Cyber defense & AI: Are you ready to protect your organization?

kaspersky bring on the future

Cyber defense & AI: Are you ready to protect your organization?

AI is disrupting security strategies, creating heightened risks alongside new opportunities to build more adaptive, effective protection – leaving cybersecurity professionals increasingly concerned.

KEY FINDINGS

46%

of respondents believe that the majority of cyberattacks experienced by their organizations in the last 12 months used AI technologies in some way.

59%

have implemented measures to ensure greater visibility of all devices, networks, and access points to spot anomalies and attacks more quickly.

50%

state that they need more qualified Information Security staff, but 39% are unable to find the right candidate.

94%

agree that the implementation of cybersecurity solutions with AI capabilities as a preventative and proactive measure is absolutely necessary.

At any time when the evolution of a new technology picks up speed, it becomes harder to be certain of the right decisions in anticipation of the changes to come. Where these changes can result in significant and tangible risks, the pressure to be one step ahead grows exponentially. Although AI has long played a role in detecting and alleviating cyberthreats, there is a distinct impression of growing nervousness among those in charge of network, system, and Information Security.

A recent global study[1] shows that nearly three quarters of those responsible for their organization's cybersecurity are seriously concerned about the risk posed by cyberattacks, which have been amplified by increasingly capable AI tools. Those attacks are now larger in scale and unpredictability because of AI, and a larger number of systems can be hit, causing greater losses. In response, Information Security professionals are looking for new ways to integrate more AI into their cyber defenses as quickly as possible.

About half of the organizations in the study report using specific AI-enabled tools and capabilities already. Almost all of those who do not have them in place now are actively working on adding new AI technologies to their arsenal.

Although recruiting qualified Information Security staff remains a top priority for protection against increasingly sophisticated attacks, the internal development of staff capabilities, the integration of software with new AI features, and improving visibility and introspection across different infrastructure layers and functions are not far behind.

Yet it is also clear that this plan of action is more an expression of concern than one of growing confidence in an effective set of protective tools and measures. Faced with increasingly intelligent, multi-faceted and effective attacks, cybersecurity leaders are nervous about the disruption and damage caused by cybercriminals that use AI to considerably increase their effectiveness.

The number of cyberattacks has increased by nearly half in the past 12 months, and among those who experienced attacks, almost half believe that most of these attacks involved AI. They report a need for external expertise, training, and support to adapt to a constantly shifting range of hazards, particularly in threat detection and elimination.

[1] Kaspersky commissioned Arlington Research to conduct a global study amongst Information Security professionals at all levels of seniority to understand their views on recent cybersecurity developments and the impact of AI on their cybersecurity strategy. Arlington interviewed 1,415 respondents who have cybersecurity responsibilities in companies with 100+ employees in the following regions: Europe (n450), Latin America (n340), APAC (n305), META (n180), and CIS (n140), covering key industries: Financial Services, Telecommunications, Information technology, Retail, Manufacturing, Critical Infrastructure & Energy, and Transport & Logistics. Fieldwork dates: 25th September to 10th October 2024.

CHAPTER 1:
CYBER DEFENSE & SECURITY NOW

Cybersecurity is a strategic issue, but internal confidence in protection is patchy

Concern over the risk posed by cyberattacks is notably top-heavy. Those dedicated to Information Security (100% of their time) demonstrate a significantly higher level of concern. For this group, 41% say this poses a very high-level risk for their organization, while only 17% of other IT professionals worry that much.

Larger businesses (Enterprise = 1,000+ employees) are significantly more likely to employ specialists who spend 100% of their time on cybersecurity (23% v 18% SMBs)

Those in the most senior roles are significantly more likely to spend 100% of their time on cybersecurity (CIO / CISO 27% v 16% IT team leaders / 15% IT professionals)

However, confidence in the measures taken by their organizations to safeguard data, systems and networks against attacks is significantly lower amongst IT professionals who spend less time working directly on Information Security. Current protection levels are seen as insufficient by 51% of these professionals, compared to 12% of those dedicated to Information Security full time.

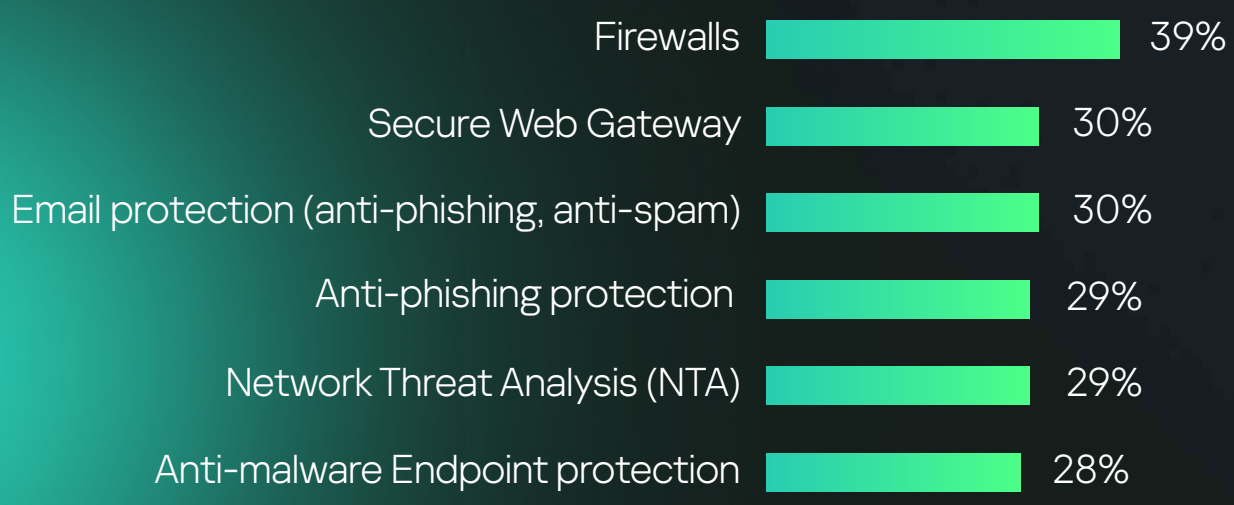
One in five sees considerable gaps in existing cyber-protection

Although current levels of protection are globally judged to be excellent by one third of respondents (34% say they have comprehensive measures in place), as many as one in five (21%) point to considerable gaps in the system, even describing the level of protection they now have against cyberthreats as 'poor'.

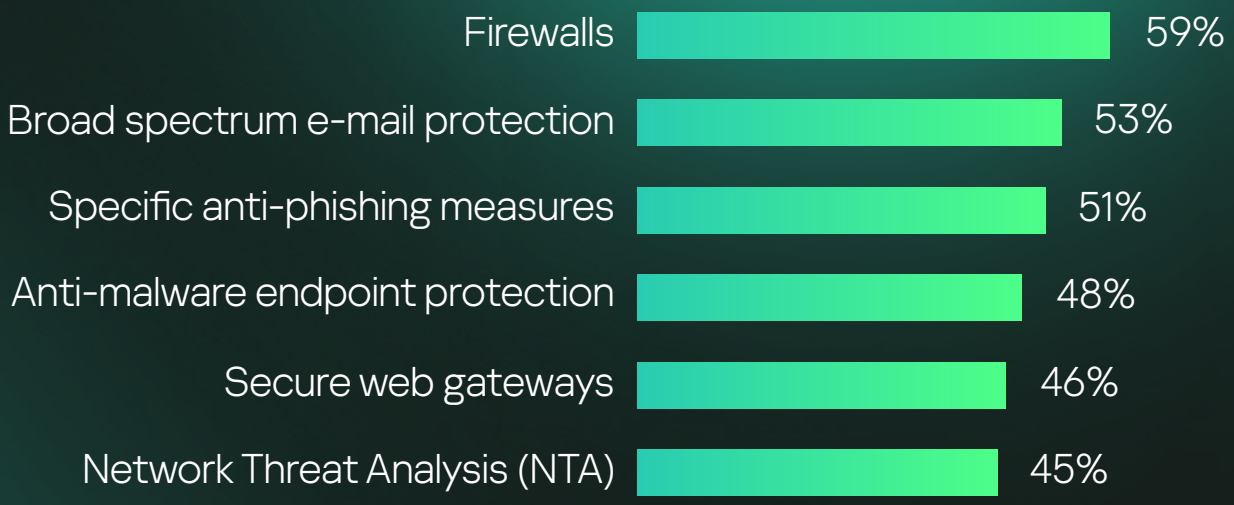
Companies of all sizes in LatAm, META and APAC are significantly more concerned than those in the Europe or in CIS regions.

A third of retailers is seriously concerned about the current risk posed by cyberattacks (33% v 24% globally), significantly more than in any other sector.

Whether their companies currently use them or not, the measures regarded as most important to protect their organization's networks, systems and information effectively from attacks include:



These priorities are largely mirrored by the most commonly used forms of protection, namely



Third party providers manage a considerable proportion of these, especially Secure Web Gateways (49%), Firewalls (48%), general Email protection (47%), Anti-phishing measures (45%), NTA (46%) and Anti-malware Endpoint protection (43%).

Only 13% use no external support for managing their cyber-protection toolset.

The future looks challenging

Looking ahead to the next two years, slightly fewer claim that their organizations currently have complete protection in place (29%). However, overall confidence remains steady, with four in five believing their organizations are future-proofed against cyberattacks during this time period.

Overall, one quarter (26%) expect the level of risk posed by cyberattacks to increase significantly over the next two years.

And the challenge of building effective cybersecurity strategies is growing all the time: The number of cyberattacks experienced by organizations in the last 12 months is reported to have increased by nearly half. Significant growth was noted by 15% and one third (33%) cited some increase in attack volume. Only 9% mentioned a reduction.

The most ubiquitous threat came from phishing attacks with 49% reporting this type of attack. Covert malware installation affected a third of organizations (named by 34%), 29% stated ransomware, and one in five mentioned BEC, SQL injection and DNS tunneling attacks (all indicated by 20%).

Phishing attacks are significantly more common in the Europe (56% report this type of attack), whilst ransomware is most frequently reported in APAC (38%). In comparison, DDoS attacks occur far more often in CIS (46% identify this type of attack).

Growing concern is driven by expanding attacks

Of those who stated cyberattacks pose a high level of risk to their organization, 70% also saw a notable increase in the number of incursions in the last 12 months.

Considering likely developments over the next 12 months, those who have already seen a marked recent increase are much more sensitive to the ever-growing volume of attacks.

They are particularly concerned about increases in ransomware attacks (41% v 33% with stable numbers of attacks), zero-day vulnerability exploitation (35% v 30%), DDoS attacks (30% v 24%), SQL injection (29% v 22%), and MitM attacks (23% v 15%).

CHAPTER 2:
AI & CYBERSECURITY NOW

AI amplifies risks and highlights recruitment challenges

The role of AI in ramping up security for systems, networks and information is a significant issue for corporate cybersecurity. Only 3% of global organizations have not yet considered the use of AI-powered cybersecurity, and only 0.5% do not see any need for this type of tool.

Nearly half (46%) believe that the majority of the cyberattacks experienced by their organizations in the last 12 months used AI technologies in some way.

While all the leading cybersecurity vendors are long using elements of AI under the hood of their solutions that do not require any operator involvement, the general notion of 'AI-enabled cybersecurity solutions' mostly implies more modern aspects allowing the operators make better sense of IT security-related context, automate the more tedious workflow elements, etc.

Interestingly, the more time IT specialists spend on Information Security, the more likely they are to believe AI played a role in cyberattacks on their organization. 46% of those with Information Security as a regular responsibility think AI was involved. This rises to 63% of those dedicated to Information Security full time.

IT decision makers in CIS are least likely to assume that cyberattacks on their organizations involved the use of AI (only 34% in CIS say that the majority of the attacks involved AI v. 46% globally). Those in META are most likely to say so (53%).

Half of organizations globally believe that they need more qualified Information Security staff, but 39% are unable to find the right candidate.

When it comes to dealing effectively with cyberattacks involving AI, highly qualified staff is seen as the most important aspect for almost two thirds of respondents (60%). Aligned with this is regular training to build up relevant internal expertise (58%). More than one third, 39% also name the use of third-party solutions (security products) as a key part of their Information Security strategy.

Half (50%) say that highly qualified staff is in place, but one in ten (10%) claim that this resource is not available to them. A further 12% say that their IT team is not large enough to handle cyberattacks involving AI technology effectively. Although the majority claim that the most important resources they need are in place or easily available to them, many are clearly troubled by the prospect of having to cope with a growing threat to their cybersecurity.

Specific steps taken by organizations to protect their networks, systems and information focus particularly on transparency and skills.

Almost two thirds (59%) have implemented measures to ensure greater visibility of all devices, networks, and access points to spot anomalies and attacks more quickly. The same number has improved breach detection, and utilizes external support for their internal cybersecurity experts to keep them up to speed with constantly changing threat scenarios.

Underpinning external support is specific training on recognizing and avoiding AI threats for employees (in place at 56% of organizations), as is external expertise to adapt to an evolving threat landscape (54%), and the use of professional services from a cybersecurity provider to assess risks and advise on countering AI threats (53%).

With IT teams being too small or insufficiently qualified, the recruitment of more Information Security professionals to the internal team is firmly on the list of actions to implement as soon as possible (44%).

Key barriers to achieving the goals for an effective cybersecurity set-up again point to the lack of highly qualified staff and deep expertise within organizations: 44% quote the lack of AI related cybersecurity training for employees as an obstacle, and the same number (44%) say that the complexity of cybersecurity infrastructure management stands in the way of fully realizing their Information Security strategy.

Implementing AI as an integral part of powering effective cybersecurity measures is fast becoming a top priority

The lack of AI-powered cybersecurity tools is an issue for 43%, while a lack of information from external experts on the current AI-related threat landscape is a hindrance for 41%, as is the lack of Information Security professionals available for hire (39%).

In line with this, **only 27% already use AI-based tools**, but as many as 46% are implementing this type of solution right now and a further 23% are actively engaged in reaching the implementation stage.

There is a broad spectrum of options for integrating AI into corporate cybersecurity, and these are being utilized by organizations across the board:

Those who are actively planning for or currently implementing AI-enabled cybersecurity, as well as those who have this in place already use these solutions to automatically **adapt and improve AI-based threat detection and response** through ML (49% have this in place, 46% are actively implementing) and to **translate natural language into complex queries for threat hunting** (48% use this already, 49% are implementing).

AI security solutions are already being used by 46% of respondents to **manage system and network vulnerabilities**, with 50% actively working on it; 47% use AI security solutions to **respond to and neutralize detected threats automatically**, and as many as 51% are actively working on putting these in place. Additionally, 47% use it to **mediate the (potential) damage caused by an attack**, while 48% are in the process of planning and implementing this.

The small number of organizations that have not yet considered deploying AI to strengthen their cybersecurity made this decision because they believe it would be too expensive (29%), or because the idea was rejected by senior management (29%). Other reasons include the fear that it would cause too much disruption (21%) and the inability to access these types of tools (also 21%).

The anticipated consequences of failing to adapt cybersecurity measures to AI-powered cyberattacks are severe

Although general concern over the risk posed by cyberattacks remains serious across the board, the growing involvement of AI in these attacks is seen by many decision-makers as an even greater danger to their organizations.

More than half point to an AI-exacerbated risk of confidential data breaches (58%), a decline in customer trust (52%), financial losses through a drop in the value of stocks and shares, and losing orders and customer accounts (52%). Almost half (47%) would also worry about reputational damage to their organization.

Concern reaches a critical point, as 95% agree that managing cybersecurity will require significantly more resources and more expertise to cope with an increasingly complex set of risks to the safety of systems, networks and information.

CHAPTER 3:
AI & CYBERSECURITY IN THE FUTURE

Information Security professionals foresee AI enabling increasingly dangerous and damaging attacks

The vast majority of those questioned (88%) expect attacks involving AI to increase.

Social engineering attacks are predicted to increase more than any other type, made more effective through comprehensive data analysis and the increasingly sophisticated removal of red flags that are used to identify and protect against phishing and similar user-focused attacks.

Almost half (48%) believe that AI usage by cybercriminals will drive an increase in the volume of cyberattacks, give malicious actors more effective ways to bypass access restrictions and security clearance requirements, and make it much easier to find gaps in the cyber-protection set-up of organizations

Almost as many (46%) expect that more units of their systems and networks will be attacked at the same time, making it harder to protect them. 45% believe that attacks using AI will cause more damage than ever before because broad-range attacks are made easier by AI (also 45%).

With AI becoming a more prevalent enabler for cybercriminals, half (50%) expect significant growth in the number of phishing attacks, a notable increase in covert malware being installed on their systems is foreseen by 39%, and 37% expect more of ransomware attacks. Strong increases in Zero-Day vulnerability exploitation attacks are expected by 33%.

As AI offers enhanced capabilities, 87% agree that there will be more effective social engineering attacks, enabled by AI-assisted OSINT and comprehensive data analysis. 83% predict red flag removal will be facilitated by AI, and 88% believe that attacks will be increasingly camouflaged, making it much harder to detect them.

Not only will these attacks be more targeted and harder to detect, but there is also great concern that AI will enable coordinated broadside offensives against multiple entry points, exploiting vulnerabilities that are very difficult for organizations to eliminate.

A significant percentage (89%) agree that there will be an increase in multi-layered attacks using IoT devices, external access channels and smart devices as entryways into organizations' systems. Furthermore, 85% anticipate that the discovery of zero-day vulnerabilities and their exploitation by malicious actors will also increase greatly.

A notable 94% agree that the implementation of cybersecurity solutions with AI capabilities as a preventative and proactive measure is absolutely necessary. Additionally, 86% are convinced that modern cyberattacks (including AI-amplified ones) can only be overpowered by these AI-powered cybersecurity solutions.

CONCLUSIONS

Most Information Security decision-makers are experiencing increased pressure from the evolving threat landscape. While many feel that their organizations are future-proofed against cyberthreats over the next two years, they acknowledge the need to bolster their defenses against the growing intensity of attacks.

Seeing the use of AI-powered tools by attackers as a key factor driving this surge, and the shortage of skilled Information Security specialists as an ongoing block to coping with the situation, they look forward to adopting new AI-enabled solutions to give their defenses a substantial boost.

Although Kaspersky's experts and the Information Security community have not observed any significant advancements in attacker tactics, techniques and procedures, AI tools can make cybercriminal operations more effective and efficient, allowing for more frequent, well-prepared attacks and lowering the entry threshold for less skilled attackers. As a result, the demand for AI-empowered tools to help security teams better interpret data and ease pressure on security officers is growing.

However, companies should be cautious about «breakthrough» AI solutions. While AI is advancing, it has not made any quantum leaps that would radically improve offensive or defensive capabilities yet. Still, monitoring ongoing developments in AI is clearly important, as meaningful progress is undeniable, and further advancements are possible.

For now, organizations should prioritize a reliable, resilient security stack that includes effective threat blocking, attack-surface reduction and comprehensive infrastructure visibility, managed by skilled Information Security professionals. Organizations without in-house expertise should consider managed protection services to bridge the skills gap.

kaspersky.com