Report 2024

Enterprise cybersecurity and increasing threats in the era of AI: Do business leaders know what they are doing?

kaspersky

LEARN MORE: KASPERSKY.COM

Contents

Introduction

Business leaders are overwhelmed amidst the complexities of securing their organizations against relentless digital assaults

In today's volatile digital landscape, safeguarding company assets against cyber threats stands as an unyielding imperative. Everyone, from CEOs and CISOs to frontline employees, acknowledges the pervasive dangers posed by cybersecurity breaches. Whether it's the sensitive customer data entrusted to us, the intricate web of employee and banking records, or the intricate threads of our supply chain information, data reigns as the lifeblood of modern businesses. Yet, despite constant reminders of cybersecurity threats and the increasing investments in digital defense mechanisms, many business leaders are overwhelmed amidst the complexities of securing their organizations against relentless digital assaults.

Although business leaders are aware of the dangers, Kaspersky research has uncovered a sobering truth: that most misunderstand the complexities of cyber threats, underestimating the ingenuity and persistence of threat actors in infiltrating their targets. This, compounded by a lack of clarity in resource allocation, leaves a significant proportion of business leaders grappling with the enigmatic labyrinth of digital defense.

Moreover, as businesses brace themselves against the relentless tide of cyber threats, they must also contend with the emerging threats caused by the new AI technologies and the resulting regulatory frameworks that loom on the horizon. Regulations like WP 29, NIS-2, the EU Resilience Act, and the forthcoming EU Supply Chain Directive covering everything from how we interact with chatbots and AI tool development, to digital supply chain transparency.

The pressing question arises: do business leaders fully grasp the magnitude of the issue, or do they find themselves trailing behind, teetering on the brink of irreparable damage to their operations and reputation?

Kaspersky is at the forefront of comprehensive cybersecurity developing solutions designed to tackle the constantly evolving threat landscape, while also addressing the shortcomings of traditional security tools and education. In this report, we will analyze the critical cybersecurity challenges faced by companies globally, drawing insights from Kaspersky's findings and other reputable sources to show there is a growing need for greater education for business leaders and IT security teams alike that both empower executives and enhance their organization's security posture.

Our insights also reveal a growing need for flexible seamless automated cybersecurity protection solutions, such as Kaspersky Next, with advanced capabilities enabling companies to effectively detect, investigate, and respond to advanced threats in real-time. Persistent gaps in cybersecurity knowledge and preparedness among C-suite decision-makers, and skill shortage also highlights a pressing need for tiered EDR and XDR products that suit varying business needs, while also delivering a proactive understandable approach to cybersecurity. Finally, we will present actionable insights and recommendations, guiding organizations towards a safer, more resilient future amidst the ever-shifting sands of the digital landscape.

Methodology

Gen AI tools were examined to gain insights into emerging challenges and concerns within cybersecurity.

This comprehensive report explores the latest research, surveys, and reports of Kaspersky, enriched by insights from Kaspersky experts, to provide a thorough analysis of the cybersecurity landscape (sources see Appendix). The reports include interviews with C-suite executives across Europe discussing their views on cybersecurity and responses from IT employees in companies in the region. Key metrics such as budget allocation trends, incident rates, and the impact of human error were extracted from these sources to offer a holistic view of the C-suite's preparedness for modern cyber warfare. Additionally, recent studies on the adoption and implications of Gen AI tools were examined to gain insights into emerging challenges and concerns within cybersecurity. The research aims to pinpoint recurring patterns, identify gaps, and highlight areas requiring urgent attention, offering a comprehensive understanding of the cybersecurity challenges facing European companies and offer possible solutions to help bolster organizations' cyber-defenses against both present and future cyberthreats.

Key findings: Companies do not know what they are doing when it comes to cybersecurity

1. According to latest Kaspersky research studies, it seems C-suite and IT decision makers in companies do not really know how to protect their company – assets, data, information – successfully against recent cyberattacks. The issue is drawn down to "normal" employees introducing cyber incidents caused by human failure – even by Infosec professionals:
   - Companies and SMBs are investing millions in IT, yet 38% say they're confused by basic cybersecurity terms like Malware, Phishing and Ransomware.
   - Almost half (48%) of C-suite security specialists reveal terms and jargon are the biggest barrier to management understanding cybersecurity and how to tackle it. Budget restrictions (47%), insufficient training (43%), are challenges as well.
   - Additionally, the global cyber skills shortage is also impacting how organizations react to threat actors, with 75% of companies viewing the scarcity of skilled staff as a serious problem.
   - Genuine errors by staff are responsible for more than 10% of cyber incidents, with regular staff causing 16% of incidents, IT employees contributing 15%, and even IT executives accounting for 14% of the damage. Intentional violations of information security policies by employees accounted for more than a quarter (26%) of all cyber incidents in the past two years.

2. Facing the AI area, companies need to urgently prepare for a raft of upcoming global artificial intelligence (AI) and digital legislation regulations. Kaspersky research shows companies should be resourcing their efforts for cybersecurity more effectively. They must proactively prepare now, so they do not fall behind in the race against cybercriminals and hackers:
   - European firms face an ever-increasing onslaught of cybersecurity challenges, yet they lack state-of-the-art security measures or adequate protocols – such as backups or robust password policies – to stay protected. This indicates that many companies are far behind in threat protection. In the region, 77% of companies have experienced at least one cyber incident in the past two years, and 75% reported these attacks were serious.
   - Additionally, with artificial intelligence driving everything from customer chatbots to data processing, firms need to prepare for regulations urgently proactively such as WP 29, NIS-2, EU Resilience Act, and forthcoming EU Supply Chain Directive.
   - Companies need to resource their cybersecurity efforts more effectively to future proof their organization.
   - Few companies have implemented safeguards, as only 59% worry about AI-related data leaks. Only 22% considered regulating its use, yet a quarter (24%) identify IT and cybersecurity as departments they are inclined to automate.

Gaps in the C-suite's knowledge

38%

Overall CEOs, CISOs, decision makers and managers in IT security do not know how to protect their company – assets, data, information – successfully against cyberattacks.

Kaspersky's latest Security Economics Report [1] shows companies and SMBs are investing millions in IT, yet according to the study, **'Separated by a Common Language' 38% say** [2] they're confused by basic cybersecurity terms like Malware, Phishing and Ransomware.

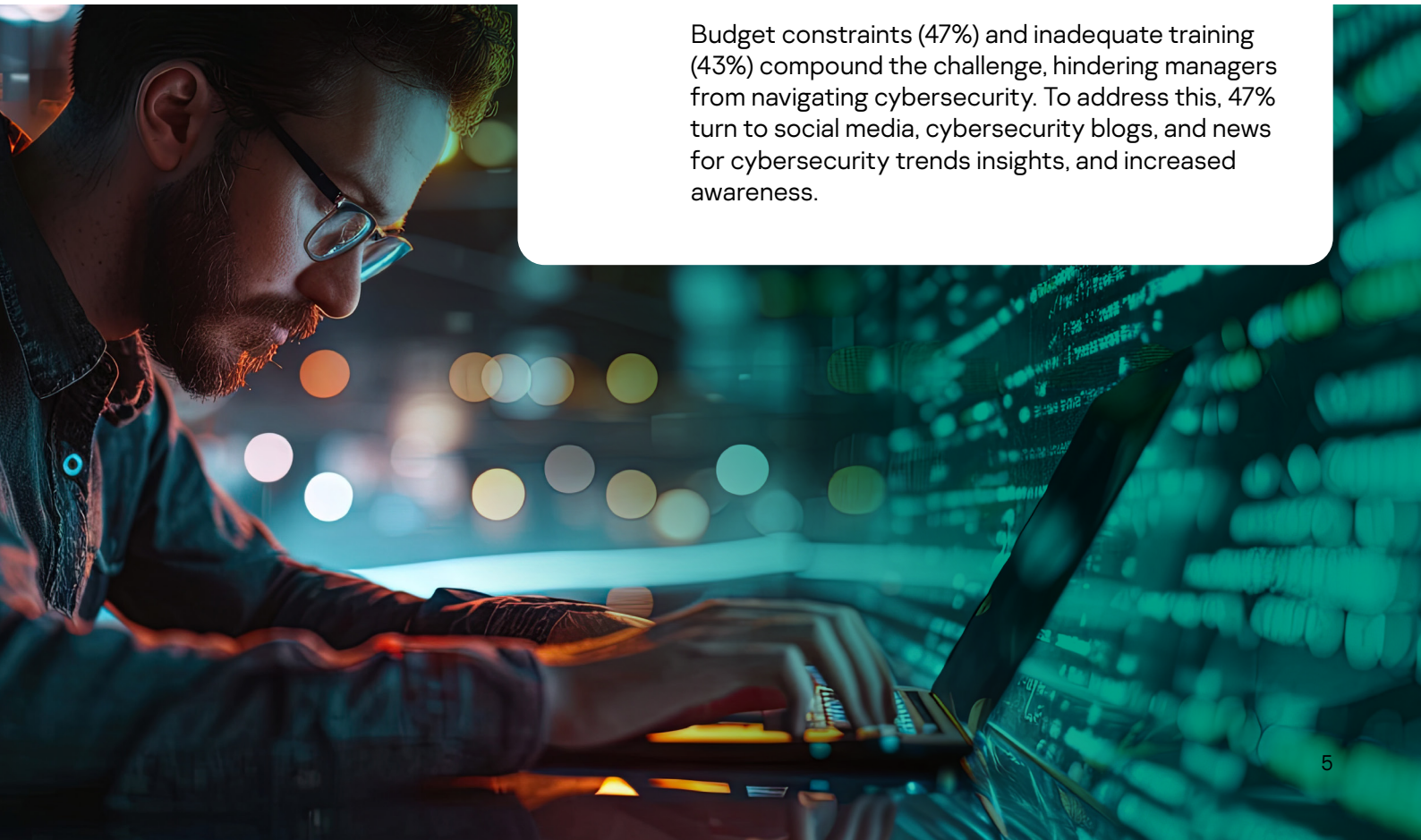
Almost half of executives (49%) acknowledge the current cyberthreat landscape concerns them more than economic factors like inflation and interest rates (37%) and prioritize the topic in the boardroom always (51%) or sometimes (43%) [3]. Yet the larger the company, the less aware the C-suite are of cyber threats with only 35% of large companies admitting they knew of attacks compared to 52% in companies SMBs.

Kaspersky also revealed that 38% C-suite decision makers in large enterprises find basic cybersecurity terms like Malware, Phishing, and Ransomware perplexing

48%

Nearly half (48%) of C-suite security specialists admit convoluted jargon and industry terminology is a primary barrier hindering understanding and effective management of cyber issues. In the report 'Separated by a Common Language' [2] Kaspersky also revealed that 38% C-suite decision makers in large enterprises find basic cybersecurity terms like Malware, Phishing, and Ransomware perplexing. Other terms such as Botnet, APT (Advanced Persistent Threats), and Zero-Day exploit threats are also unknown, as well as cybersecurity terms like DecSecOps, ZeroTrust, SOC, and Pentesting.

Budget constraints (47%) and inadequate training (43%) compound the challenge, hindering managers from navigating cybersecurity. To address this, 47% turn to social media, cybersecurity blogs, and news for cybersecurity trends insights, and increased awareness.



Most cybersecurity incidents caused by employees

64%

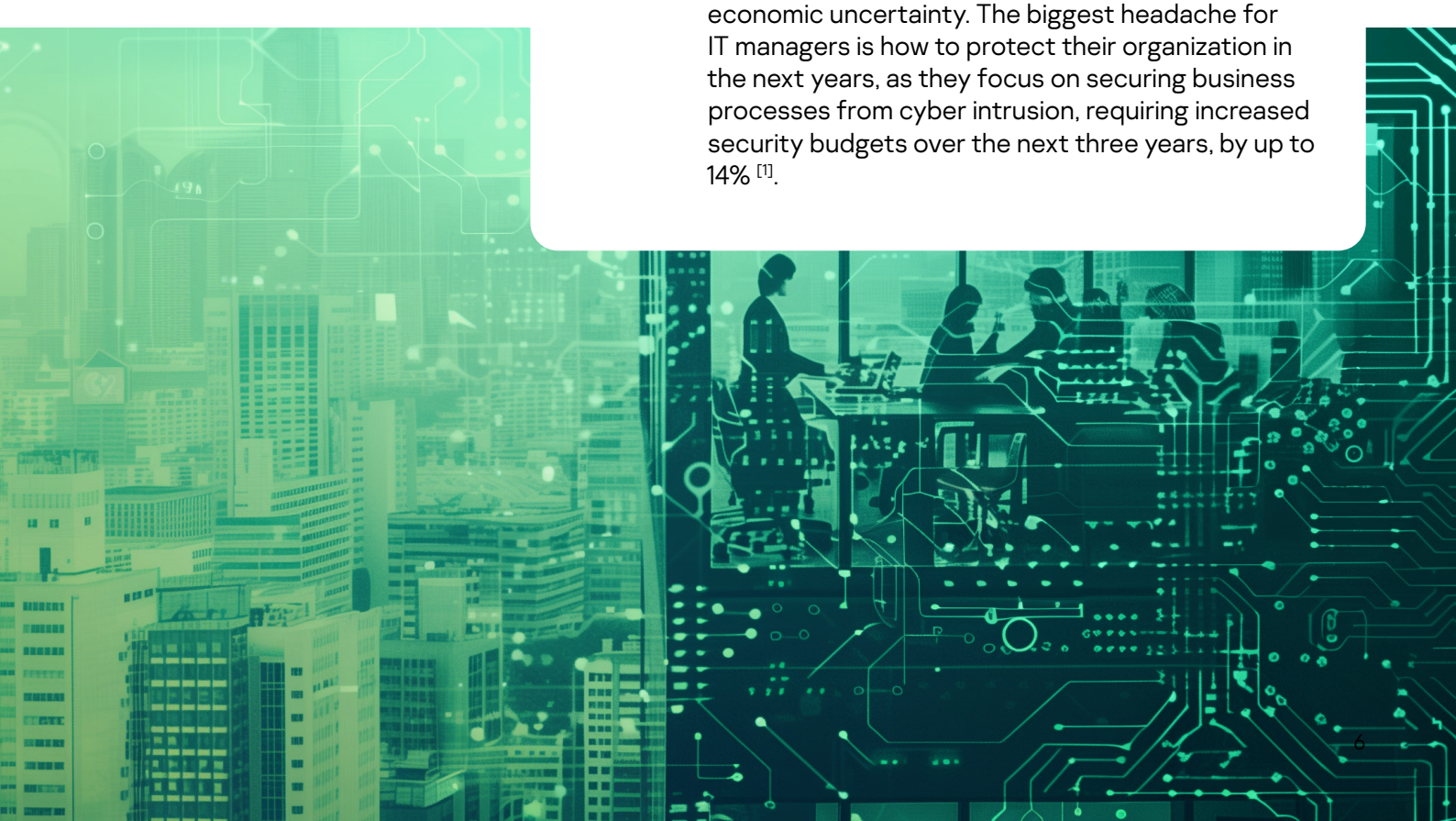
To compound the increased threats, the human factor also contributes to the problem. The Kaspersky study 'Redefining the Human Factor in Cybersecurity' [3], employee errors are also partly responsible for the problem. This report found 64% of all cyber incidents in the past two years resulted from human error. Unintentional errors made by internal staff are the most common cause of cybersecurity breaches. Mistakes by IT professionals accounted for 15% and 14% by senior infosec professionals; non-IT workers caused 16% of these breaches.

Our research also reveals IT security teams are now battling data leakages caused by employees almost as frequently as breaches caused by cyberattacks, following the introduction of new staff laptops or tablets, and Virtual Private Networks to enable remote working last year. This year we found there has also been a shift in the mindsets of organizations as many transitioned certain functions to outsourced services such as managed service providers (MSP) and managed security service providers (MSSP) to find more efficient ways of delivering cybersecurity solutions. This contrasts with 2023, when IT managers were considering transitioning to cloud servers and collaboration software.

General cybersecurity trends are pushing organizations into a proactive position as they now have to protect themselves under conditions of rapid digitalization

26%

But worryingly, 26% of cybersecurity breaches [3] were caused by staff deliberately violating company protocol. This behavior poses a comparable risk to business security as external hacking, which was reported by 30% of respondents. General cybersecurity trends are pushing organizations into a proactive position as they now have to protect themselves under conditions of rapid digitalization, and skills shortages amid continuing geopolitical and economic uncertainty. The biggest headache for IT managers is how to protect their organization in the next years, as they focus on securing business processes from cyber intrusion, requiring increased security budgets over the next three years, by up to 14% [1].



Understaffed and under skilled IT departments

Of staff hired

53% [4]

did not hold a post-graduate degree.

In its study, **'Redefining the Human Factor in Cybersecurity'** [3], Kaspersky also found out another reason companies feel vulnerable to cyberattacks is skills shortages, with 18% saying incidents occurred for this reason. This concern is widespread, with three-quarters of companies viewing the scarcity of skilled staff as a serious problem.

In response to identified gaps in their cybersecurity infrastructures, 41% of companies [4] plan to ramp up investments in this domain in the foreseeable future. However, among the surveyed companies in the **'Redefining the Human Factor in Cybersecurity'** [3] study, 21% of respondents reported lacking the budget to implement sufficient cybersecurity measures, while 28% expressed confidence in possessing the necessary resources to preempt potential threats.

Yet even those companies with the budget and the will to hire qualified staff are having difficulties filling those vital roles. In its study, **'The portrait of a modern information security professional'** [4], Kaspersky discovered also that 1% of InfoSec professionals say their organization's cyber security teams are "somewhat" or "significantly understaffed". But they also said they could not find the staff with the desired qualifications.

Trends found in the research revealed the possible reasons for these shortages. Whilst many companies were looking for graduates with both professional and practical experience, very few candidates possess this combination. Of staff hired, **53%** [4] did not hold a post-graduate degree. Most European respondents said there was not a good selection of cybersecurity training programs and half of these professionals said the theoretical knowledge received in their formal education was useless when it came to performing their current job.

Companies' response to these trends were found to be increased training for their existing staff. Additionally, more than one-in-four (41%) say they are considering outsourcing the InfoSec roles to professional cybersecurity companies. This includes in-house training or paying for external courses, which are options for companies wishing to upskill their staff.

Enough budget to fight increasing cyberthreat landscape?

More than

$188bn

were allocated to security and risk management products and services worldwide.

Billions of dollars are being spent on cybersecurity by businesses worldwide. In 2023, Gartner **experts** estimate that more than $188bn were allocated to security and risk management products and services worldwide. The figure is expected by some to climb to more than $223bn by 2024.

In its IT Security Economics reports, Kaspersky has found though that enterprises' average spending on IT security fell from $13.7m in 2017 to an average of $3.75m for enterprises and $150k for SMBs in 2022. However, respondents from 2022, which examined 3,230 companies, said they were planning to increase budgets 14 percent in the following three years. But despite the increased spend, cybersecurity attacks on organizations continue to grow.

And in its latest **MDR report** [5], Kaspersky reported an average of two high-severity incidents with direct human involvement per day. Although this represents a drop compared to last year, high-severity incidents are alarming because they are carefully planned, targeted attacks aimed at inflicting a maximum amount of reputational and financial damage. Furthermore, medium, and low-severity incidents increased, due to the widespread use of previously leaked or widely available tools for automated attacks, facilitated Malware-as-a-Service. The insurgency by threat actors shows no signs of abating; in 2023, the World Economic Forum **predicted** that cybercrime could cost up to $23.84 trillion by 2027.

Gen AI and digital regulations transforming cybersecurity approaches

With

91%

of business leaders wish to learn more about Gen AI's workings and data management processes, reflecting a proactive approach towards harnessing its potential.

Gen AI is emerging as a transformative force, revolutionizing our daily work both in the way companies use it, and how people interact with it, from interactions with digital customer service chatbots in sales or support functions, to process automation, and data storage, impacting governments and businesses alike.

Beginning in 2024, a raft of upcoming digital legislation regulating everything from the cars we drive, to common cybersecurity standards for digital products and transparent supply chains in the EU, including WP 29, NIS-2, the EU Resilience Act, and the EU Supply Chain Directive. Besides the intricacies of company cybersecurity, business leaders need to also prepare themselves for upcoming legislation relating to Gen-AI. New regulations are on the books that will regulate every aspect of AI like the EU AI Act, from how AI tools are developed, how humans in the loop manage AI's machine learning training, testing and implementation, to AI data storage. Companies that aren't aware of their impact, should start allocating cybersecurity resources more effectively and prepare for it now.

Kaspersky's Gen AI Business Infiltration study [6] shows that while Gen AI is becoming mainstream in the workplace, business leaders still need to be educated on the cyber risks surrounding implementing this new technology. With an overwhelming 95% of C-suite executives acknowledging its presence in their companies, and more than half (53%) saying it seamlessly drives pivotal streamline operations. This signals a paradigm shift towards innovation and efficiency, with the 'new normal' also ushering in remote work and the 'bring your own device' (BYOD) culture.

But these innovations have introduced new perils as employees often disregard company policies and security measures. But as AI becomes integral to business – from website chatbots to data analysis – executives remain complacent, unaware they are risking a cybersecurity crisis. The Kaspersky study on Gen AI also revealed that 91% of business leaders wish to learn more about Gen AI's workings and data management processes, reflecting a proactive approach towards harnessing its potential.

However, alarmingly few have implemented safeguards, as only 59% worry about AI-related data leaks. Only 22% considered regulating its use, yet a quarter (24%) identify IT and cybersecurity as departments they are inclined to automate. To foster innovation, 26% of senior executives use Gen AI. Half aim to deploy Gen AI to automate tasks, while 44% focus on streamlining work processes, bridging the skills gaps (40%) and enhancing workforce development initiatives.

Less than a quarter (22%) have discussed AI regulations, indicating a balanced approach towards using Gen AI while managing associated risks. Just under a quarter (24%) identify IT and cybersecurity as prime candidates for automation, while showcasing confidence in Gen AI's capabilities to enhance operational efficiency and mitigate security threats.

Cybersecurity is getting more complex

There are more than

51%

of businesses state that their current tools struggle to detect and investigate these threats in a timely manner.

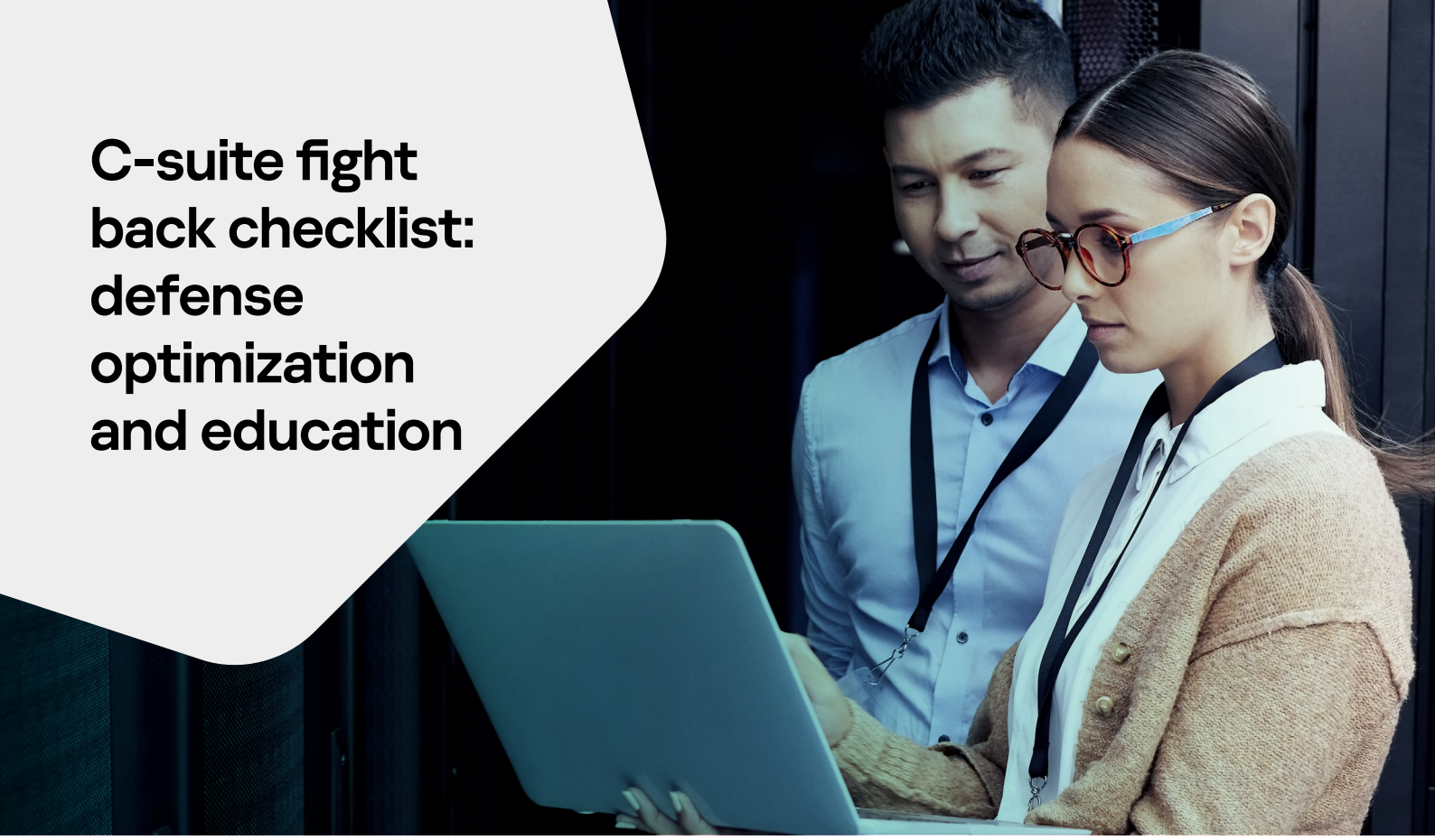
The pressing question arises: do business leaders fully grasp the magnitude of the issue, or do they find themselves trailing behind, teetering on the brink of irreparable damage to their operations and reputation?

Kaspersky's report 'SOC Modernization and the Role of XDR' [7] shows that most companies (52%) are finding security operations more difficult today – in 2024 – compared to three years ago. This problem is attributed to several factors, including the rapidly evolving threat landscape (41%), the increase in volume and complexity of security alerts (37%), gaps in security monitoring tools and processes (24%), and a shortage of cybersecurity skills or staff to handle security analytics and operations (20%).

More than half (51%) of businesses state that their current tools struggle to detect and investigate these threats in a timely manner. A significant portion (70%) also find it difficult to keep pace with the sheer volume of security alerts generated by their analytics tools.

To address these challenges, a considerable number of companies (66%) are actively consolidating their security operations tools with third party cybersecurity solutions such as Kaspersky Next, with an additional 32% planning to do so in the future.

C-suite fight back checklist: defense optimization and education



Four years ago, the Kaspersky IT Security Economics report [1] revealed a significant portion of decision-makers took months to detect data breaches. With the new advancements in technology, this snail's pace response is now in the past. However, it's evident the cybersecurity landscape continues to be increasingly challenging for businesses with new and existing threats. To address this both now and in the future, business leaders and organizations need to take the following steps:

- **Invest in educational training** courses and cybersecurity initiatives and awareness at all employer levels. Implement security awareness training to address specific security needs and minimize the risk of internal cybersecurity incidents
- **Consider utilizing threat intelligence services** such as Kaspersky Expert training to enhance InfoSec professionals' skills, third party support and threat intelligence services with state-of-the-art EDR, MDR, XDR solutions such as **Kaspersky Next**
- **Update and inform** all your staff members, including IT and InfoSec professionals, about prevailing cyber threats and proactive measures to counter them in preparation for upcoming regulations like WP 29. NIS-2, EU RCE (resilience) or EU Supply Chain Act
- **Utilize interactive simulators** to assess individuals' expertise and decision-making abilities in critical scenarios. Explore interactive education games options to observe and respond to simulated attacks alongside IT department scenarios
- **Integrate and cultivate a cybersecurity resilience culture** and empower the workforce to mitigate emerging threats effectively.

Appendix

[1] Kaspersky Security Economics Reports 2019 to 2022

Kaspersky Report 'IT Security Economics 2022'

Kaspersky Report 'IT Security Economics 2021'

Kaspersky Report 'IT Security Economics 2020'

Kaspersky Report 'IT Security Economics 2019'

See, also: https://calculator.kaspersky.com/report

[2] Kaspersky Report 'Separated by a common language', 2023: https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky-Speaks-your-Language-1122.pdf

[3] Kaspersky Report 'Redefining the human factor in Cybersecurity' 2023: https://media.kasperskydaily.com/wp-content/uploads/sites/92/2023/11/22070742/KasperskyHumanFactor360Report2023.pdf

[4] Kaspersky Report 'The portrait of a modern information security professional', 2024: https://www.kaspersky.com/blog/portrait-of-modern-infosec-professional-research-2024-labor-market/ and https://www.kaspersky.com/blog/portrait-of-modern-infosec-professional-research-2024-education/

[5] Kaspersky Analyst Report 'Managed Detection and Response', 2023: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2024/05/03142303/Kaspersky_MDR_Report_Eng_2023_01.pdf

[6] Kaspersky Report 'Gen AI Business Infiltration', 2023: https://media.kasperskydaily.com/wp-content/uploads/sites/86/2023/10/25123633/Report-ENG-Gen-AI-Business-Infiltration-Oct-2023-v2.2.pdf

[7] Kaspersky Report 'SOC Modernization and the Role of XDR', 2022: https://me-en.kaspersky.com/about/press-releases/2024_meet-kaspersky-next-new-flagship-product-line-for-business and https://go.kaspersky.com/xdr_report

About XDR

Extended Detection and Response or XDR involves a strategic shift from reactivity to proactivity. XDR is more a strategy rather than just a product. Is XDR just the latest tech-itch looking for a scratch, or a potential game-changer? The itches are certainly there, from the global skills shortage, overworked IT security staff, and a threat landscape that never stands still, to alert overload, disparate tools, weak threat intelligence and the expanding attack surface. IDC says XDR will be "a disruptive force, impacting sales of SIEM, EDR, SOAR, network intelligence and threat analytics platforms, as well as providers of external threat intelligence".

Source: IDC, Global Security Products Analysis: From Power Point to Power Product, Where Is XDR Right Now? 2022

XDR detects advanced threats better XDR's threat detection capabilities span endpoints, networks, and cloud environments. It uses machine learning algorithms and behavioral analytics to identify sophisticated threats, including malware, ransomware, and advanced persistent threats (APTs).

XDR automates response and remediation actions, enabling organizations to contain threats quickly and minimize any potential damage.

XDR leverages rich endpoint telemetry and behavioral analytics to provide deep insights into endpoint activities.

XDR provides real-time visibility into your organization's security posture. It collects and analyzes data from various sources, such as endpoints, servers, firewalls, and cloud platforms. With true proactive threat hunting and faster incident response security teams identify suspicious activities and potential security incidents more efficiently.

When it leverages high quality threat intelligence and a comprehensive threat intelligence database, XDR provides highly useful contextual information about threats and attackers what simplifies investigation alerts and incident handling.

Properly integrated, XDR will slot into your current infrastructure effortlessly to deliver the best results from automation, and give full visibility and awareness without having to replace third-party security solutions already in use.

Source: Kaspersky Whitepaper "Kaspersky Next XDR Expert", 2024: **https://content.kaspersky-labs.com/se/media/en/business-security/enterprise/en-kaspersky-next-xdr-expert-whitepaper-web-en.pdf**

www.kaspersky.co.uk

kaspersky

Cyberthreat news: securelist.com
IT security news: business.kaspersky.com
Business leaders magazine: kaspersky.com/securefutures
Enterprise cybersecurity: kaspersky.com/enterprise