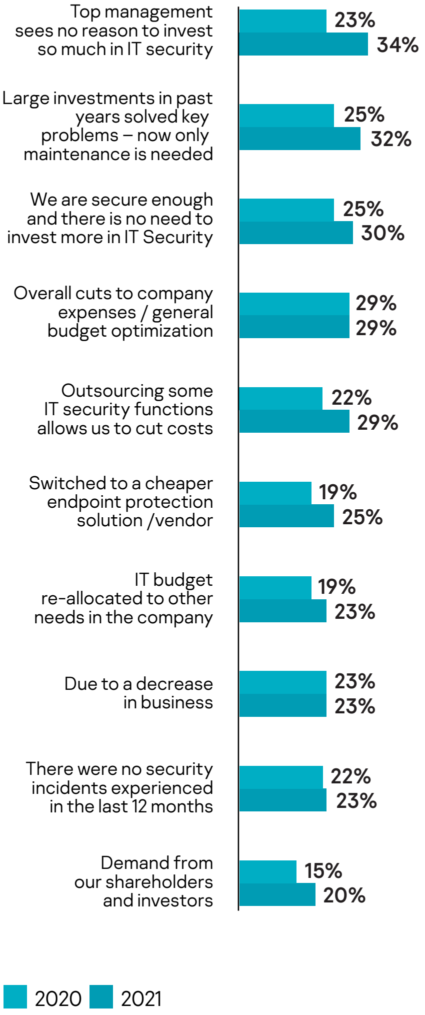
Chart 10: The percentage of IT budget spent on cybersecurity



	2018	2019	2020	2021	2018	2019	2020	2021
Average IT budget	$1.1m	$1.2m	$1.1m	$1.0m	$42.1m	$74.1m	$54.3m	$42.9m
Average IT security budget	$256k	$267k	$275k	$267k	$10.2m	$18.9m	$14.0m	$11.4m
Expected growth of IT security budget (over three years)	+14%	+11%	+12%	+12%	+15%	+11%	+11%	+12%

[1] The numbers for IT and IT security budgets provide the average budget based on answers from IT and IT security employees globally across companies of different sizes and industries.

Top reasons for reducing the IT security budget, SMB



Despite that, the importance of budget dedicated to cybersecurity continues to grow year-on-year. The estimation of its importance in the IT ecosystem has increased overall from 63% in 2020 to 65% in 2021. That's an increase from 61% to 63% for SMBs, and from 67% to 68% for Enterprises.

"**Overall, we expect that cybersecurity budgets should only increase, although there are some factors that impact this situation. Firstly, with everything being moved to the cloud, there is less need for infrastructure, leading to cuts in hardware capital budgets. Also, built-in security options that significantly influence the market. By getting built-in security options, businesses don't see the real price of cybersecurity. In addition, such options are multi-purpose and don't provide for all of the client's needs and nuances. In most cases such security options need additional layers adapted to the specifics of a client's business, such as leading threat intelligence. That would inevitably require additional investments into cybersecurity**," says Evgeniya Naumova.

When it comes to defining a budget for cybersecurity, Evgeniya also highlights the possible issue when cybersecurity is considered as part of the overall IT budget: "**Different organizations have different attitudes towards financial documentation and budget processes. However, it is not a matter of a line in an organization's budget, but acknowledging that cybersecurity is important and therefore requires dedicated resources and attention.**

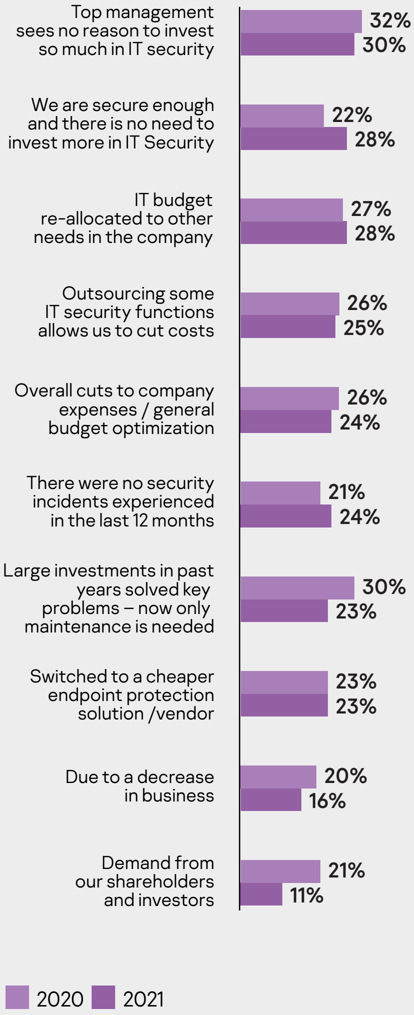
In general, for information security function to be successful, its projects and activities must be sponsored and supported at board level. Therefore, it is highly important that company boards are aware of the needs of a cybersecurity budget and take responsibility for supporting them.

If a board is not aware of an information security situation or doesn't pay enough attention to this area, it could become just another cost center. The inclusion of an information security budget into the general IT budget means an additional layer of approvals and quite often cybersecurity experts do not have an opportunity to defend their positions and projects in front of the board".

The companies surveyed this year also share positive hopes for the further growth of cybersecurity expenses, with 12% of both SMBs and enterprises expecting that to occur over the next few years. This positive forecast has also been highlighted by **Gartner**, which predicts an 8.4% growth of overall global IT spending in 2021.

Factors in budget decreases

Top reasons for reducing the IT security budget, enterprises



“Though this decrease in IT budgets is temporary, many companies switched to a tough cost-saving mode in 2021. We’ve seen a number of factors for this.

Organizations tend to utilize their IT and cybersecurity budgets as effectively as possible. This year, some companies may have bought a service before the pandemic, but in the process, realized that they needed another offering, so requests changed to match their current needs. Normally, companies would simply allocate additional budget in this case. Instead, they are trying to understand which services they have already paid for, but have not yet provided, which they can exit from in favour of a service that is more business critical.

In addition, the growth of information security budgets occurs, not because teams need support for existing systems but because they need to introduce new products. In the face of a pandemic and the transition to home offices, many companies have introduced a suspension on new IT projects. For example, if existing information security tools work effectively, they may decide it is better not to touch them, while major updates or new projects may be stopped or postponed. In my understanding, more than half of the budget decrease is because of this factor.

Another factor to consider is the increasing pace of cloud adoption. According to our observations, two years ago a large number of customers preferred on-premise solutions in private clouds. That involved the purchase of a large amount of hardware. Now, even very closed organizations tend to use public cloud.

This entailed a change in the need for information security systems. A number of projects that have been created over the years and were supposed to be used in on-premises infrastructure may have now lost their relevance.

It will take some time for customers to mature a set of requirements for the cloud and for vendors to form a package of solutions. But the request is here, and the new package of cybersecurity solutions for implementation will be formed.

Moving from CapEx to OpEx models also impacts the budgeting process. As the intensity of attacks and new samples has grown, IT services have had to focus on surviving in extreme conditions. In that context, there was nothing left to do but hire external service providers, such as MSSPs. At the same time, budgets that previously were dedicated to purchasing hardware are now being used to pay for services. But a piece of hardware was bought to last for several years, while a service is paid monthly. Therefore, when we compare year-on-year, a part of the budget has moved from CapEx to OpEx. But since MSSPs are paid for on a monthly basis, its contribution to the overall spending is not as noticeable.

Although all these factors led to a decrease in budgets, they actually lead to a new era for us. I have no doubt that budgets will recover and even grow, but this will happen in a new landscape of IT systems, more active use of the service model and cloud,” — says Veniamin Levtsov, VP, Center of Corporate Business Expertise at Kaspersky.

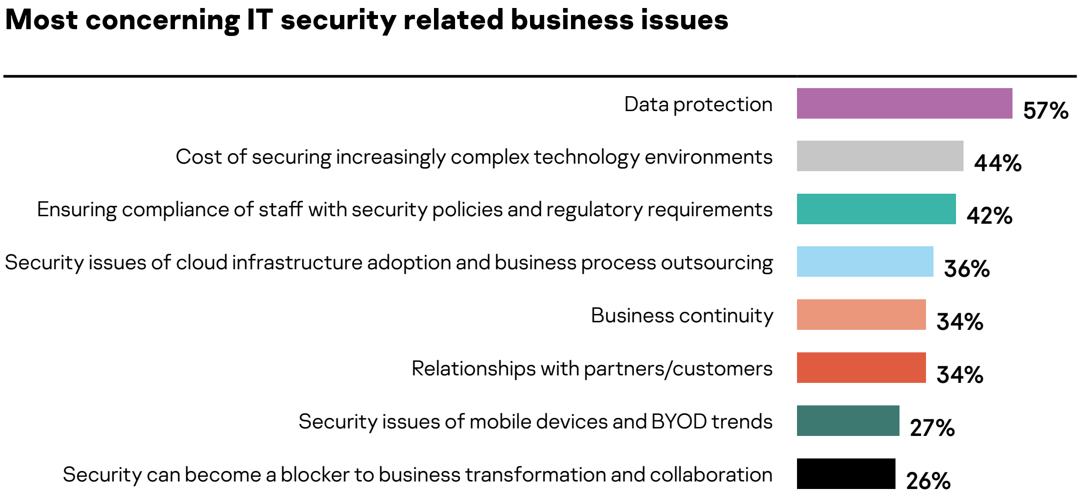
IT complexity becomes a top challenge for business

For many businesses, increasingly complex IT infrastructure and the demand for relevant expertise to support and protect it has also become a defining factor for investment.

In the top challenges that IT leaders say their businesses are facing, the cost of securing increasingly complex environments has soared to second place (44%). That's up from third place last year (41%) and sixth place in 2018. As a challenge, it's beaten only by data protection which takes the top spot (57%).

This complexity is also seeing budgets need to rise. Almost half (47%) of enterprises named increased complexity of their IT infrastructure as the top reason to expand the IT security budget (compared to 43% in 2020).

Chart 11: Top IT concerns for businesses



Rank of concern

	2018	2019	2020	2021
Data protection	1st	1st	1st	1st
Cost of securing increasingly complex technology environments	6rd	3nd	3nd	▲ 2nd
Ensuring compliance of staff with security policies and regulatory requirements	3th	2rd	2rd	▼ 3rd
Security issues of cloud infrastructure adoption and business process outsourcing	2nd	5th	4th	4th
Business continuity	5th	4th	5th	5th
Relationships with partners/customers	4th	6th	6th	6th
Security issues of mobile devices and BYOD trends	7th	7th	7th	7th
Security can become a blocker to business transformation and collaboration	N/A	8th	8th	8th

In 2021, businesses have felt even more pressure to provide continuous business functionality while also ensuring the security of their customers' digital assets, and they're turning to outsourced help to do this.

Our research found that businesses are increasingly turning to MSPs for particular skillsets to protect them in a challenging landscape. Both SMBs (52%) and enterprise (56%) stated 'requirements in special expertise' as their number one reason for appointing third party security specialists. In 2020, the main reasons for outsourcing IT security were efficiency in delivering security solutions for enterprises (70%) and financial effectiveness for SMBs (42%).

The rapid adoption of new technologies and change in work patterns, combined with the exponential growth of IT complexity, encouraged businesses to outsource security challenges to highly skilled professionals outside their organization.

With today's companies under huge pressure to keep up with the always-on, always-connected digital economy and the demand for constant innovation, we can assume that trend of engaging third-party experts will continue to grow.

Conclusion

In another difficult year for businesses, IT teams are under growing levels of pressure. Despite that pressure, our research has identified a number of recurring trends and suggests a positive outlook for the management of data breaches and security incidents.

The falling financial impact of a data breach is good news for the industry, suggesting that work and bolstering they have introduced to their IT infrastructure over the past year to secure their networks is working.

However, not all is positive. With 47% of enterprises seeing increased complexity of their IT infrastructure as the top reason to increase IT security budget, it is clear that IT teams are facing heightened challenges from a denser and more intricate tech framework.

As business challenges grow following the impact of the pandemic, IT teams are faced with protecting their organizations across a more remote IT infrastructure. In that context, the reduction of cybersecurity budgets overall is a concern, albeit an understandable one, given the cost-saving measures businesses have had to take over the past year.

IT decision-makers should be prepared for the next round of budget planning. The pandemic is still not over and the challenges of securing complex, partially remote infrastructure remain, so they need to be effective and find solutions to meet changing corporate security needs.

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.

- 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.

- In the current business environment, it's extremely important to allocate cybersecurity investments in tools which deliver optimal efficacy and ROI. This means tools which lower the level of false positives, reduce time to attack detection, time spent per case and other metrics important to any IT security team, providing the most reliable level of protection and optimizing internal resources.

- Outsourcing advanced security tasks, for example, by requesting Managed Detection and Response service from **established IT security specialists**[2] can be a good option for organizations that don't have the necessary internal expertise. Agreeing to a guaranteed service level agreement (SLA) with a 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**.

- Use **a dedicated set for effective endpoint protection**, threat detection and response products to timely detect and remediate even new and evasive threats. Kaspersky Optimum Security Framework includes the essential set of endpoint protection empowered with EDR and MDR, while Kaspersky Expert Security additionally offers anti-APT, latest threat intelligence and regular professional training to upskill your SOC team.

[2] Forrester has recognized Kaspersky as a 'Leader' in external threat intelligence services in 'The Forrester Wave™: External Threat Intelligence Services Q1, 2021' report.

Additional charts

Chart 12: Top 10 types of security incident experienced by SMBs

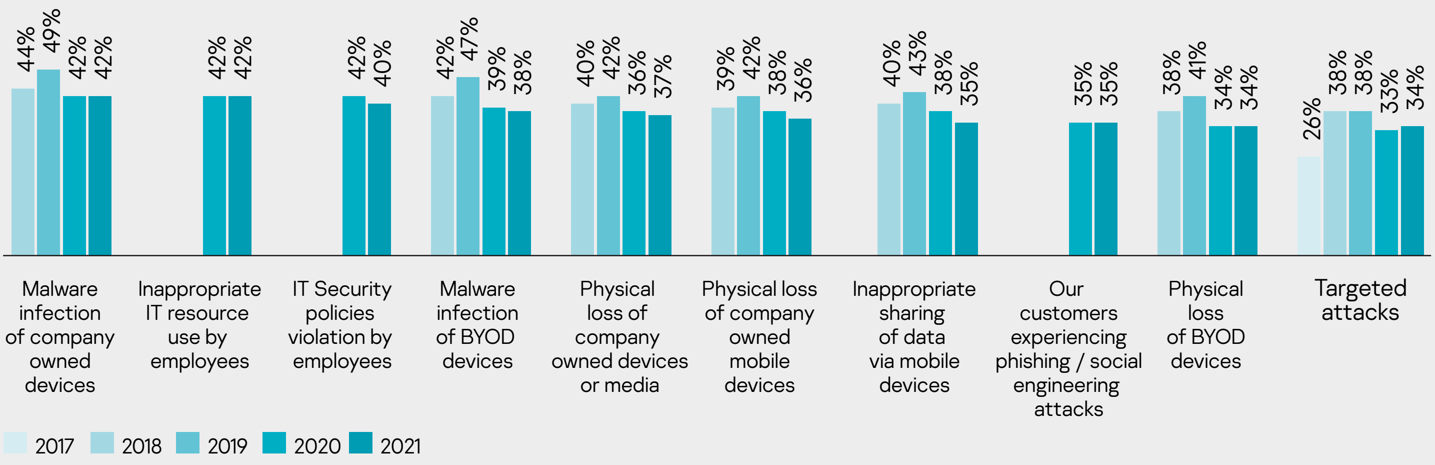


Chart 13: Top 10 types of security incident experienced, enterprises

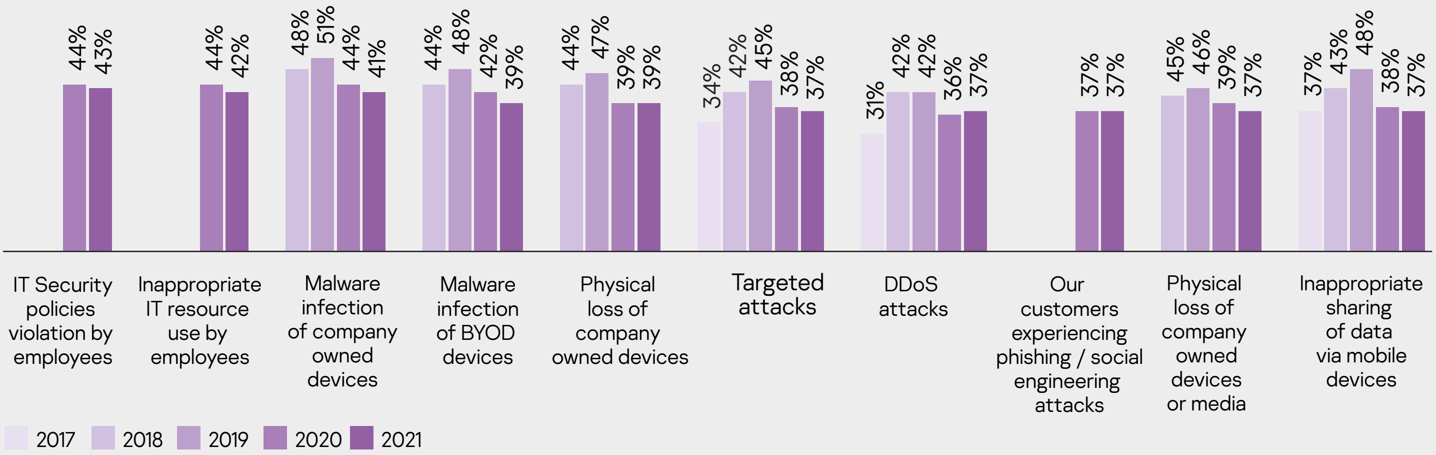


Chart 14: Top IT concerns for businesses

Most important challenges to protect against complex incidents
(by percentage, each challenge ranked in the top three for SMBs and enterprises)

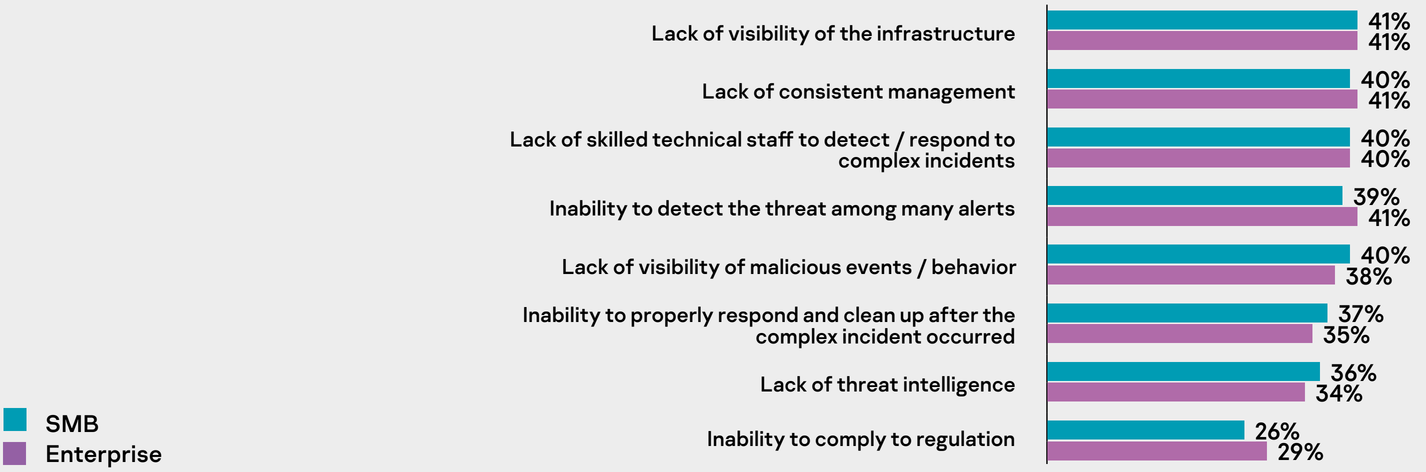


Chart 15: Reasons for outsourcing functions to MSPs / MSSPs

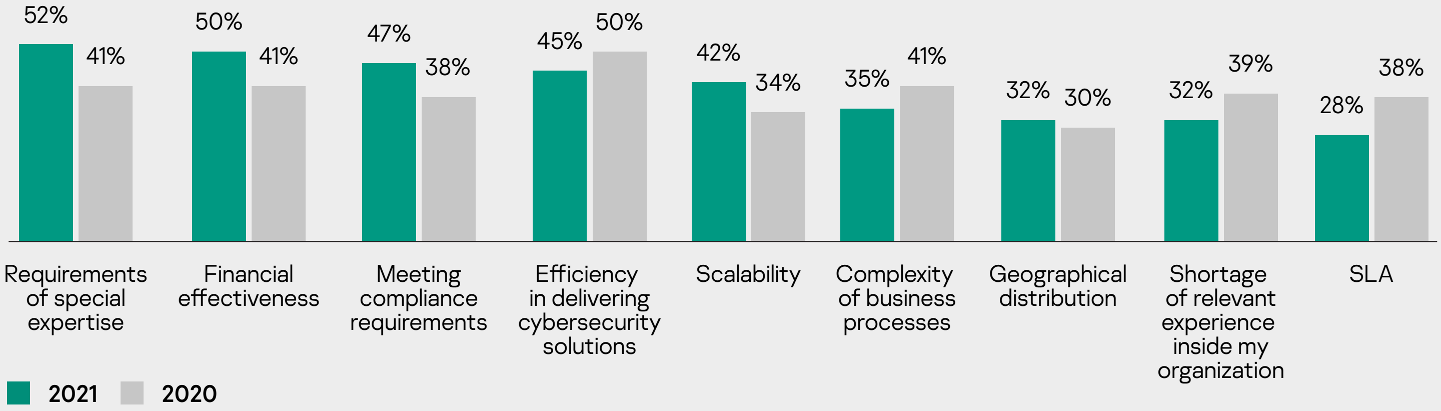


Chart 16: Time taken to detect a data breach

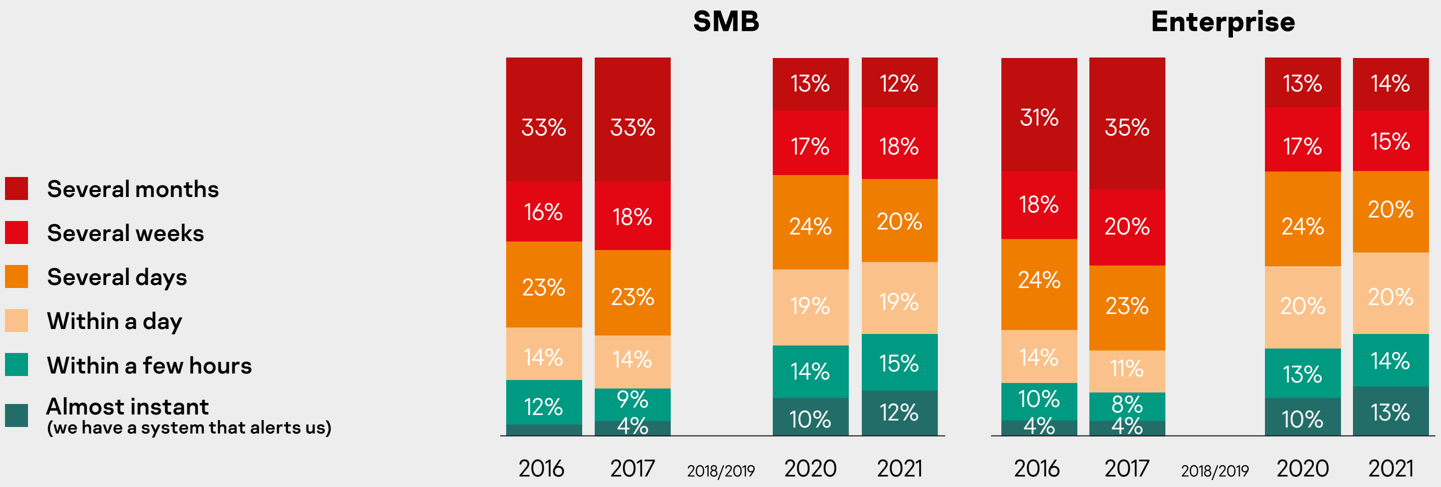


Chart 17: Breakdown of devices of different types with endpoint security software installed

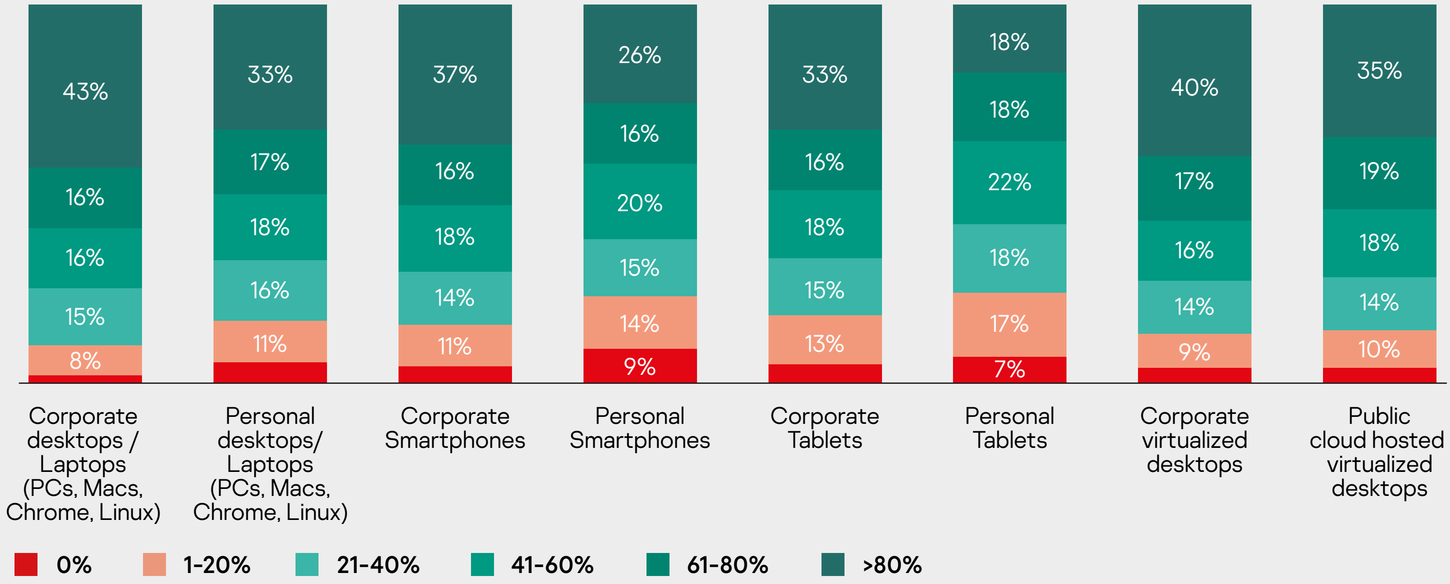


Chart 18: Devices with endpoint security software installed, by type

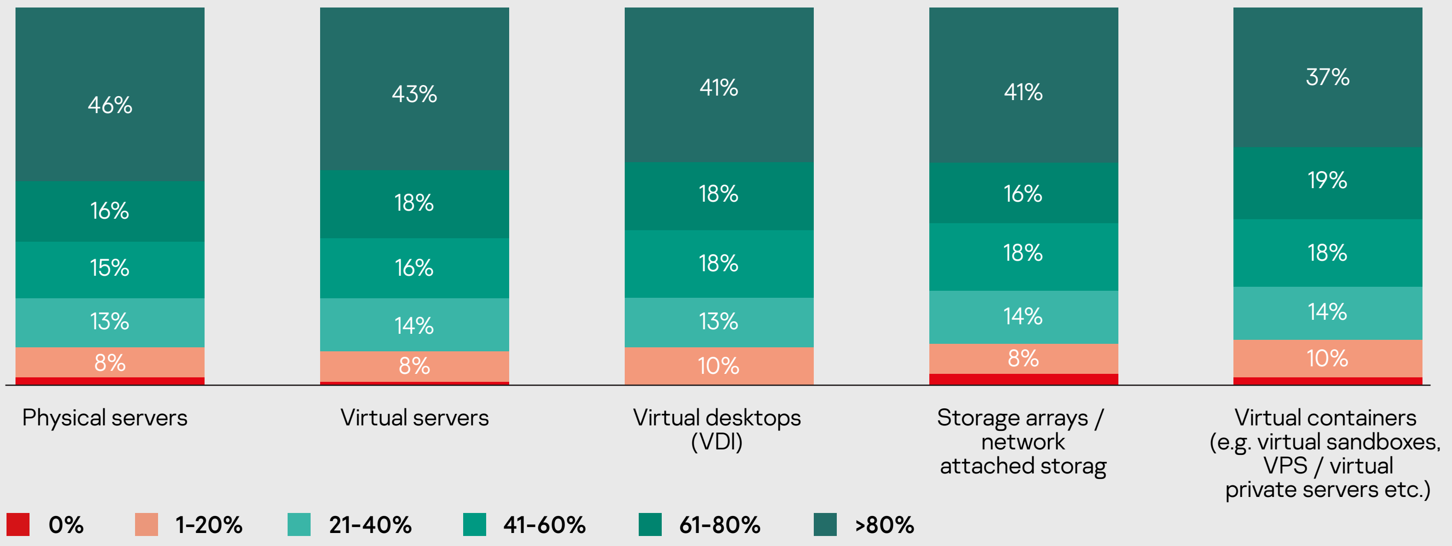


Chart 19: Top reasons for increasing IT security budgets in enterprises

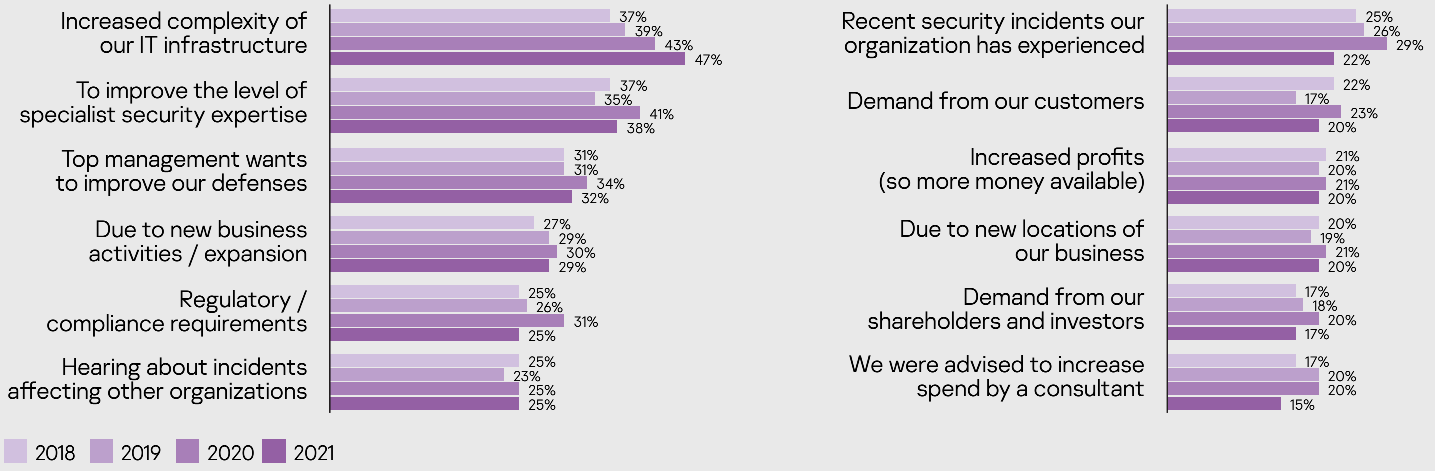
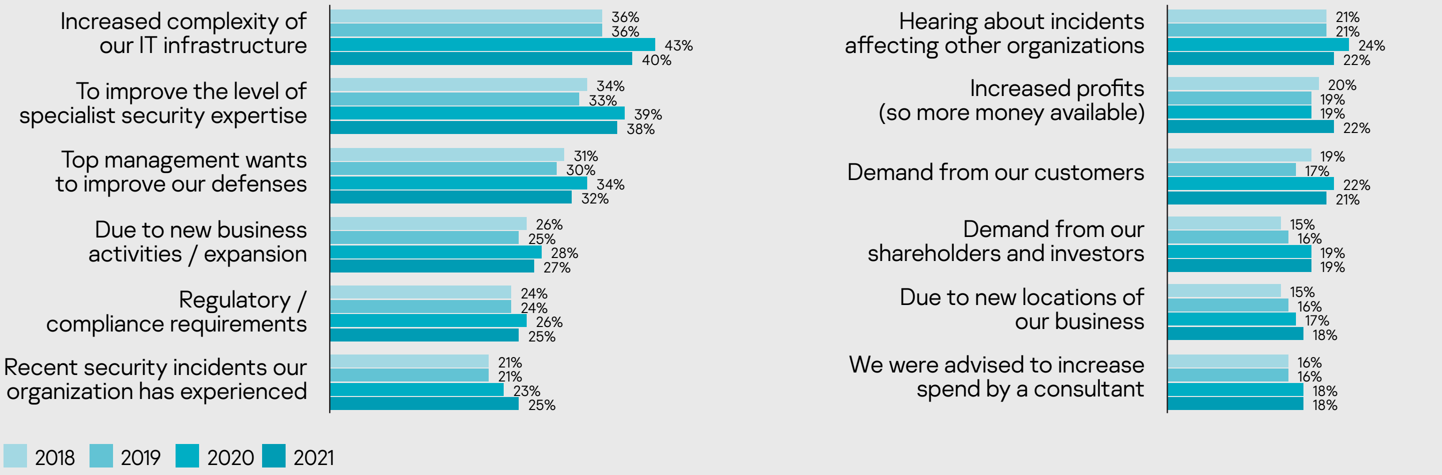


Chart 20: Top reasons for increasing IT security budgets in SMBs



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

kaspersky.com

kaspersky