



**Kaspersky Human
Factor 360° report 2023**

Redefining the Human Factor in Cybersecurity

Adopting a Human Factor 360° model to assess
the global cybersecurity landscape

kaspersky bring on
the future

Introduction

The concept of the 'human factor' in cybersecurity needs to be looked at and understood with new eyes. To this end, Kaspersky proposes a 360° Human Factor model where all relevant staff are included in the cybersecurity conversation.

In the past two years alone, more than three-quarters (77%) of companies experienced at least one cybersecurity breach, with many enduring up to six in that period. What companies attribute these incidents to differ, however – and so does their response. For some, investing in new automation tools is a priority. For others, hiring new IT staff is the way forward. Others are looking to outsource their security.

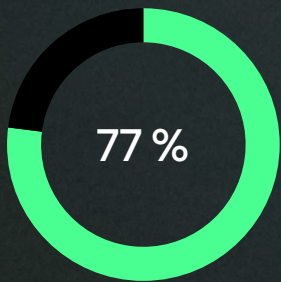
Education is also part of this strategic mix, but perhaps not to the extent it should be, especially considering that 64% of all cyber incidents in the past two years were caused by human error.

To get a better understanding of the dynamic of threat versus response, we conducted our 2023 Human Factor survey, to give us a clearer view of the cybersecurity ecosystem through the human lens. This included non-IT employees, IT staff and decision-makers operating within an organization. They, in turn, discussed and analyzed their relationships with vendors and outsource partners. As a result, we have gained a 360-degree view of the 'human factor'.

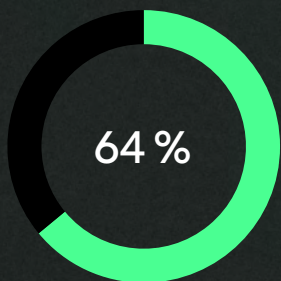
In this report, we have focused on how these various demographics combine to provide an overall threat surface that organizations across numerous sectors and regions are facing. We have looked at the influence of each group, and at how organizations are currently perceiving and handling the threat landscape. We have analyzed the current levels of investment being injected into cybersecurity, and where decision-makers feel greater improvements are needed in the future – are they investing in people, or is automation seen as the best way to sidestep both human frailty and human threat?

We have sought to show the level of security that is needed to ensure resilience and preparedness, despite human involvement from all sides, in all ways, at all times.

In the past two years alone, more than three-quarters (77%) of companies experienced at least one cybersecurity breach



64% of all cyber incidents in the past two years were caused by human error



Methodology

Arlington Research conducted 1,260 interviews with IT & IT security engineers. The survey covered 19 countries: Brazil, Chile, China, Colombia, France, Germany, India, Indonesia, Japan, Kazakhstan, Mexico, Russia, Saudi Arabia, South Africa, Spain, Turkey, UAE, UK and USA. All respondents were at Manager+ level working for SMEs with 100+ employees, or Enterprises with more than 1,000 employees.



Key findings

77%

of companies experienced at least one cyber incident in the past two years.

75%

report that the cybersecurity incidents experienced by their company during this period were serious.

26%

of all cyber incidents in the past two years were caused by employees' intentional information security policies violations. These internal actions reflect almost the same level of danger to business security as hacking, which 30% of respondents reported.

14%

of cyber incidents are due to senior IT security staff errors, compounded by a further 15% of errors being caused by other IT staff.

18%

of respondents report that a skills shortage in cybersecurity is the cause of incidents in their companies. This is reflected in an overall concern where 75% of companies regard the shortage of skilled staff as a serious problem.

41%

of companies feel they have gaps in their cybersecurity infrastructures plan to increase investments in this area moving forward.

21%

of respondents say they do not have the budget to take adequate cybersecurity measures, while 28% believe they have what they need to stay ahead of potential threats.

Industry breakdown



Financial Services: vulnerable to information security policies violations

Compared to a global average of just 8%, the extent of incidents caused by information security policies violations by non-IT employees sits at an alarming 22%. This is compounded by 34% reporting that intentionally malicious behavior is a significantly more common issue in financial services.



Telecommunications: a sector with much to learn

More than one-third (34%) of companies in the telecommunications sector have experienced more than four cyber breaches in the past two years. This is higher than in any other industry – an industry where 66% of employees are under the age of 35, and who you would expect to be more tech-savvy.



Information Technology: IT staff lose sight of their non-IT colleagues

IT is another industry with 54% of employees under the age of 35. However, they experience more issues with human error among non-IT staff than any other industry (23%). The main concern here is that, even in an IT setting, the visibility of non-IT workers can be lost or ignored. This serves as a reminder that cyber capability and understanding is a company-wide concern.



Retail: a sector under serious threat, heads to the cloud

While retail didn't experience the most frequent extent of breaches over the past two years, it did suffer the most serious outcomes. More than half (52%) confirmed the incidents they experienced were either very serious, or extremely serious. A priority for this sector, as a result, is to implement SaaS cloud solutions (37%, the highest of any industry).



Manufacturing: an investment drive to close consistent gaps

Manufacturing companies (37%), more than any other sector, reported that they have endured between two and three cyber incidents over the past two years. This consistent and troubling statistic explains why it is also one of the leading sectors targeting investments to close cybersecurity gaps (50%).



Critical infrastructure: skills shortages and information security policies violations

The impact of skills shortages came through most prominently in the industrial realms of critical infrastructure, energy and oil & gas (24%). Often criticized in the past for its lack of innovation, it seems that cybersecurity skills shortages are still an issue – an issue compounded by 33% (a sector high) of workers reporting incidents of intentional information security policies violations among non-IT staff.



Transport & Logistics: accidents happen all too frequently

Unintentional human error was a common risk on a global scale, even surpassing the threat of hacking. However, it was most severe in transport & logistics, where 49% reported the link between accidental human error from both inside and outside the IT department, and a cybersecurity breach in the past two years. It is no surprise that the sector is highly motivated to invest in closing existing cybersecurity gaps (51%).

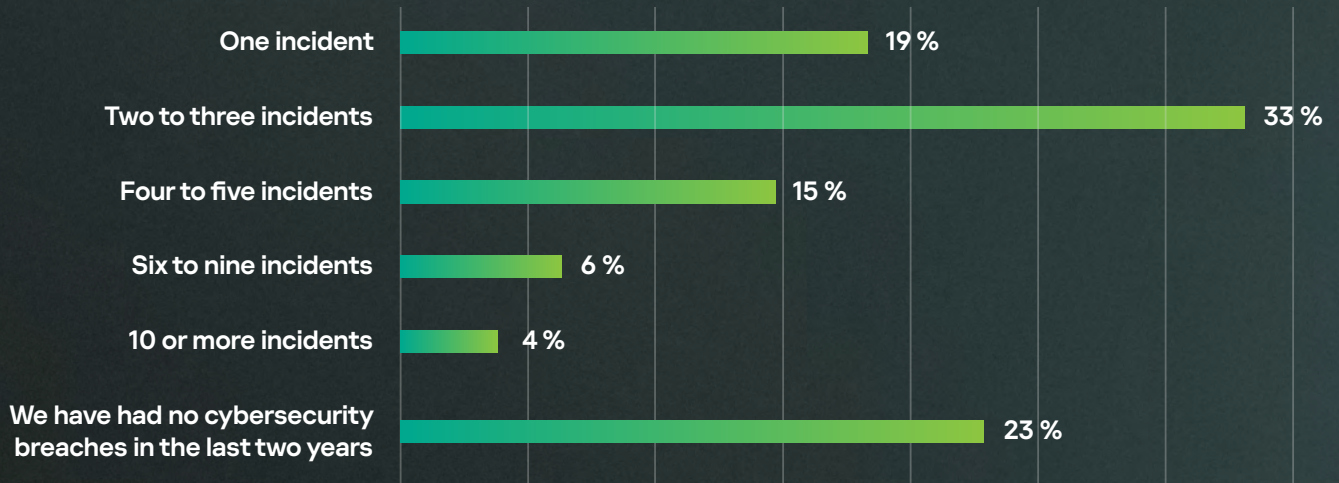


Setting the cybersecurity scene

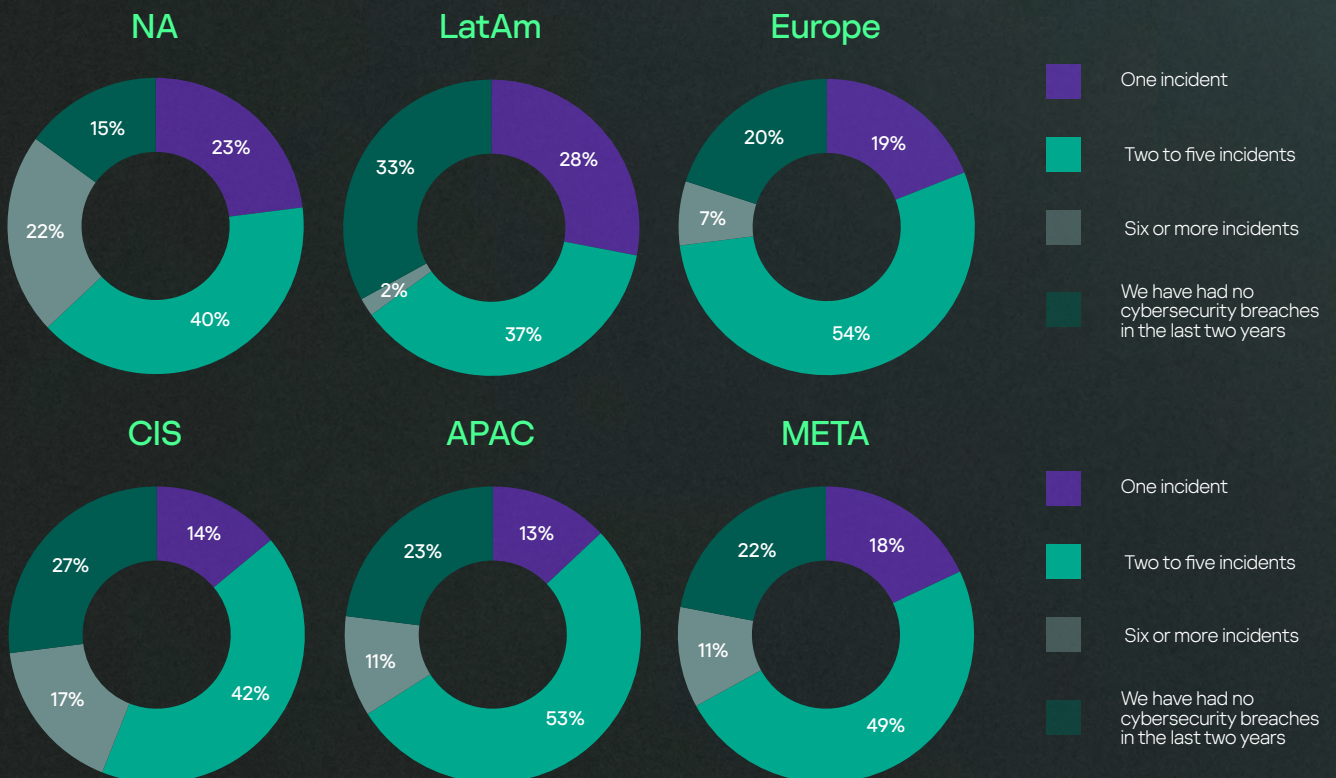
Over the past two years, most companies around the world experienced one or more cyber incidents

Over the past two years, most companies around the world experienced one or more cyber incidents. As many as 77% confirmed that despite growing calls for greater cyber hygiene and more resilient security processes and technologies, breaches are still very common.

Has your company experienced any breaches of cybersecurity within the last two years? In the last two years, we have had...



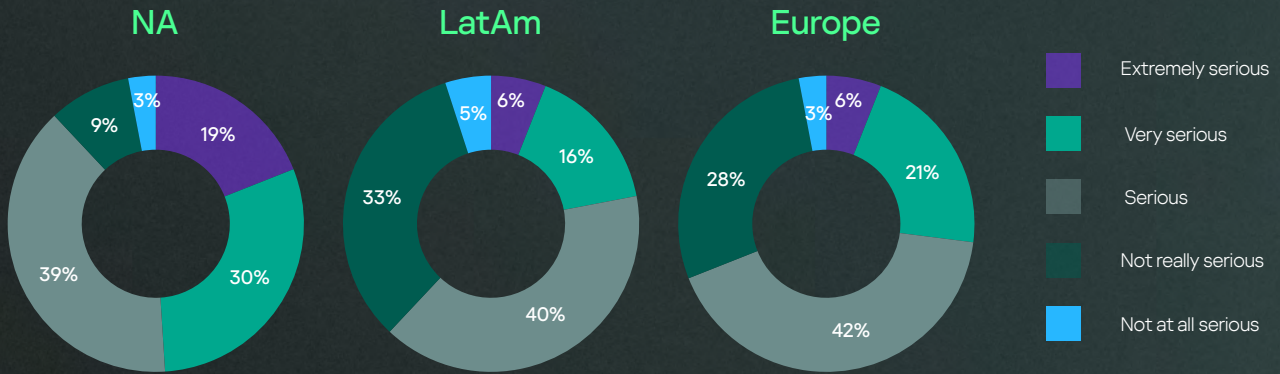
In some regions, this statistic is even more concerning. In North America for example, only 15% have not experienced any type of cyber incident over the past 24 months. Almost one-quarter (22%) endured more than six incidents in the past two years alone. The CIS region also reported a higher likelihood of numerous incidents (17% with more than six breaches), suggesting that those who are initially vulnerable struggle to find a suitable defense or solution quickly. APAC and META regions report similar numbers, each experiencing 11% of incidents over the past two years there.



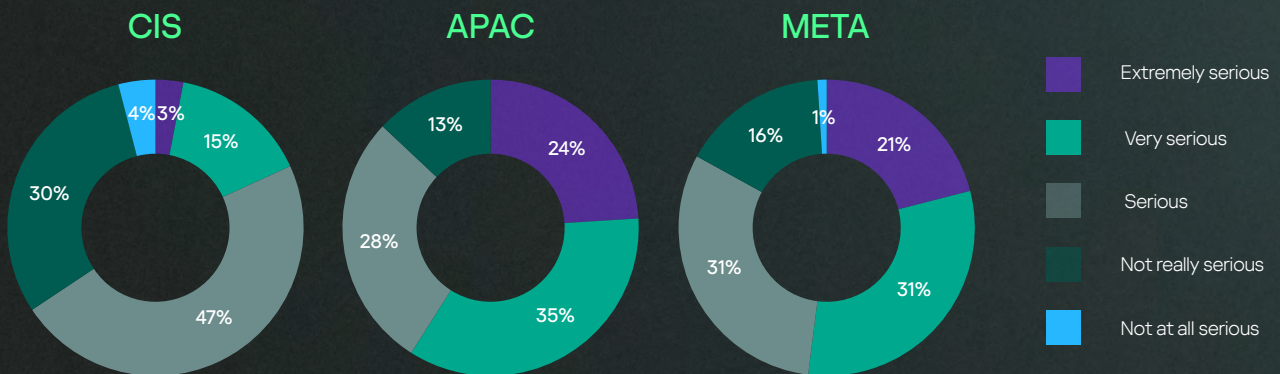
When asked about the level of severity, 75% of respondents globally confirmed that the breaches experienced by their company were 'serious' or worse

The seriousness of these cyber incidents also varies. When asked about the level of severity, 75% of respondents globally confirmed that the breaches experienced by their company were 'serious' or worse. Within this group, one-quarter went as far as saying the incident was 'very serious' and 13% confirmed it was 'extremely serious'.

'Seriousness' in this context related to confidential data being leaked, with negative impacts on reputation, customer trust and on the business's financial standing. It is worrying, therefore, that in North America once again, 88% experienced a serious (or worse) incident creating those negative outcomes, in the past two years.



While the global picture shows that incidents are still incredibly frequent, and often serious, the extent of concern differs from region to region. In Latin America (38%), CIS (35%) and Europe (31%), the extent of non-serious incidents is more reassuring. However, APAC (87%) and META (83%) show figures much higher than the global average.



The overall picture of cybersecurity over the past two years is one of regular and often serious breaches

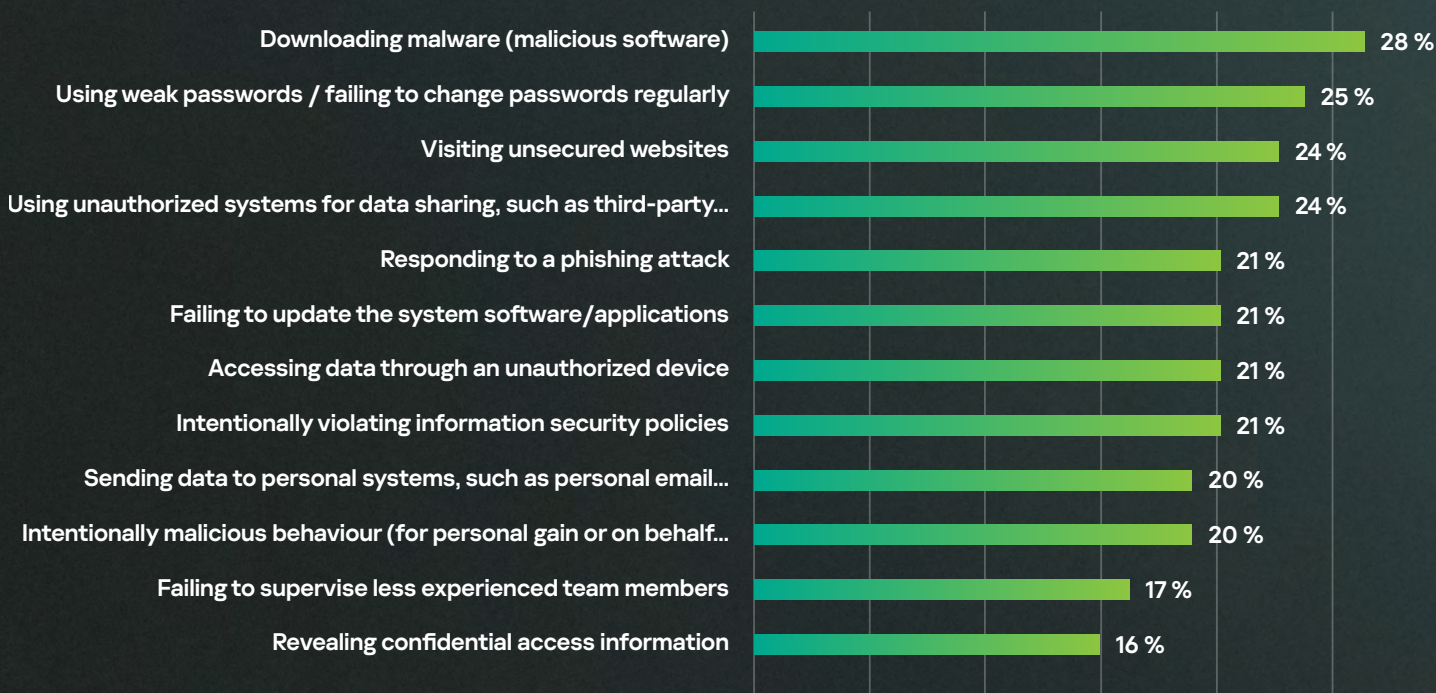
The overall picture of cybersecurity over the past two years is one of regular and often serious breaches. This situation is most pronounced in North America, APAC and META, but no other region has been fully immune. For example, despite the lowest figure in Europe among all the regions, the UK and Spain report high severity of cyber incidents they've experienced. 88% of cyber breaches in the UK and 70% in Spain were claimed to be serious to different extent. At the same time, LatAm's Chile rates 90% of cyber incidents as serious and very serious. All corners of the world report a majority who have not only experienced incidents, but serious ones. It is now time to find out where these organizations believe the gaps in their defenses are.

Non-IT: the human - error - factor

Like all staff members, especially in the modern, flexible working climate, non-IT professionals use different devices. This might involve a combination of a desktop in the workplace and a laptop when working remotely and includes access credentials from these devices and sharing confidential data within the company. As non-IT professionals, there is an expectation that these staff would be more likely to make errors that lead to cyber incidents. But are they really the most common source of danger for cybersecurity within an organization?

Indeed, at first glance, it is accidental human error (38%) that accounted for more incidents than any other factor over the past two years. However, when analyzing the full rundown of error types, the human factor of breaches appears in different ways. Most common is the download of malware (28%), although almost every possible cause received more than 20% of selections. Using weak passwords or not changing passwords often enough (25%), visiting unsecured websites (24%) and using unauthorized systems to share data (24%) are among the next most common 'human errors'.

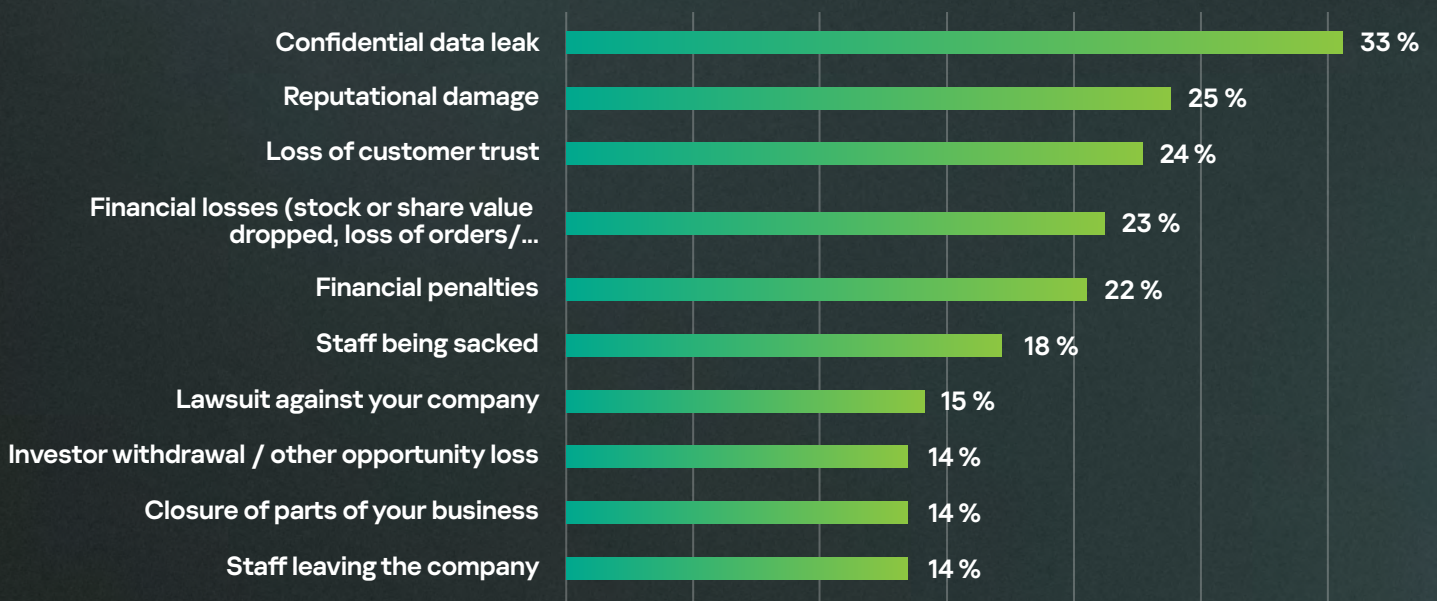
What did employees do to cause the incident?



The complete list of causes behind cyber incidents further highlights the volume of factors an employee – especially one outside of the IT function – must consider reducing the likelihood of a mistake. For example, the deployment of shadow IT (11%) is a growing concern among organizations as employees spend more and more time outside the office and must be trusted with remote devices (both work and personal).

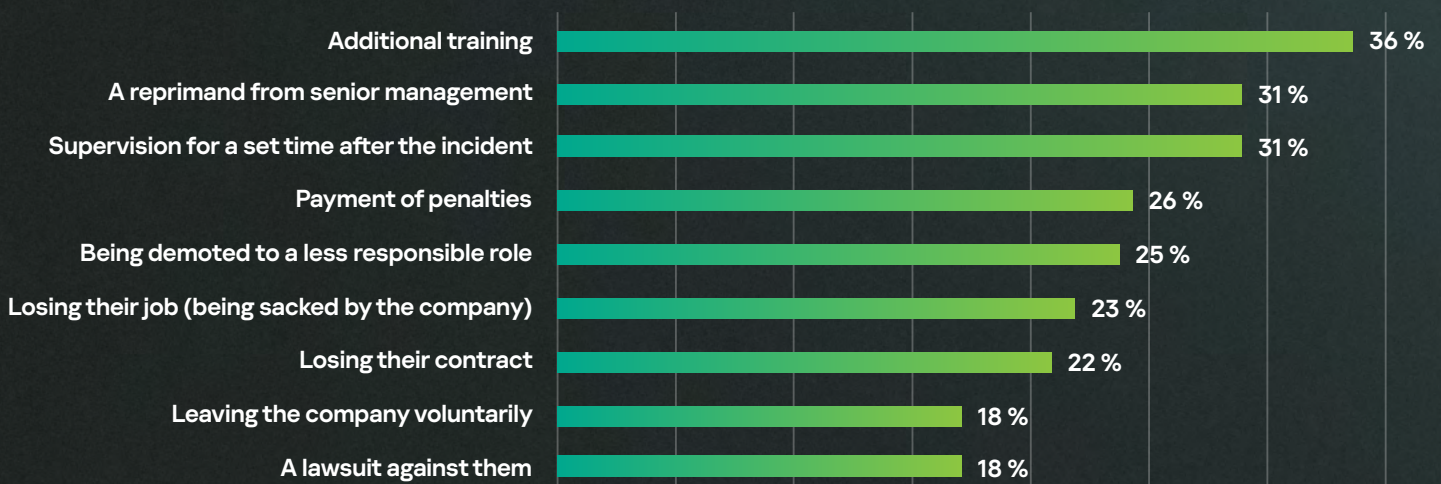
It should be noted that these causes are more likely to be accidental than deliberate. Only 8% of incidents were caused by an information security policies violation by non-IT employee. However, the financial services sector is an anomaly in this regard. Information security policies violations by non-IT staff in this industry are responsible for 22% of cyber incidents, while 34% reported intentionally malicious behavior by both IT and non-IT employees as a significantly more common issue.

What were the consequences of an incident for your company?



Regardless of whether it is accidental human error or an information security policies violation, the consequences can be severe. In one-third of cases, a confidential data leak occurred, implicating employees but also customers who are unlikely to be loyal to a business from then on. Indeed, 25% took a reputational hit following the breach, and 24% confirmed a loss of customer trust. Financial penalties (22%) were also common. And, considering all the above, it is perhaps unsurprising that in 18% of cases, the breach led to a staff member being sacked.

What were the consequences of an incident for the employee?



When looking through the lens of the employee, being dismissed was the outcome on 23% of occasions. A reprimand from senior management (31%), subsequent supervision (31%), payments of penalties (26%) and demotions (25%) were all relatively common. However, additional training (36%) was the most frequent 'punishment'.

IT professionals: skills shortages cause security shortfalls closer to home

The above statistics exploring the role of non-IT professionals suggest that they have a big impact on security breaches. But are they the only ones? Let's look at the other part of the human factor – IT and IT security professionals. Contrary to assumptions, the responses to this survey suggest that IT and IT security professionals are not above causing cyber incidents.

Senior IT security professionals were responsible for 14% of cyber incidents through unintentional human error over the past two years

Senior IT security professionals were responsible for 14% of cyber incidents through unintentional human error over the past two years. Other IT staff within the organization contributed to 15% of incidents, and this is before you consider deliberate violations. While they are again quite low in general terms, more than 12% of incidents are caused by information security policies violations by IT staff. In 11% of cases, such acts come from senior IT security workers.

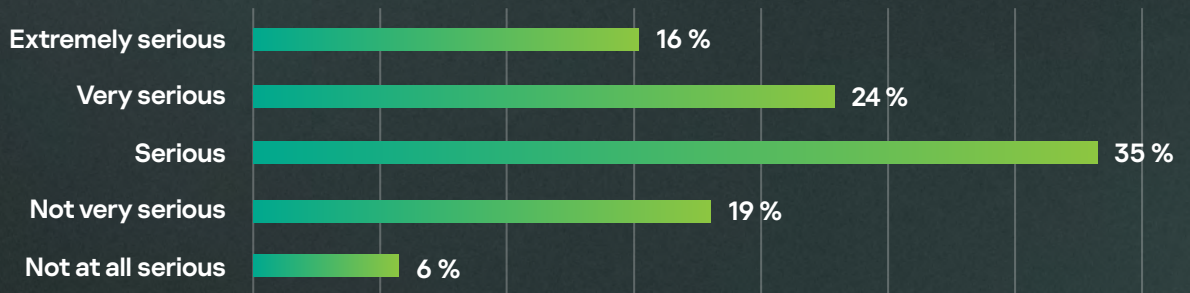
	Senior IT security professionals	Other IT staff	Non-IT workers
Unintentional human error	14%	15%	16%
Intentional information security policies violations	11%	12%	8%

Comparing the impact of IT and non-IT professionals on cybersecurity, there is very little difference, and when combining instances of both accidental and deliberate actions, IT workers are shown to be more of a risk than non-IT staff.

However, it is the statistic between them that a lot of organizations are focusing on. A skills shortage (18%) is given the same level of impact as hackers installing trojans (18%), once again emphasizing the human factor, especially within the confines of the company.

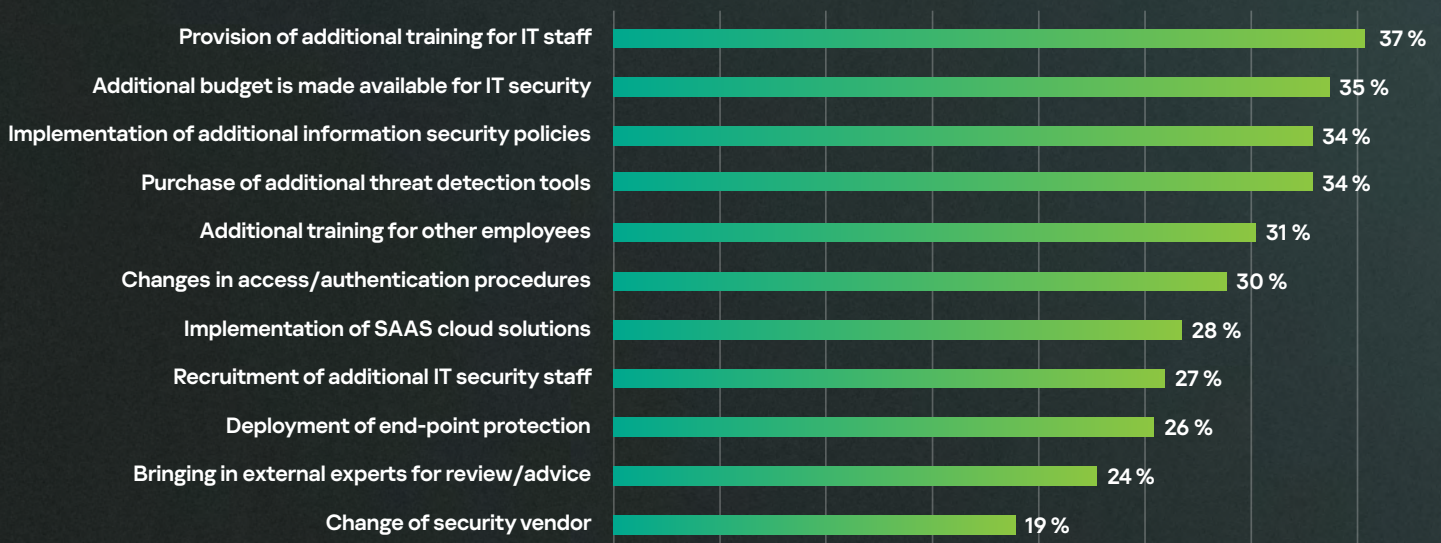


What is the impact of skilled staff shortages in cybersecurity?

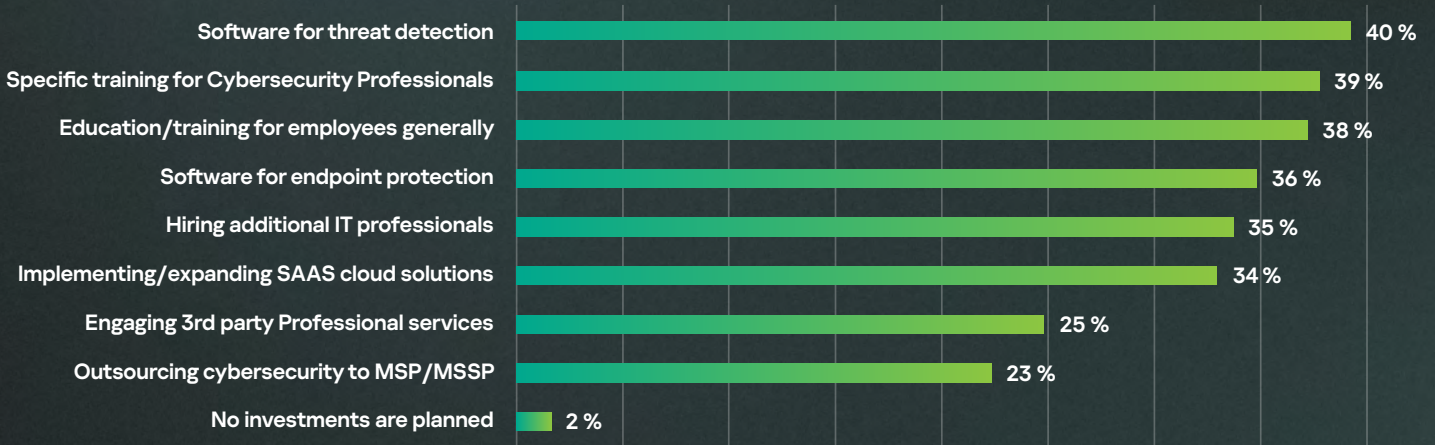


Three-quarters of organizations around the world see cybersecurity skills shortages as a serious issue, to varying degrees. Almost one-quarter (24%) say the issue is 'very serious'. In the APAC region, this number rises to 87%, while META is not far behind (85%). In both regions, almost one-quarter (APAC – 24%; META – 22%) view the issue as extremely serious.

The answer for many, as documented earlier, is additional training – a plan of action taken up by 36% of respondents following a breach. Looking to the future, the provision of additional training for IT staff is set to be a strategy for 37% of organizations – more than any other tactic to prevent future cybersecurity breaches.



However, when asked directly about investments, while hiring additional IT professionals (35%) and training for all employees (38%) were on the agenda; outsourcing (41%) outweighed both individual plans.



NET: Tools **71 %**

NET: Education **60 %**

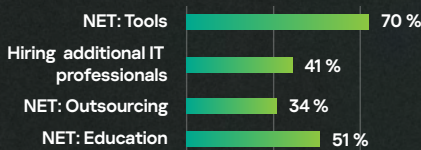
NET: Outsourcing **41 %**

Among this sample, almost one-quarter (23%) is targeting outsourcing of cybersecurity to a managed service provider (MSP) or managed security service provider (MSSP). Outsourcing is a more common strategy in APAC (57%), although this is included alongside education initiatives (71%) for a balanced plan. In all regions, the order of priorities for future investment reads:

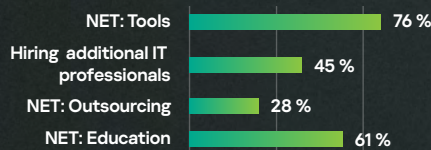


But only in Latin America does the idea of outsourcing IT functions drop below 30%, and for Europe, CIS, APAC and META regions, it is a preferable option to hiring additional IT professionals.

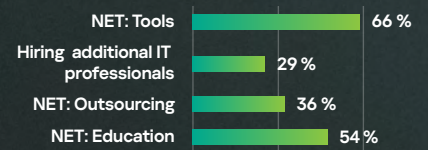
NA



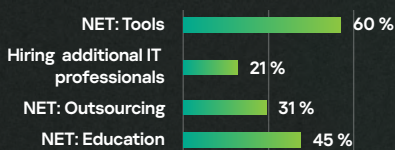
LatAm



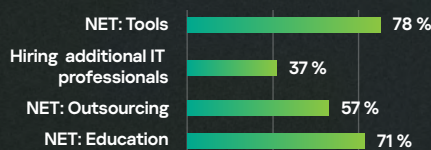
Europe



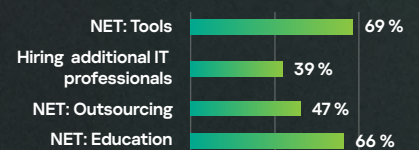
CIS



APAC



META

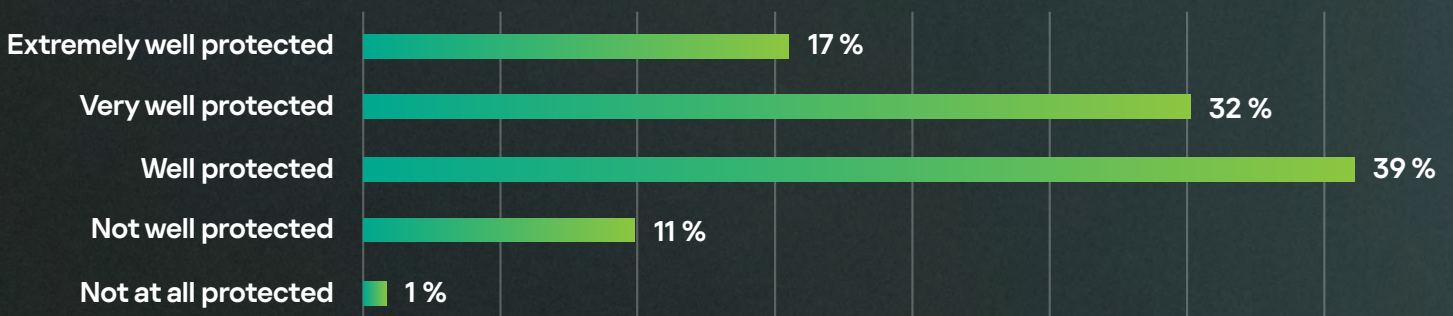


Decision time: where are the gaps and what is my budget?

Just as with IT professionals, decision-makers have not been immune from responsibility when it comes to cyber incidents over the past two years. But do they feel they are being equipped well enough?

Just as with IT professionals, decision-makers have not been immune from responsibility when it comes to cyber incidents over the past two years. But do they feel they are being equipped well enough? The decisions they have made come from a situation where 18% of respondents believe incidents were caused by a lack of necessary tools for threat detection, and 16% lack focus on threat prevention more generally. It is interesting that 15% claim that insufficient investments into cybersecurity is also a problem in their company. Are decision-makers not focusing on the right strategies, or do they not need to improve cybersecurity levels?

How well do you feel your company is protected against cybersecurity breaches?

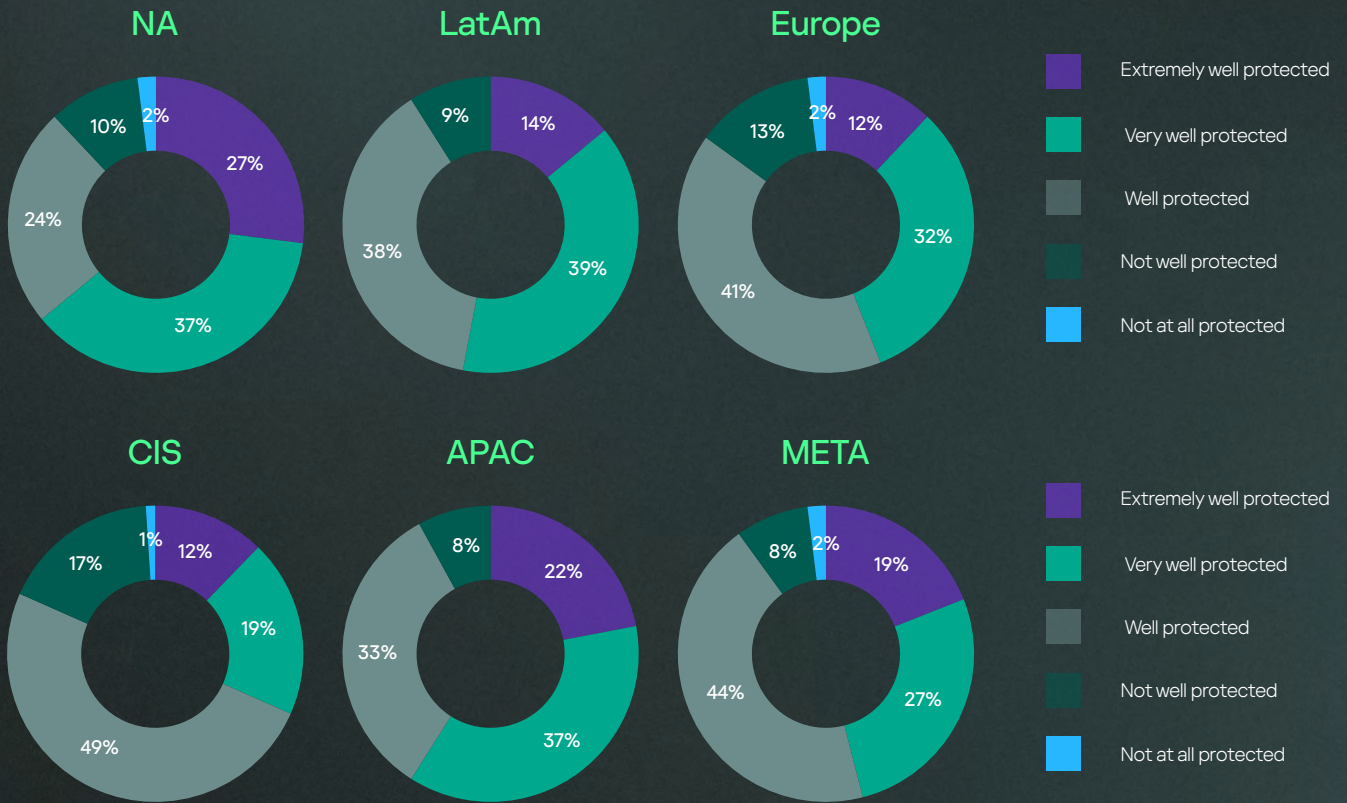


While the vast majority believe they are protected, only half (49%) say they feel 'very well protected' or better. Perhaps more concerning is that 12% don't feel well protected, or not at all protected. This group is entering a situation where they may even anticipate a daily breach or cyber incident.

The situation in CIS countries is slightly more alarming, with 19% (almost one in five) believing their organizations are not well – or not at all – protected. Europe (15%) also increases the global average in this respect.

Comparatively, North America (27%), APAC (22%) and the META (19%) all score above the global average in working for companies they believe are 'extremely well protected'. This is interesting given that each of these regions were also vocal in terms of their shortcomings. In North America especially, they reported the highest number of serious incidents over the past two years, despite believing their protection levels are high. APAC's confidence in protection levels, meanwhile, is despite citing skills shortages as a serious issue.





These kinds of conflicting statistics could illustrate the lack of clear visibility that decision-makers also have at present, where a general feeling of protection doesn't necessarily correlate with the level of incidents that are occurring.

It might also stem from perceptions of investments so far. Half believe that the budget for cybersecurity measures within their company covers simply what they need to keep up with new and potential threats.

Would you say the budget for cybersecurity measures in your company?



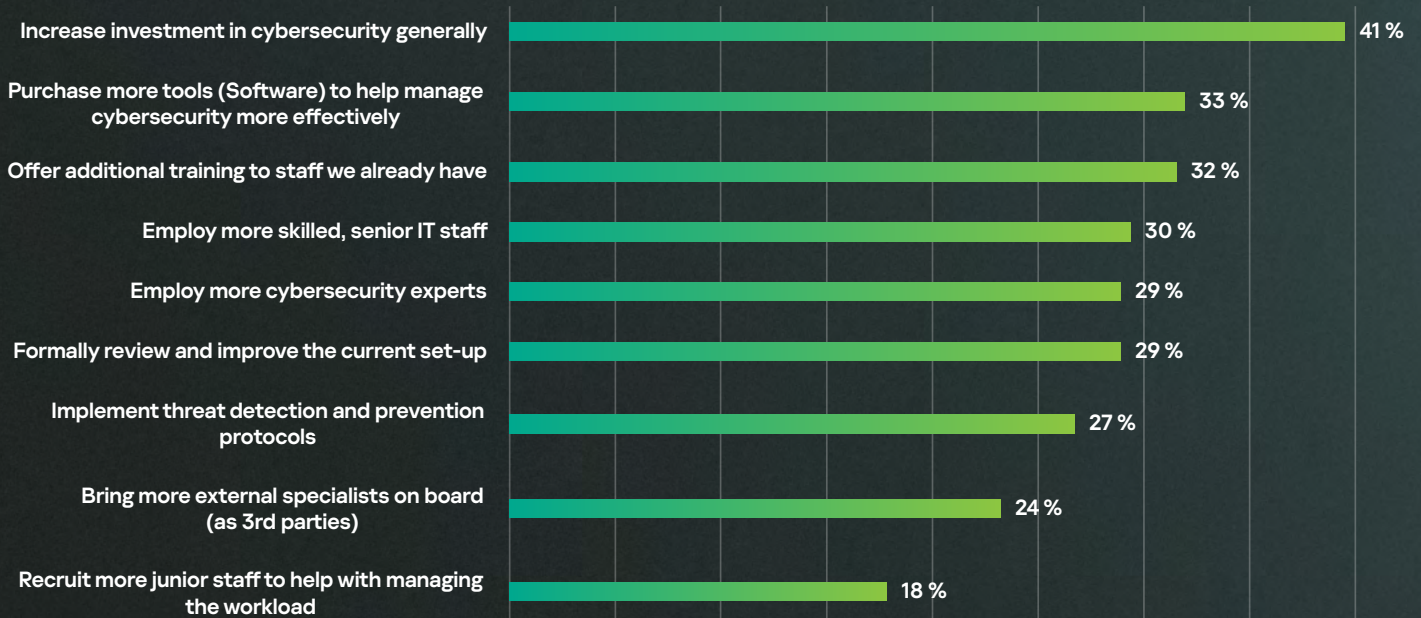
However, more than one-quarter (28%) believe they can stay ahead of the curve. This supports the idea that most believe they are at least protected for the time being, even if the extent of breaches suggests otherwise. For one in five companies (18%), the budget accessible to decision-makers falls short of what they need to keep up with new and potential threats, while for 3% there simply is no budget.

In total, tools (71%) are by far the priority for investment

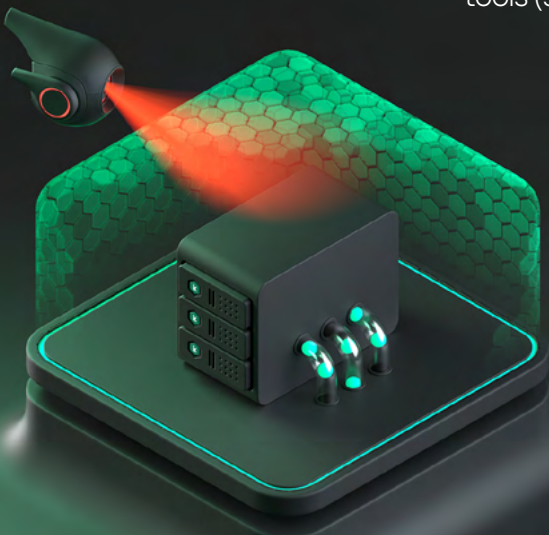
Finding a fitting solution: attention turns to tech

In line with the above responses around budget capabilities, it is important to see where companies are planning to target their investments in cybersecurity in the next 12-18 months. As discussed, education and outsourcing are high on the agenda for many, but neither outweigh the focus on new tools and technology. Software for threat detection was the most common answer at 40%, just ahead of specific training for cybersecurity professionals (39%) and education for employees generally (38%). In total, tools (71%) are by far the priority for investment, with this number rising to 76% in Latin America where outsourcing (28%) is a less-considered strategy; and in APAC (78%) where all solutions still seem to be on the table.

What do you need to close cybersecurity skill & tool gaps?

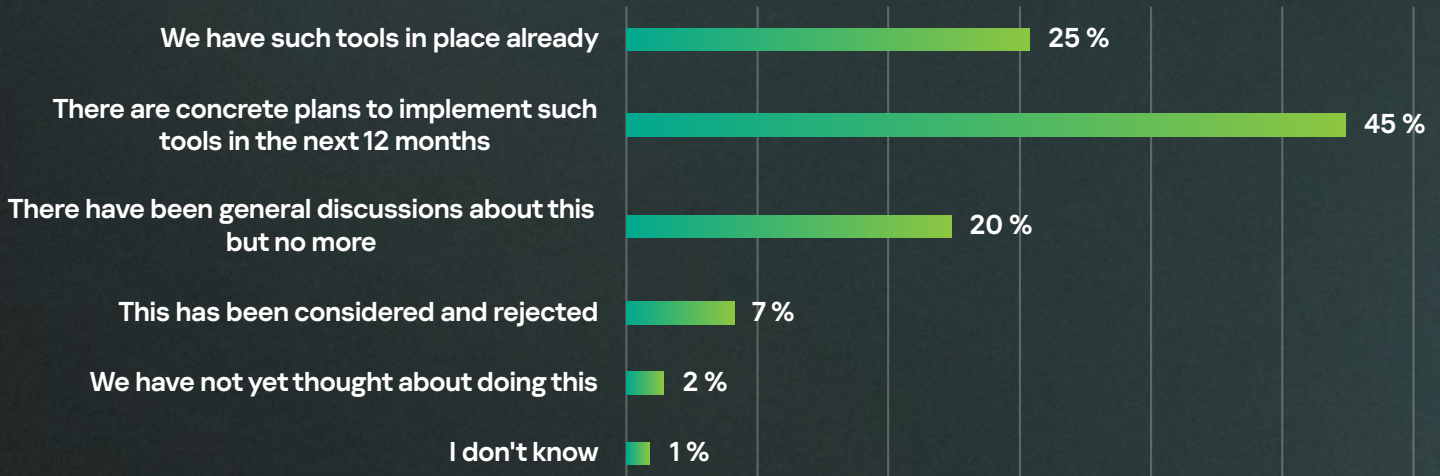


This focus on tools and new software is confirmed when respondents are asked about the best way to plug gaps in their cybersecurity defenses. By far the most common answer was general cybersecurity investment increases (41%), compounded by the specific aim of purchasing more tools (software) which one-third agreed with.



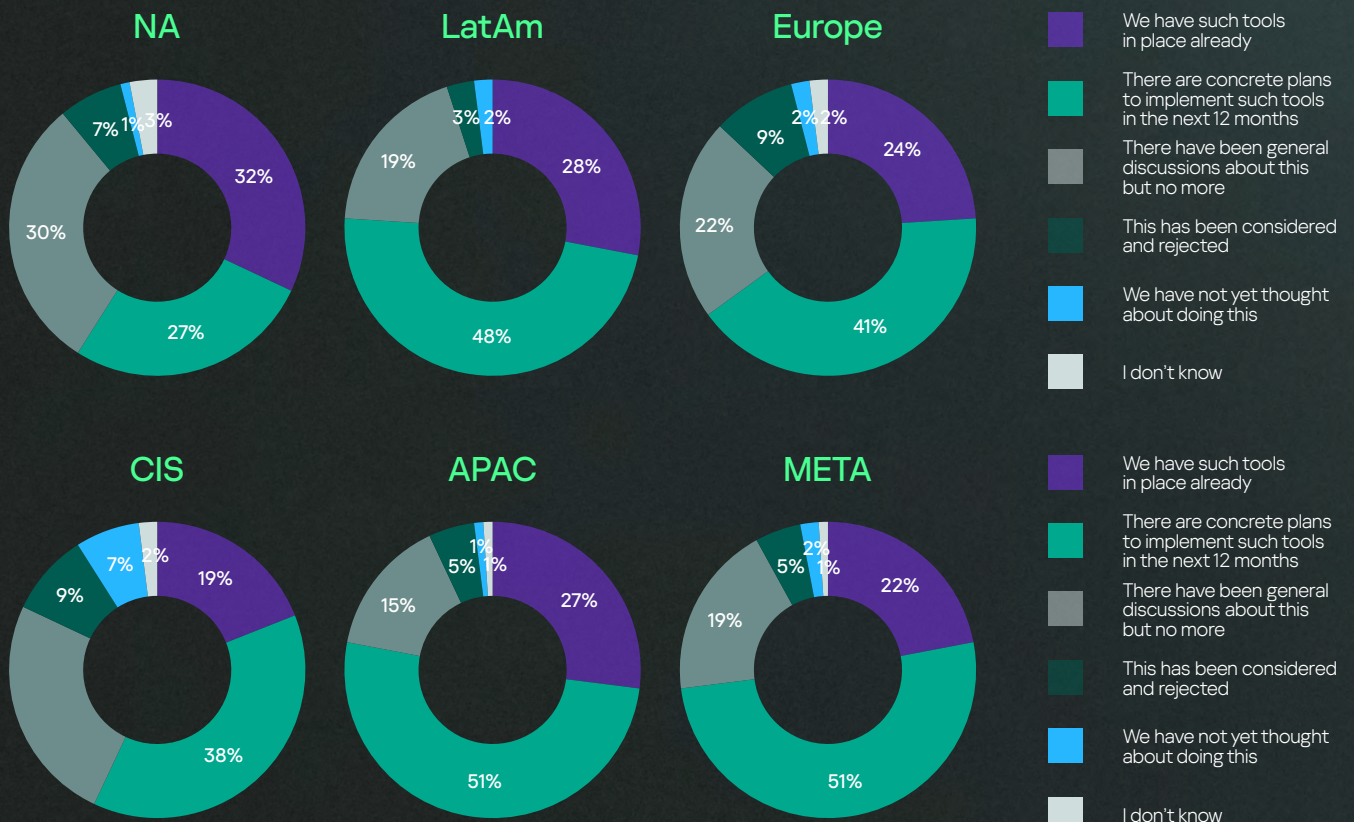
These tools often include elements of automation:

Is your company considering the implementation of software tools that automatically manage parts of your cybersecurity?

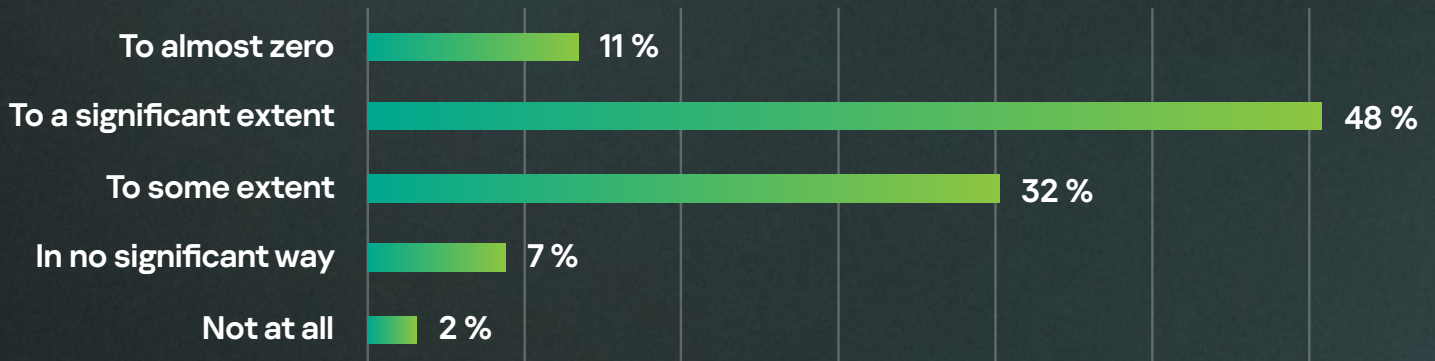


One-quarter of respondents work for companies with automation tools already in place, while almost double that number (45%) have concrete plans to introduce these in the next 12 months. Only 9% have either rejected the idea or not considered automation yet.

North America (32%), LatAm (28%) and APAC (27%) have the highest volume of automation tools already in place, which might explain their strong confidence around current protection levels. However, North America also has the second highest proportion of those who have only discussed the possibility. This suggests that most have either already done it, or don't plan to do it any time soon. In all other regions, the most common response was a middle ground where they plan to introduce automation tools in the next 12 months.

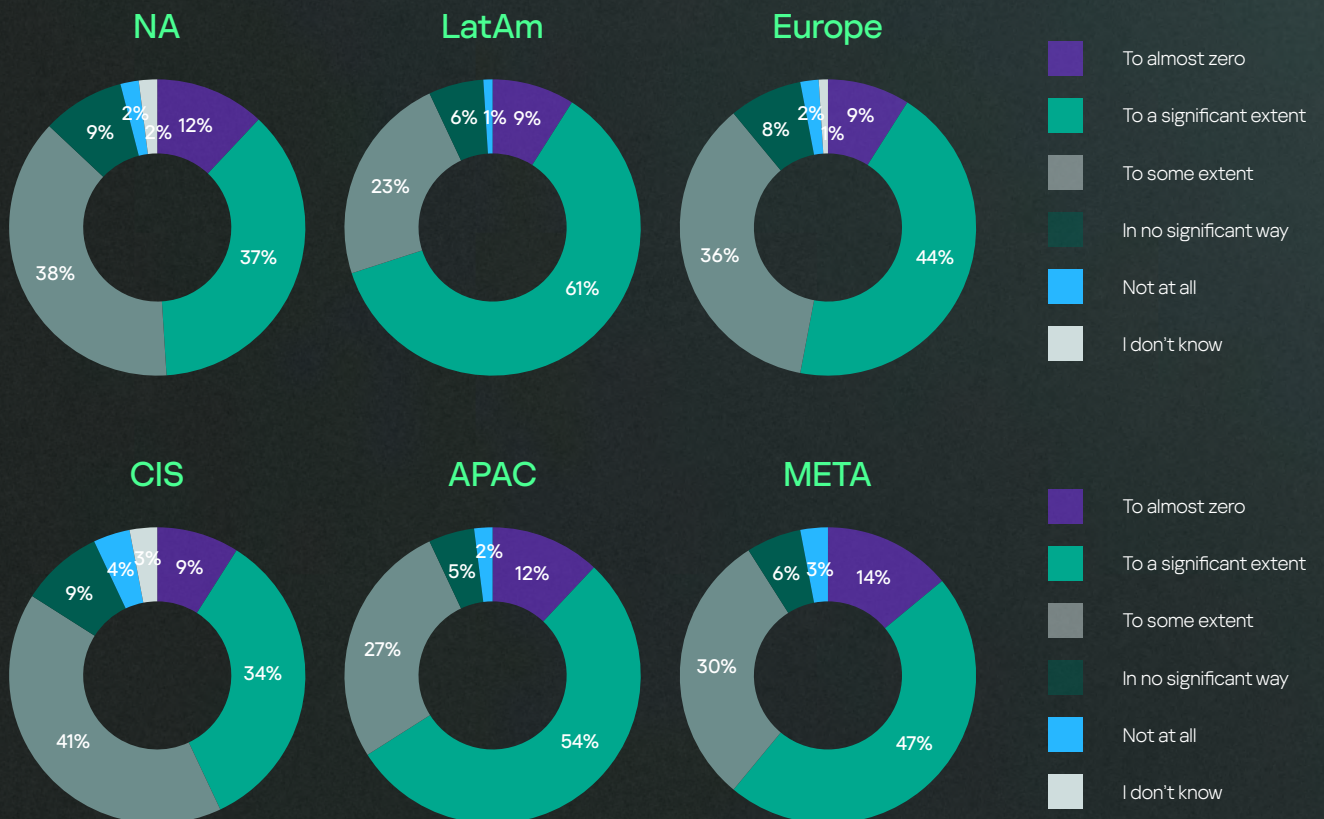


Automation tools will reduce the cybersecurity risk posed by human error...



Only 9% don't believe automation tools will have a positive impact on reducing risks associated with human error, with far more (59%) believing the risk will be reduced significantly (if not to almost zero).

Again, North America's polarized response to automation comes through, with one of the highest proportions who believe risk would be eliminated (12%), alongside 11% who think it would have no significant impact at all. Latin America and APAC have the most confidence in the role of automation tools, with only 7% in each case believing there would be no significant impact to risk from its introduction. In turn, despite a high level of doubt about the full effectiveness of automation in META, they also show the highest level of confidence that automation will reduce risks of human error to almost zero (14%).



Automation is the flavor of the month, year and possibly the future, too. But companies must proceed with caution.

A revised approach to cybersecurity and the human factor

It is easy to forget where the risk is coming from when investments are being made in new technologies, but automation doesn't remove humans from the work process. And it is humans who have been shown to create the biggest risk to cyber defenses

Across the board, automation has clearly been identified as a vital tool to enhance cybersecurity levels and protect companies more effectively. In most cases, the conversation around automation has already happened, and for many, implementation has begun. In some regions, investment in automation has led to strong confidence around general cybersecurity protection.

However, the general volume of incidents that are still occurring around the world suggest that this confidence should be tempered slightly. It is easy to forget where the risk is coming from when investments are being made in new technologies, but automation doesn't remove humans from the work process. And it is humans who have been shown to create the biggest risk to cyber defenses, no matter the size of the company.

This is why automation must dovetail with ongoing education of both non-IT staff and IT professionals. It must be part of an investment plan that also embraces software that protects endpoints, that safeguards internet and mail gateways, and that provides direct professional consultative services. It must form part of an overall matrix where prevention, detection and response interlink as an ecosystem of solutions. And, most importantly, it must bring both non-IT and IT staff along with them through every investment.

Tools to help safeguard against human error are a vital step forward, but they can't exclude employee education and skills development. After all, the threats that lurk outside company walls are also human-based – hackers continuously seeking to outrun the pace of innovation and exploit not only software, but fallible staff members as well.

This is why the whole human factor must be considered when identifying the next phase of cybersecurity – a 360° view of the entire threat landscape, beginning with those closest to home.



www.kaspersky.com

© 2023 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.

kaspersky