

Report 2024

IT Security Economics

Tackling complexity in an era of AI, digitalisation, and cloud transformation

kaspersky

kaspersky.com

Contents

Introduction 3

Methodology 4

Key Insights 6

Increases in IT Security Spending Across the Board 6

IT Security Costing SMBs 6

A Lack of Training Poses Serious Risks 7

Incidents Overview 8

IT Security by Size 10

Large Enterprises 10

SMEs 10

SMBs 10

Sector-Specific Insights 12

Public services (Government, Education, Defense) 12

IT & Telecom 13

BFSI (Banking, Financial Services, and Insurance) 14

Manufacturing 15

HoReCa & HealthCare 16

B2B Services 17

In conclusion 18

Product recommendations 19

Introduction

IT security requirements are ever-changing. The rise of artificial intelligence (AI), digitalisation, and cloud adoption are transforming industries, **but they also introduce risks** that IT decision-makers must navigate. This report, IT Security Economics, explores how these shifts are impacting security strategies for businesses of all sizes and sectors, from large enterprises to small businesses, including public sector organisations.

AI and automation are reshaping how companies operate. AI drives innovation and efficiency, but it also exposes vulnerabilities. Cybercriminals are increasingly using AI-driven tools to launch more sophisticated attacks, while automated systems present new entry points for hackers[1]. IT teams must adapt quickly, balancing the benefits of AI with the need to **protect their digital environments.** The rapid pace of digitalisation across industries amplifies this challenge, making it crucial for security teams to stay ahead of threats in real time.

The shift towards Everything-as-a-Service (XaaS) and cloud infrastructure has seen businesses moving to subscription-based models, which offer flexibility and scalability. However, this shift brings new risks. Cloud environments, public, private and hybrid, require constant monitoring to secure vast amounts of data, and this is particularly challenging for smaller businesses with limited IT resources[2]. Large enterprises also face risks, with multi-cloud environments adding complexity to their security efforts. Public sector organisations, which often handle sensitive data, must also navigate these risks while ensuring compliance with regulations.

The globalisation of supply chains presents both opportunities and challenges for IT security[3]. Global networks enhance efficiency but create vulnerabilities. A single breach in one part of the supply chain can ripple across an entire industry, affecting businesses worldwide. At the same time, there's a growing trend towards localisation, with companies seeking to produce more goods closer to home to enhance resilience. While this helps minimise global risks, localised operations still face targeted cyberattacks, particularly in critical sectors such as **healthcare, energy, and government.**

Supply chain resilience has become **a major focus** for IT security teams, with more businesses recognising the need for greater oversight and control over their suppliers. The pandemic revealed the fragility of global supply chains, and cybersecurity is now a key part of that conversation. IT decision-makers must work to secure their entire supply chain, not just their own systems. This involves assessing vendor security practices, monitoring potential risks, and ensuring that all partners adhere to strict security protocols.

[1]Kaspersky: more than 36 million AI & gaming credentials compromised by infostealers in 3 years
[2]New group exploits public cloud services to spy on Russian agencies, Kaspersky says
[3]Kaspersky highlights AI-driven security risks in supply chains

In recent years, several high-profile cyberattacks have underscored the critical importance of robust cybersecurity.

In 2022,

the Lapsus$ hacking group targeted major companies including Microsoft and Okta, compromising sensitive customer data and leading to significant reputational damage[4].

In 2023,

Capita, a major UK outsourcing firm, suffered a cyberattack that affected its clients across the public and private sectors, costing the company an estimated **£25** million in recovery efforts[5].

For small and medium-sized businesses (SMBs), these trends present significant challenges. Limited budgets and fewer IT staff make it harder to defend against complex threats, particularly in the context of AI and cloud-based attacks. Large enterprises, with more resources, are better equipped but must manage the complexity of securing vast infrastructures across multiple geographies. Public sector institutions, too, are struggling with these issues, needing to protect critical infrastructure and sensitive information while often operating under strict budget constraints.

This report delves into these challenges and offers insights on how businesses of all sizes can better prepare for the evolving security landscape. As AI, digitalisation, and cloudification continue to reshape industries, IT decision-makers must prioritise security strategies that can keep pace with these megatrends.

[4]Lapsus$ cyberattacks: the latest news on the hacking group
[5]Cyber-attack to cost outsourcing firm Capita up to £25m

Methodology

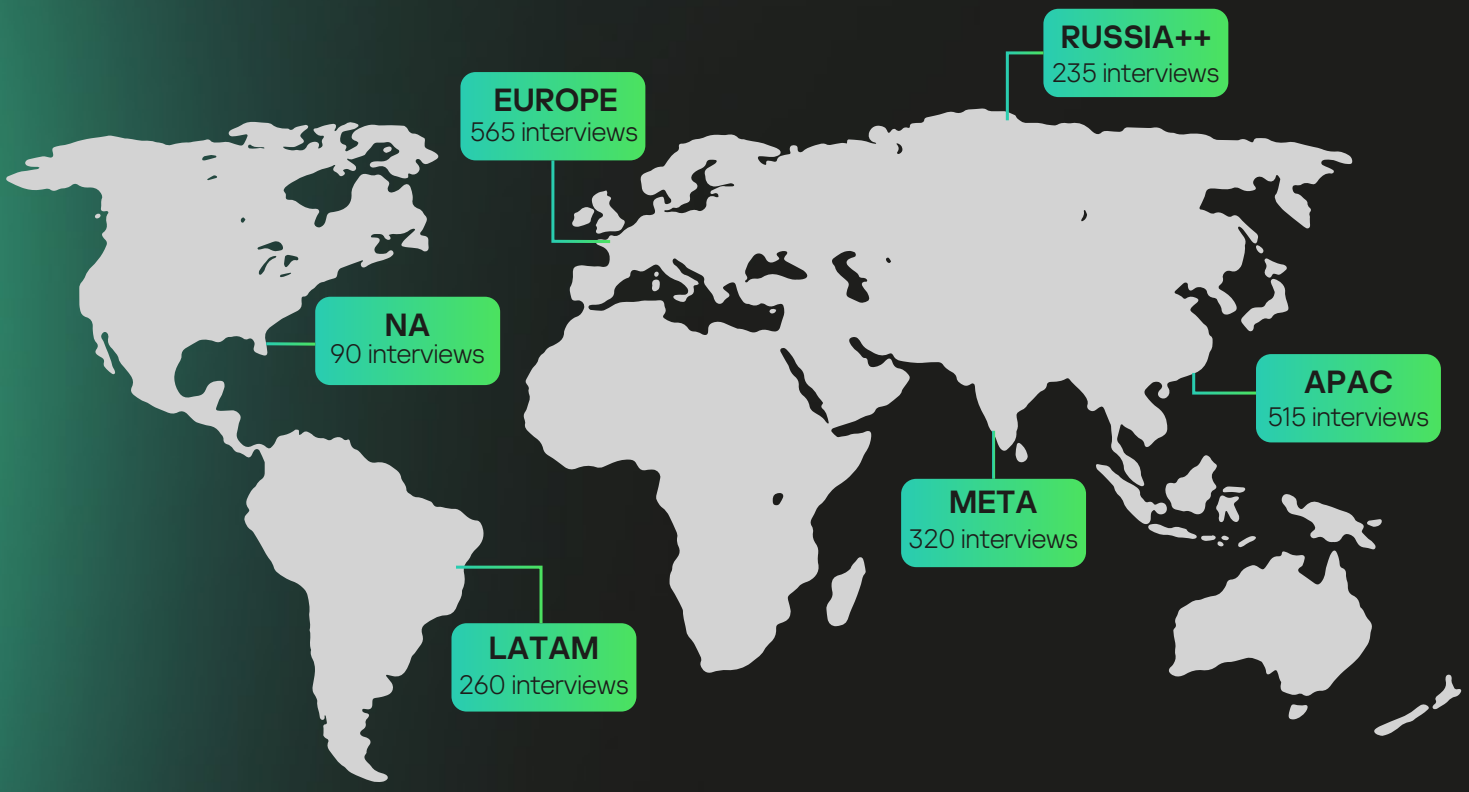
This study is based on data gathered from **1985 interviews** with decision-makers and IT security specialists working in organisations of various sizes, from

SMBs with **fewer than 500** employees,

SMEs with **between 500 and 5,000** employees

and large enterprises with **more than 5,000** employees*

It was conducted **across 27 countries** in the major markets where Kaspersky operates[6]. The scope includes a detailed analysis of IT security budgets, staffing, vulnerabilities, and industry-specific insights.



[6]Brazil, Chile, China, Egypt, France, Germany, India, Indonesia, Italy, Japan, Kazakhstan, KSA, Malaysia, Mexico, Pakistan, Philippines, Russia, South Africa, S. Korea, Singapore, Spain, Thailand, Turkey, UAE, UK and US. Respondents from these countries were questioned in 2023.
*SMB = small and medium-sized businesses; SME = small and medium-sized enterprises

Key Insights

Increases in IT Security Spending Across the Board

The survey revealed that budget allocations toward IT security have increased for all sizes of organisations.

Company size	Total IT Budget	IT Security Budget	Ratio of IT Security vs Total IT spend	Planned increase in IT Security Spend*
Large enterprises	$41.8M	$5.7M	13.6%	+ 8.5%
SMEs	$10.5M	$1.2M	11.6%	+ 9.2%
SMBs	$1.6M	$0.2M	12.5%	+ 8.8%

*Changes over the next 2 years

The relatively consistent ratio of IT security spend across different organisation sizes, coupled with a projected **almost 10%** increase over the next two years, reflects a growing recognition that cybersecurity is integral to overall IT investment, regardless of scale. As digital infrastructures become more critical, this upward trend underscores a shared industry understanding that **security** is not a discretionary expense but **a necessary safeguard to protect evolving IT environments.**

IT Security Costing SMBs

Company size	Total IT Staff	IT Security Specialists	Average number of solutions	Ratio of IT Sec to Overal IT Staff
Large enterprises	105	23	15	21.9%
SMEs	29	9	12	31%
SMBs	12	4	9	33.3%

Despite the complexity and scale of their IT security systems, large enterprises allocate a smaller proportion of their overall IT staff to security, suggesting that their significant investments in advanced IT solutions and automation deliver **greater economies of scale,** reducing the need for specialised personnel while maintaining robust security capabilities.

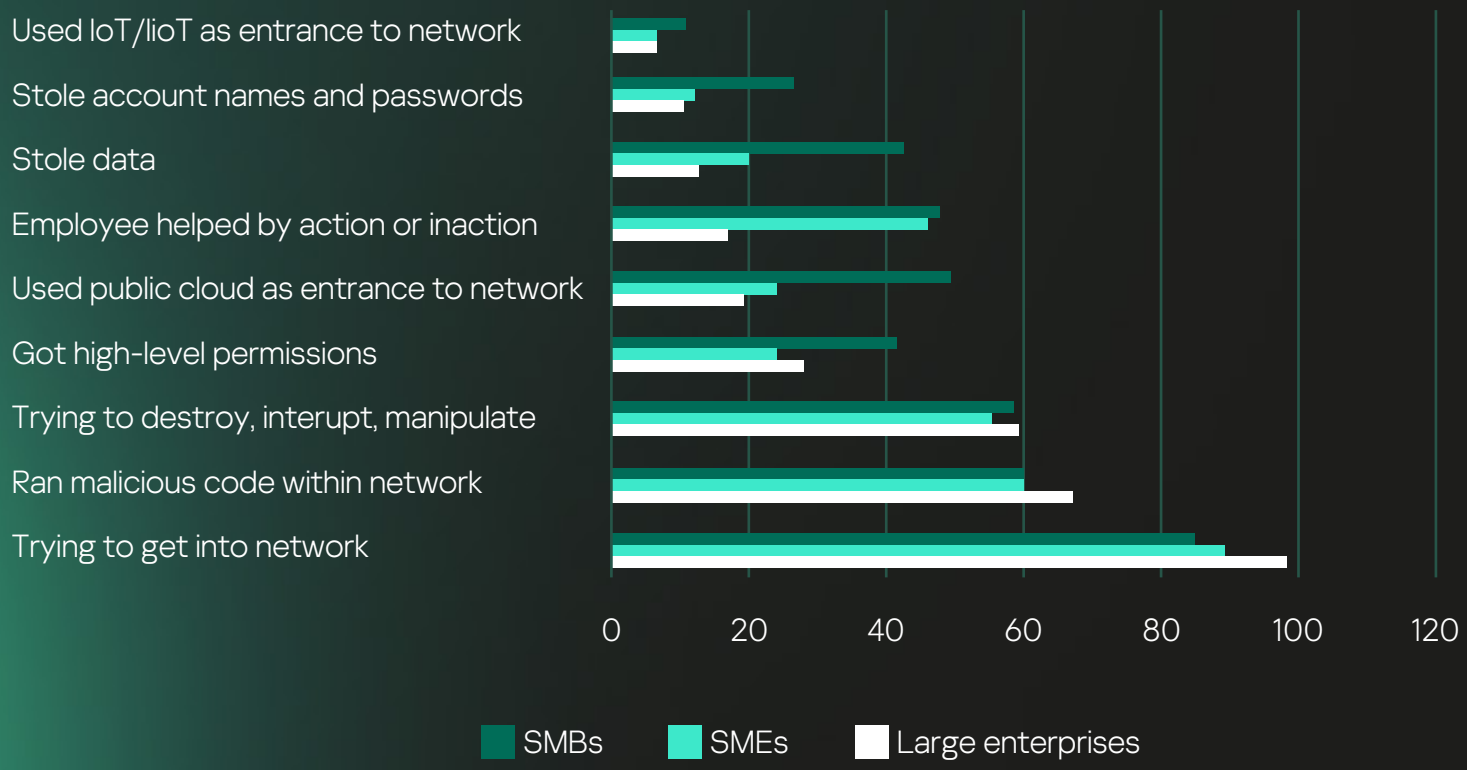
A Lack of Training Poses Serious Risks

IT Security Solution	Percentage of respondents using each solution (as an average across companies in all sectors and of all sizes)
Endpoint Security	100%
Network Security	94%
Cloud Security	83%
Security Services	75%
Cybersecurity Analytics, Intelligence, Response & Orchestration	69%
Security Training	53%

The fact that 100% of enterprises, regardless of size, have implemented Endpoint Security and nearly all have **Network Security (94%)** and **Cloud Security (83%)** and **Security Services (75%)** indicates that organisations **recognise the importance of securing** their core digital infrastructure.

However, the significantly smaller focus on **Security Training (53%)** suggests that many companies are missing crucial layers of defence. With social engineering and human error remaining among the top security vulnerabilities, the lack of employee training represents a significant gap. Without adequate training, even the most advanced technological defences can be undermined by simple, preventable mistakes.

Incidents Overview



Despite millions being spent on IT security and the near-universal adoption of network security across organisations of all sizes, an **overwhelming majority** continue to report network attacks. Large enterprises lead with **97% reporting an attack,** followed by SMEs at **88%,** and SMBs at **83%**.

The high rate of attacks, even among organisations with substantial investments in security, **highlights the persistent and evolving threat landscape.** It suggests that while securing network perimeters remains essential, attackers are finding new and sophisticated ways to breach systems, often exploiting vulnerabilities that traditional network security measures alone cannot fully address.

SMBs, in particular, are more vulnerable to data theft via public cloud services, with 49% of SMBs reporting such incidents compared to only 19% in large enterprises. This discrepancy may stem from SMBs having fewer stringent policies or systems that control the use of public cloud services, allowing employees to access or store sensitive data in unsecured environments.

Additionally, SMBs are more likely to rely on public cloud solutions rather than investing in on-premise infrastructure, which large enterprises often maintain to exert greater control over their data. This reliance on third-party services without adequate oversight can increase the risk of data exposure and theft.

"The concepts of 'network perimeter security' and 'trusted networks' have long lost their relevance. However, many companies still rely only on network security solutions such as firewalls and IPS, while attackers are already using alternative attack vectors, such as phishing emails with malicious links or supply chain attacks. To carry out a successful attack on a company, an attacker does not forcibly need to rely on zero-day exploits. Sometimes, it may be enough for just one user to click on a malicious link, or for a contractor's vulnerable infrastructure to lack proper information security protection. All this confirms the idea that information security should be based on a comprehensive and systematic approach, rather than being limited to the implementation of individual point-specific measures," **comments Alexey Vovk, Information Security Director at Kaspersky.**

Another key factor contributing to security breaches, particularly among smaller firms, is human error. Mistakes or negligence by employees, whether due to a lack of security awareness or insufficient training, are leading causes of breaches in organisations[7] .

With **only 53% of companies** investing in security training, many remain exposed to social engineering attacks, phishing, and other forms of human-related vulnerabilities. Strengthening employee education on security best practices could significantly reduce the number of incidents stemming from avoidable errors.

[7]Redefining the Human Factor in Cybersecurty

IT Security by Size

	Large enterprises	SMEs	SMBs
IT budget	$41.8M	$10.5	$1.6M
Spend on IT security	$5.7M	$1.2M	$0.2M
Increase IT spend over two years	+8.5%	+9.2%	+8.8%
Average number of incidents	12	13	16
Average company losses	$6.2M (1.1x their security budget)	$1.7M (1.4x their security budget)	$0.3M (1.5x their security budget)

Despite their larger resources and advanced security infrastructures, the sheer scale and complexity of large enterprise organisations make them more susceptible to costly breaches. While these enterprises are often better equipped to detect incidents quickly, the time required to fully respond and mitigate these threats can span hours, underscoring the challenge of managing widespread, complex IT environments.

SMBs are the most disproportionately affected group in terms of budgetary impact. SMBs often lack robust cybersecurity policies and procedures, which leaves them vulnerable to incidents involving employees, public cloud misconfigurations, and high-level permissions.



"The data illustrates the continuation of the current trend of increasing cybersecurity spending across all market segments and verticals. This growth is driven by at least three key factors. First, the constant growth in the complexity of cybersecurity threats. In practice, we see that most situations security teams encounter are related to advanced or emerging threats. As a result, traditional solutions become less efficient, and organizations are forced to adopt other tools that enhance the detection of attack traces, reduce the workload on security personnel, and automate responses.

Secondly, we see increasing concerns from governments regarding digital sovereignty, which includes monitoring cybersecurity events in Critical Infrastructure networks. This has led to the emergence of new regulations and regulatory requirements. All of this inevitably leads to new expenses and the hiring of new employees.

The third factor influencing the growth of cybersecurity budgets and costs, and thus the prices of services offered by MSSPs, is the constant increase in salary expectations for professionals in various cybersecurity fields.

Regarding the cost structure in the small and medium business segment, the complexity and high costs of infrastructure support leave businesses with little choice but to rely more heavily on service providers. This is particularly true for cloud data storage, backup, and cybersecurity tasks, such as endpoint event monitoring or email traffic scanning. As a result, payments to service providers are becoming an increasingly significant part of the SMB sector's cost structure. This steady rise drives budget growth while enabling these companies to survive in the harsh world of modern cybersecurity threats," **comments Veniamin Levtsov, Vice President, Center of Corporate Business Expertise at Kaspersky.**

As cloud adoption and remote work continue to rise, the human factor and inadequate cloud security policies remain critical areas of vulnerability, especially for these smaller enterprises. These insights underscore the importance of tailored security strategies that address the specific risks faced by organizations based on their size and resources.

Sector-Specific Insights

Public services (Government, Education, Defense)

IT budget	$8.2M
Spend on IT security	$1M
Increase IT spend over two years	+8.9%
Average number of incidents	18
Average company losses	$1.1M (1.1x ratio versus IT security budget)

Top Concerns	Top Challenges
39% Suffering downtime/loss of productivity	**34%** Loss of access to customer service; **33%** IT security considered as a blocker to business transformation; **32%** Long time taken to respond
34% Cost of complex securing tech. environments	**45%** Involving non computing devices; **36%** Managing security across platforms: **31%** Incorrect operation
24% Issues with data protection	**40%** Physical loss; **35%** Leakage of data [employees]; **34%** Leakage of data [cyberattacks]

With an IT budget of **$8.2M** and a **$1M** spend on security, this sector demonstrates a relatively low-security investment relative to its size and complexity. The high number of incidents **(18)** and average company losses of **$1.1M,** which equate to **1.1** times their security budget, indicate that these organisations are frequently targeted but lack the resources and maturity to prevent or respond effectively. With lower adoption of key security solutions like Anti-DDoS, Threat Intelligence (TI), and Vulnerability Management (VM), this sector often struggles with employee-related incidents and data theft. Longer response times suggest a need for better incident management and faster detection to reduce losses.

IT & Telecom

IT budget	$6.9M
Spend on IT security	$1.1M
Increase IT spend over two years	+8.9%
Average number of incidents	10
Average company losses	$2.8M (2.5x ratio versus IT security budget)

Top Concerns	Top Challenges
38% Cost of complex securing tech. environments	**46%** Involving non computing devices; **39%** CS errors leave systems unprotected; **35%** Managing security across platforms
34% Suffering downtime/loss of productivity	**49%** Long time to detect; **40%** Long time to respond: **39%** Loss of access to customer services
32% Issues with data protection	**48%** Physical loss of devices or media; **34%** Leakage of data [cyberattacks]; **27%** Leakage of data [employees]

With a mature security posture, IT & Telecom spends **$1.1M** on security and experiences relatively few incidents **(10)**. However, when breaches do occur, they are costly, with average losses of **$2.8M (2.5x the security budget)**. The sector's extensive use of advanced security solutions like EDR, XDR, and Cloud Infrastructure Entitlement Management (CIEM) helps prevent frequent intrusions, but when targeted, the attacks are often sophisticated and go undetected for long periods, resulting in major financial and operational damage.

BFSI (Banking, Financial Services, and Insurance)

IT budget	$8.3M
Spend on IT security	$1.2M
Increase IT spend over two years	+9.3%
Average number of incidents	8
Average company losses	$3.2M (2.7x ratio versus IT security budget)

Top Concerns	Top Challenges
41% Suffering downtime/loss of productivity	**46%** Long time to detect; **42%** Loss of access to customer services; **41%** Loss of access to internal services
36% Cost of complex securing tech. environments	**43%** Managing security across platforms: **39%** Incorrect operation: **35%** Involving non computing devices
27% Issues with cloud infrastructure adoption	**45%** Affecting virtualized environments; **42%** Affecting IT infrastructure hosted by a 3rd party; **32%** Affecting 3rd party cloud services used

BFSI leads in security investment with a **$1.2M** budget and robust adoption of security services like SIEM and Extended Detection and Response (XDR). With fewer incidents **(8)** and faster detection and response times, BFSI demonstrates that heavy security investment pays off. Despite this, their average loss per incident is **$3.2M (2.7x their security budget)**, reflecting the high stakes involved in financial services. However, the sector's focus on security education and sophisticated tools underscores the effectiveness of well-funded security programs in reducing the frequency and impact of breaches.

Manufacturing

IT budget	$6M
Spend on IT security	$0.7M
Increase IT spend over two years	+8.4%
Average number of incidents	17
Average company losses	$1.8M (2.5x ratio versus IT security budget)

Top Concerns	Top Challenges
43% Suffering downtime/loss of productivity	**44%** Long time to detect; **35%** Loss of access to customer services; **33%** Long time to respond
38% Issues with data protection	**46%** Leakage of data [cyberattacks]; **36%** Leakage of data [employees]; **33%** Physical loss
33% Cost of complex securing tech. environments	**47%** Involving non computing devices; **33%** Managing security across platforms; **27%** Incorrect operation

Manufacturing operates with a smaller IT budget **($6M)** and a modest **$0.7M** spend on security, leading to substantial financial losses—**$1.8M** per incident, or **2.5 times** their security budget. While this sector has a higher usage of solutions like Managed Detection and Response (MDR) and Threat Intelligence compared to similar maturity-level industries, it still faces significant challenges in detecting and responding to incidents, particularly involving IoT, password theft, and high-permission breaches.
The need for several days to respond to threats highlights the vulnerability of manufacturing operations to persistent attacks.

HoReCa & HealthCare

IT budget	$5.4M
Spend on IT security	$0.6M
Increase IT spend over two years	+9.3%
Average number of incidents	18
Average company losses	$1.8M (2x ratio versus IT security budget)

Top Concerns	Top Challenges
40% Issues with data protection	**44%** Physical loss of devices or media; **37%** Leakage of data [cyberattacks]; **33%** Leakage of data [employees]
34% Cost of complex securing tech. environments	**41%** Involving non computing devices; **37%** Managing security across platforms: **29%** Identifying vulnerabilities in IT systems
33% Suffering downtime/loss of productivity	**37%** Long time to detect; **34%** Long time to respond; **32%** Loss of access to customer services

HoReCa & Healthcare while having different operational requirements have been grouped together because they have the similar statistics on the incidents and IT budgets. With an average IT budget of **$5.4M** and a security spend of **$0.6M,** this sector is underfunded when compared to the threats it faces. Despite an average number of incidents of **18**, the sector's security maturity remains low, with only a strong focus on security training. The average losses of **$1.8M (2x their security budget)** reflect this gap, particularly as these industries face incidents involving malware, public cloud vulnerabilities, and high-permission breaches. Detection and response times often span weeks, leaving these organizations exposed to prolonged risks.

B2B Services

IT budget	$2.2M
Spend on IT security	$0.3M
Increase IT spend over two years	+8.9%
Average number of incidents	11
Average company losses	$0.6M (2x ratio versus IT security budget)

Top Concerns	Top Challenges
42% Suffering downtime/loss of productivity	**33%** Long time to detect; **31%** Long time to respond: **31%** Loss of access to customer services
31% Issues with data protection	**39%** Leakage of data [employees]; **38%** Leakage of data [cyberattacks]; **38%** Physical loss
28% Cost of complex securing tech. environments	**43%** Managing security across platforms; **32%** Involving non computing devices; **23%** Maintaining security of olde systems

With a smaller IT budget of **$2.2M and $0.3M** allocated to security, B2B businesses face fewer incidents **(11 on average),** but the ratio of losses **($0.6M)** to security budget **(2x)** reveals that even a few incidents can cause significant damage. With the lowest security budget and team size among the sectors, this vertical underutilises most security solutions, making it more prone to data and password theft. However, its lower profile may reduce the frequency of attacks, even as reliance on cloud services remains a key vulnerability.

In conclusion

The evolving landscape of IT security poses significant challenges for businesses of all sizes. As AI, digitalisation, and cloud adoption continue to reshape industries, organisations must remain vigilant against increasingly sophisticated cyber threats. The data gathered in this report highlights the critical importance of investing in robust cybersecurity strategies, from securing cloud environments to safeguarding operational technology.

While large enterprises often face complex security issues due to the scale of their operations, SMBs and public sector institutions struggle with limited resources and high-impact incidents. Across all sectors, the integration of advanced security solutions, coupled with a focus on employee training, is essential to mitigating risks and maintaining resilience in an ever-changing threat landscape.

In addition to investing in cybersecurity solutions additional help is at hand. To support organisations of all sizes across all sectors, Kaspersky has five Expertise Centers that embody the organisation's leadership in global cybersecurity, each playing a critical role in addressing complex digital threats.

The Global Research and Analysis Team (GReAT) leads investigations into sophisticated attacks, cyber espionage, and major malware trends.

The Threat Research Center specialises in anti-malware and content filtering, actively developing detection methodologies and secure software development practices.

The AI Technology Research Center focuses on AI-powered threat detection and generative AI solutions to enhance cybersecurity.

The Security Services Center provides managed detection, incident response, and security assessments.

The ICS CERT Center focuses on industrial cybersecurity, delivering specialised research and consultancy for critical infrastructure.

Together, these entities leverage the expertise of over 5,000 specialists to deliver cutting-edge cybersecurity solutions and services globally.

Product recommendations

Anticipate and budget cyber and data risks relevant to your country and industry by using specialised resources such as **IT Security Calculator.** This tool will help you to maximise the efficiency of your protective measures.

To protect the company against a wide range of threats, use solutions from **Kaspersky Next** product line that provide real-time protection, threat visibility, investigation and response capabilities of EDR and XDR for organisations of any size and industry. Depending on your current needs and available resources, you can choose the most relevant product tier and easily migrate to another one if your cybersecurity requirements are changing.

Additional expertise without additional hiring can be achieved by adopting a managed security service such as **Kaspersky Managed Detection and Response.** It allows the best possible advanced automated security services and analysis of corporate data gathered every day, in real time, 24/7, to help protect against sophisticated cyberattacks, even if company lacks security workers.

Provide your InfoSec professionals with in-depth visibility into cyberthreats targeting your organization. The latest **Kaspersky Threat Intelligence** will supply them with rich and meaningful context across the entire incident management cycle and help to identify cyber risks in time.

To make your cloud adoption, digital transformation and DevOps practice safer, use solutions from **Kaspersky Cloud Workload Security** ecosystem that frees up your information security service resources to address other tasks, reduces operational and infrastructure costs, improves visibility and ensures compliance in any cloud environment.

Invest in additional cybersecurity courses for your staff to keep them up to date with the latest knowledge. With practically oriented **Kaspersky Expert training,** InfoSec professionals can advance their hard skills and be able to defend their companies against sophisticated attacks.