Cybersecurity in the era of AI

F.A.Z. INSTITUT

sopra steria

Contents

Sopra Steria SE, Hans-Henny-Jahnn-Weg 29, 22085 Hamburg, Germany
F.A.Z.-Institut für Management-, Markt- und Medieninformationen GmbH, Pariser Straße 1, 60486 Frankfurt am Main, Germany

Publishing house: F.A.Z. BUSINESS MEDIA GmbH — Ein Unternehmen der F.A.Z.-Gruppe, Pariser Straße 1, 60486 Frankfurt am Main, Germany; Managing directors: Dominik Heyer, Hannes Ludwig

Cover photo: AI-generated

Editorial board: Jacqueline Preußer, Dr Fabian Sickenberger, Fabian Westermeyer, Mira Würzberger
Design and layout: Christine Lambert
Proofreading: Geraldine Diserens (English version)

FOREWORD

The new cyber risks posed by generative artificial intelligence (GenAI) are not a topic for the future – they are here now, across all industries. The results of the survey of 564 specialists and managers as well as 1,003 employees in Germany provide an overview of the current situation. The analysis shows the extent to which companies and authorities are currently affected and how they are strategically addressing the risks.

The new situation requires a rethink – a security strategy that takes AI into account on the attacking side and integrates it on the defending side. The strategy should be designed to use automated learning to bring about a permanent and, above all, rapid adaptation of defence capabilities. It is crucial for organisations to rely on AI.

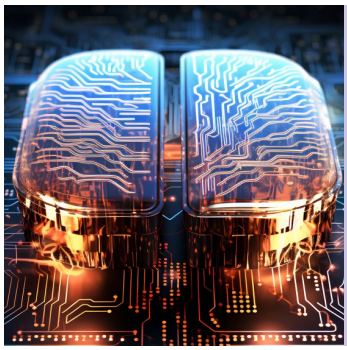
This includes attack detection that is not only based on classic rules and known cases but is supplemented by systematic anomaly detection – the keyword being: AI on big data. This allows unknown attack patterns to be recognised earlier and more effectively. In addition, business and public administration need well-trained personnel with GenAI and security expertise who can train, monitor, and integrate AI solutions. This mix is rare, as this report shows. But there are ways out of this dilemma.

One solution is more collaboration: everyone is still more or less doing their own thing and competing for experts. If companies and public administration pool resources and expertise between them and across the board to address common issues, everyone will benefit. This also includes cooperation with start-ups and cybersecurity partners.

A strategic reorientation is now required. Because only this will enable companies and authorities to manage cyber risks properly. The motto should be: Better armed with AI instead of hopeless without AI.

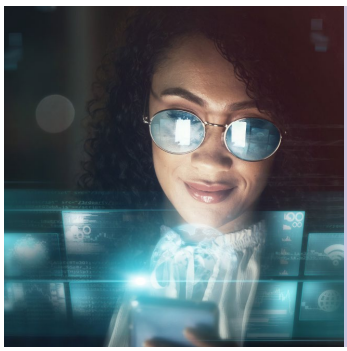
Sopra Steria
F.A.Z.-Institut

Executive Summary



- 73 per cent of the organisations surveyed see a heightened threat in the digital space due to the malicious use of AI.
- 81 per cent of respondents plan to invest in increased cybersecurity in the next twelve months.
- 54 per cent say that organisations who do not use AI in cybersecurity will have no chance against cybercriminals in the future.

- Employees are often the gateway for cyberattacks.
- Phishing is on the rise – and is becoming more difficult to recognise.
- Only 48 per cent of organisations provide their employees with regular cybersecurity training.
- 65 per cent of employees have already used AI at work. However, clear guidelines are rare, which harbours risks.



- 34 per cent of organisations cite new protection possibilities offered by AI as a reason for increasing their cybersecurity.
- More than half of those surveyed are confronted with a lack of personnel and expertise in the domain of cybersecurity.
- 80 per cent believe that organisations should work together to protect themselves effectively against cyberattacks.

- Respondents see the greatest damage scenarios in the theft, sabotage and encryption of data.
- 72 per cent see cybersecurity as a strategic issue that they consider every time they set up a new process in their organisation.
- The understanding of cyber defence is no longer up to date: In the era of AI, there needs to be a paradigm shift towards cyber resilience.

Methodology

F.A.Z.-Institut and Sopra Steria commissioned F.A.Z. Business Media I research to conduct two surveys in April and May 2024 on how organisations and employees are currently positioned when it comes to cybersecurity and the use of AI. These survey results are combined with expert perspectives in this study "Cybersecurity in the era of AI".

Survey of specialists and managers

For this survey, 564 people were surveyed via computer-assisted web interview (CAWI). They work in specialist and management positions in their respective organisations and are spread across three selected sectors: 38 per cent of respondents work for financial service providers, including mainly banks and insurance companies. Around a third come from public administration, including local, state, and federal government. Around a quarter belong to the automotive and supplier sector.

Employee survey

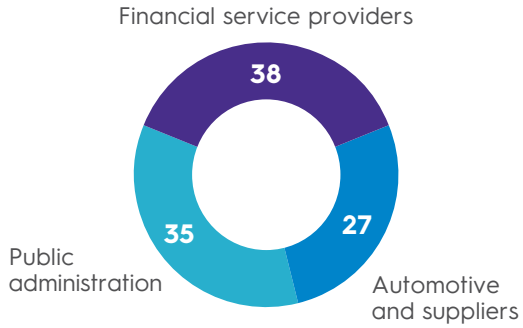
In the second survey, 1,003 working individuals (mainly employees and some self-employed) in Germany aged 15 and over were surveyed using a computer-assisted web interview (CAWI). The survey is quota-representative for the characteristics of gender, age, sector, and federal territory (North, East, South, West).

Expert interviews for more context

Four expert interviews supplement the survey results. The interviews provide in-depth information on the analyses and supply additional background knowledge. The interviews and quotes reflect the opinions of the respective interviewees.

Organisations surveyed, by sector

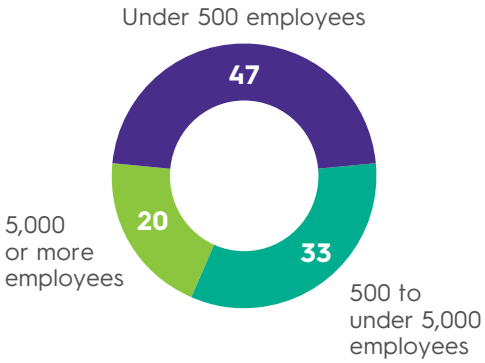
As a percentage of respondents, n = 564



Source: F.A.Z.-Institut, Sopra Steria

Number of employees in the organisations surveyed

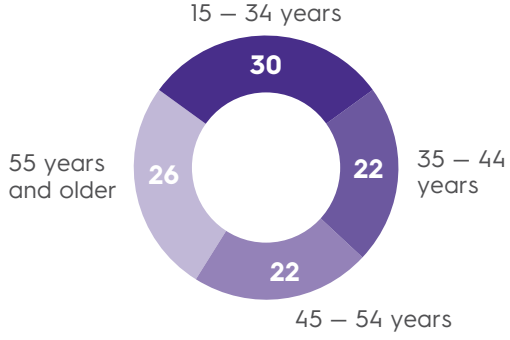
As a percentage of respondents, n = 564



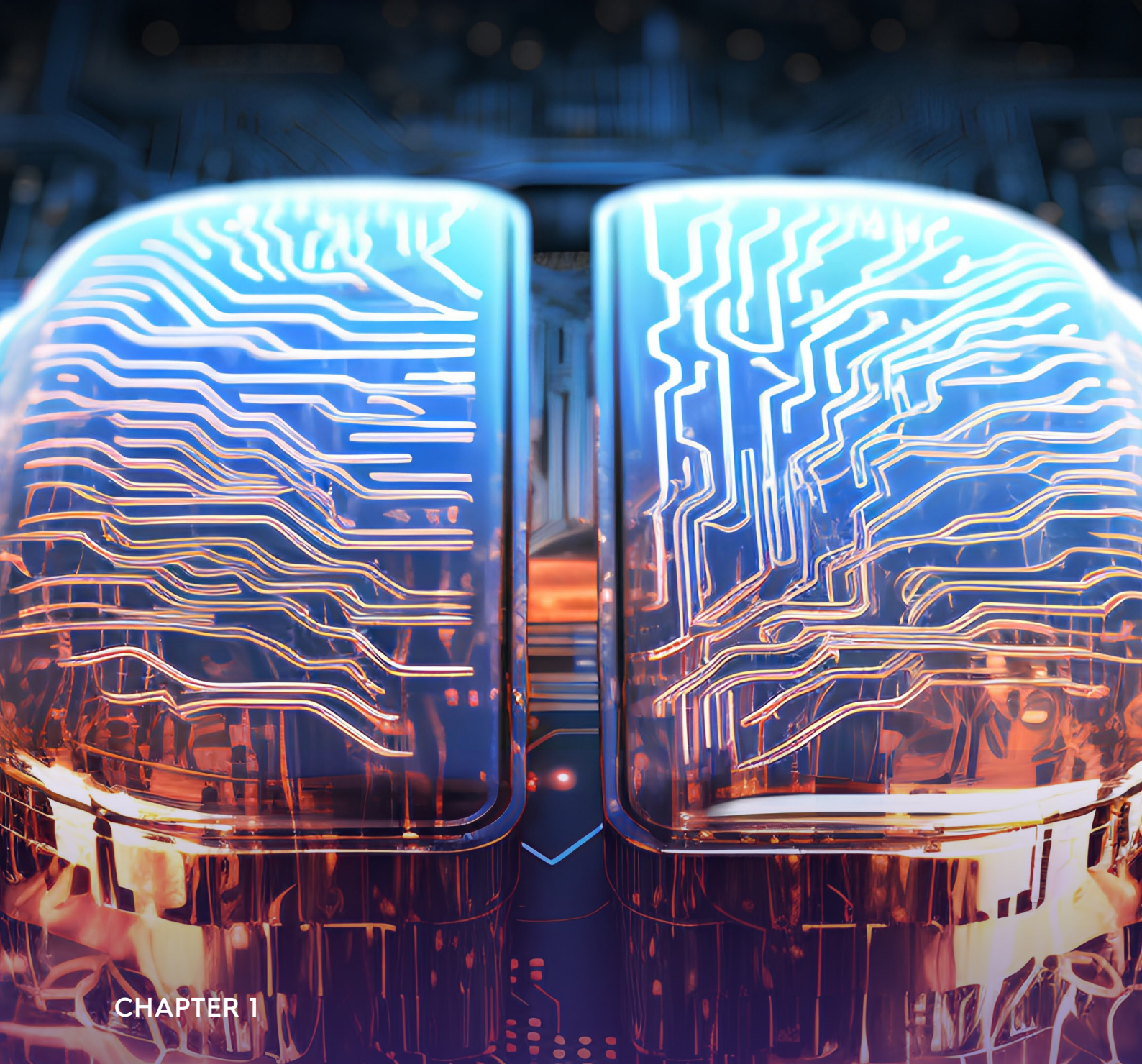
Source: F.A.Z.-Institut, Sopra Steria

Age distribution of the employees surveyed

As a percentage of respondents, n = 1,003



Source: F.A.Z.-Institut, Sopra Steria



CHAPTER 1

AI is transforming cybersecurity

The arsenal of cybercriminals has never been as powerful as it is today – one reason for this is artificial intelligence. It heightens the threat level for companies and authorities. However, AI applications are not always harmful; they can also be very helpful.

The use of AI is changing the cyberworld at groundbreaking speed. In 2024, it has become an integral part of it – for those who use it for attacks, but also for organisations that have to deal with such attacks. AI, and especially GenAI, facilitates the mass production and customisation of cyberattacks. Organisations must adapt to these new challenges.

73%

say the malicious use of AI has drastically raised the threat level in the digital space.

564 specialists and managers
Source: F.A.Z.-Institut, Sopra Steria

The threat has become more acute

Cybercriminals are using technology to personalise and automate attacks. With the help of language generation driven by GenAI, for example, they can make the 'grandchild trick' appear more authentic. AI enables them to analyse relationships in social networks quickly and easily. This allows them to target their attacks even more individually.

Most companies and authorities are feeling the resulting pressure: Around three quarters of the decision-makers surveyed stated that the malicious use of AI has drastically exacerbated the threat level in the digital space. Looking ahead, there is no easing in sight either: 93 per cent assume that certain threat scenarios will intensify over the next twelve months.

Attacks are increasing – and getting more sophisticated

Cyberattacks can be scaled better using AI. With large-scale phishing campaigns, even small organisations that do not see themselves as the focus of cybercriminals can quickly become victims. However, the perceived threat is not only related to the increased frequency of cyberattacks, but also to their higher quality. As a result, almost half of those surveyed say that AI has taken cybercrime to a whole new level.

The major motivators for greater cybersecurity

Why does your organisation want to increase its cybersecurity?

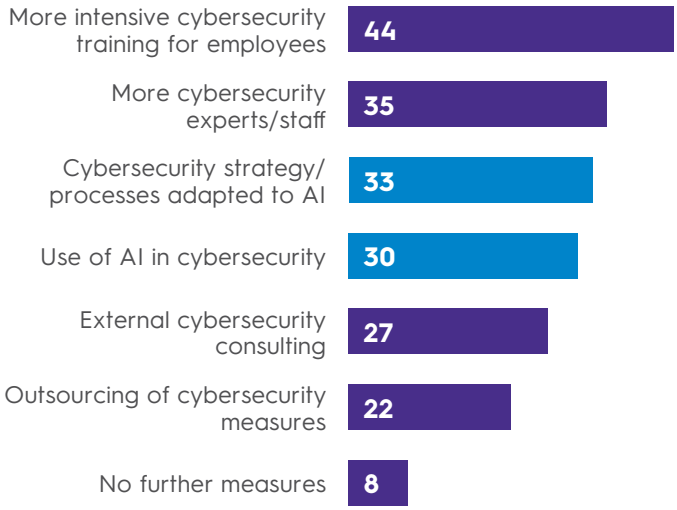
Specialists and managers who previously stated that they would invest in their own cybersecurity in the next twelve months; n = 461
Source: F.A.Z.-Institut, Sopra Steria

Do not wait, act now

AI-based cyberattacks are not an issue for the future – but one that must have an immediate impact on cybersecurity strategies. For this reason, most specialists and managers believe that prompt investment is necessary to improve protection: 81 per cent state that they intend to invest in their own cybersecurity in the coming year to boost it. One in three are specifically focusing on the misuse of AI and are adapting their cybersecurity strategy and corresponding processes accordingly. Fundamentally, however, the planned measures are broadly diversified.

AI is becoming increasingly important

What areas is your organisation planning to invest in over the next twelve months to increase its own cybersecurity?



Multiple answers possible; as a percentage of the 564 specialists and executives; without "Do not know/no answer" (11%)

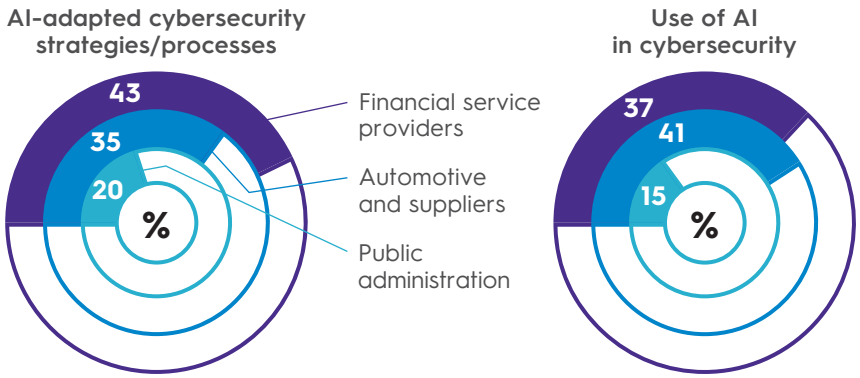
Source: F.A.Z.-Institut, Sopra Steria

Authorities are lagging behind

While planned investments in cybersecurity are similar among financial service providers and in the automotive sector, the plans are less comprehensive in public administration. This is particularly evident regarding AI: Only one in five authorities is planning a cybersecurity strategy or processes that are adapted to AI, and 15 per cent plan to use of AI in cybersecurity. Public administration is lagging behind here. At 13 per cent, it also has the highest proportion of those who are not planning any further measures in the medium term.

AI does not receive the same attention across the board

In which areas does your organisation plan to invest in the next twelve months to further enhance its cybersecurity?



Multiple answers possible; selected response options; 564 specialists and managers
Financial service providers n = 214; Automotive and suppliers n = 153; Public administration n = 197

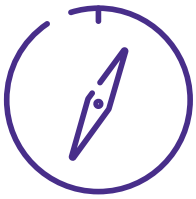
Source: F.A.Z.-Institut, Sopra Steria

Fighting AI attacks with AI

AI offers numerous opportunities to act preventively rather than reactively. With the help of this technology, it is possible to stay one or more steps ahead of attackers. AI applications help organisations to recognise patterns, learn from data, create situation reports and forecasts, or automatically run analyses. The majority of respondents (54 per cent) have recognised that without the use of AI in cybersecurity, organisations will not stand a chance against cybercriminals in the future. Hence the awareness exists, but there is still a lack of investment across the board.

Organisations are struggling to keep up

While hacker groups have specialised in circumventing organisations' cybersecurity, organisations can only invest a fraction of their resources in cybersecurity, given that their main business is in another area. This is also reflected in the respondents' assessment of AI expertise in companies and public administrations: More than seven out of ten assume that cybercriminals use AI significantly better for attacks than organisations do for defence. Only around one in nine disagree with this statement.



71%

believe that cybercriminals use AI significantly better for attacks than organisations do for defending against attacks.

564 specialists and managers

Source: F.A.Z.-Institut, Sopra Steria

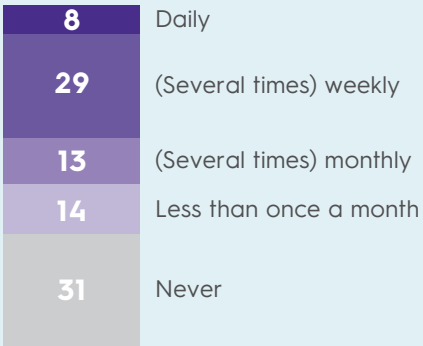
EMPLOYEE SURVEY

AI tools help employees

In addition to the 564 decision-makers from companies and public administration, 1,003 working individuals (mainly employees and few self-employed) were surveyed. The results are revealing with respect to the relevance of AI in everyday working life: Almost two thirds of those surveyed have already used AI tools such as ChatGPT, DeepL or Midjourney in their job. 37 per cent use AI applications on a weekly or even daily basis. In view of the obvious benefits, usage is likely to increase even further. AI applications can speed up numerous work steps, and some routine tasks can even be completely automated. This saves time – which in turn frees up resources for creative and strategically important tasks.

In the thick of it, not just an observer

How often do you use AI applications like ChatGPT, Midjourney, or DeepL at work?



As a percentage of the 1,003 employees; without "Do not know/no answer" (4%)

Source: F.A.Z.-Institut, Sopra Steria

INTERVIEW

"This is all happening now – there is no lead time"

GenAI is fundamentally changing the entire cyberinfrastructure. Cybersecurity expert Dr Barbara Korte explains how organisations can navigate this altered environment.

Dr Korte, why does the use of GenAI represent a turning point for cybersecurity?

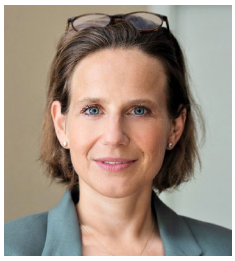
With GenAI, information from the internet can be used, for example, to create individualised phishing attacks. Language models help in coding what is known as polymorphic malware, which adapts to its target environment and thus cannot be detected. This combination of individualisation and scalability is revolutionary. Today, cybersecurity must recognise anomalies from their context instead of looking for known attack patterns, as was customary in the past. And just as attackers can systematically play through attack vectors using neural networks, pentesters can of course do the same. So, AI helps us too.

How can we protect ourselves against GenAI-based cybercrime?

US General Stanley McChrystal said this about the fight against the Al-Qaeda terrorist network: "It takes a network to defeat a network." This applies here too. Anyone who wants to effectively combat AI-supported attacks will only be able to do so with the help of neural networks.

What do you recommend for AI-based cybersecurity?

Firstly, you must be aware of this: This is all happening now – there is no lead time. Our report demonstrates this too. Secondly, we should not expect GenAI solutions to be perfect yet. The current development is astonishing, and yet there is still much room for improvement. Thirdly, GenAI must be considered as a whole and every possible use case and every transfer option for models must be examined. A fourth point is that an AI-based cybersecurity strategy requires expertise in AI as well as specialist knowledge in cybersecurity. This combination must be reflected in personnel. In addition, what neuroscientist Manfred Spitzer says about AI in general also applies to cybersecurity: AI will not replace experts – but experts who use AI will be clearly superior to those who do not. Therefore, every investment in AI training is worthwhile.



Dr Barbara Korte
is an expert on AI in cybersecurity at Sopra Steria.
barbara.korte@soprasteria.com

54%

say that without the use of AI in cybersecurity, organisations will stand no chance against future cyberattacks.

564 specialists and managers
Source: F.A.Z.-Institut, Sopra Steria

CHAPTER 2

Human vulnerability

People make mistakes. Cybercriminals try to provoke and exploit these mistakes. It is therefore important to develop a comprehensive awareness of the importance of cybersecurity among the workforce. So far, however, many organisations have been very negligent in this regard.

Employees continue to pose the main risk to cybersecurity. In the eyes of specialists and managers, inappropriate reactions to phishing messages and other attacks are still the greatest vulnerability in 2024. Despite the knowledge of human vulnerability, companies and authorities are not creating a lasting awareness of it.

48%

state that their organisation regularly trains its workforce on cybersecurity topics.

564 specialists and managers

Source: F.A.Z.-Institut, Sopra Steria

Train, train, and train again

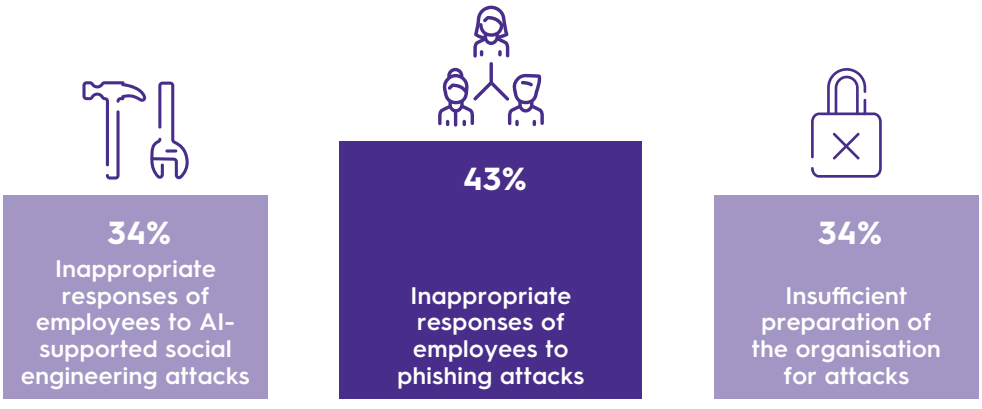
All employees in companies and public administrations are equally targets for large-scale phishing campaigns or social engineering attacks. As they generally do not have IT expertise, it is therefore important to establish a basic understanding of cybersecurity and an awareness of the dangers of cybercrime. If this is not achieved, many other efforts will remain ineffective. This requires organisations to provide their employees with professional, regular, and personalised training. However, only 48 per cent of respondents state that they currently do this. This lack of training extends across all sectors surveyed.

Raising awareness of the dangers and potential of AI

For those organisations that regularly offer cybersecurity training, AI already plays a key role. Almost three out of four specialists and managers state that they systematically prepare their staff for AI-enhanced phishing attacks. Identity theft and social engineering are covered in around half of cybersecurity training courses, while training in the secure use of AI tools has so far been the exception.

The main risk: the human factor

What do you currently see as the three biggest vulnerabilities in your organisation's cybersecurity?



Multiple answers possible with a maximum of three; depiction of the three most frequent answers; 564 specialists and managers

Source: F.A.Z.-Institut, Sopra Steria

EMPLOYEE SURVEY

Phishing is on the rise – and getting better

Fraudulent messages are a major threat to organisations. Although spam filters and security precautions in email programs are constantly improving, hackers' methods of attack are also evolving. The fact that phishing messages are landing more and more frequently in email inboxes or on smartphones is confirmed by the employee survey: Around four out of ten respondents report an increase in such messages.

41%

of respondents reported receiving more phishing emails in the past twelve months than previously.

1,003 employees
Source: F.A.Z.-Institut, Sopra Steria

However, these figures only relate to those organisations that provide regular training. In relation to all respondents, the figures are only half as high. This means that not even one in eight organisations currently offers training on how to use AI tools such as ChatGPT at work.

Increasing security in dealing with AI

In a comparison of industries, financial service providers offer particularly comprehensive training on AI, followed by automotive and – lagging well behind – public administration. This applies to training in both the possibilities of identity theft as well as in social engineering and the secure use of ChatGPT and similar applications within the organisation. One reason for this is that banks and insurance companies have already been providing products and services entirely online for several years now and are therefore aware of the importance of cybersecurity awareness strategies.

73%

state that they train employees to deal with phishing attacks by cybercriminals which are more sophisticated through the use of AI.

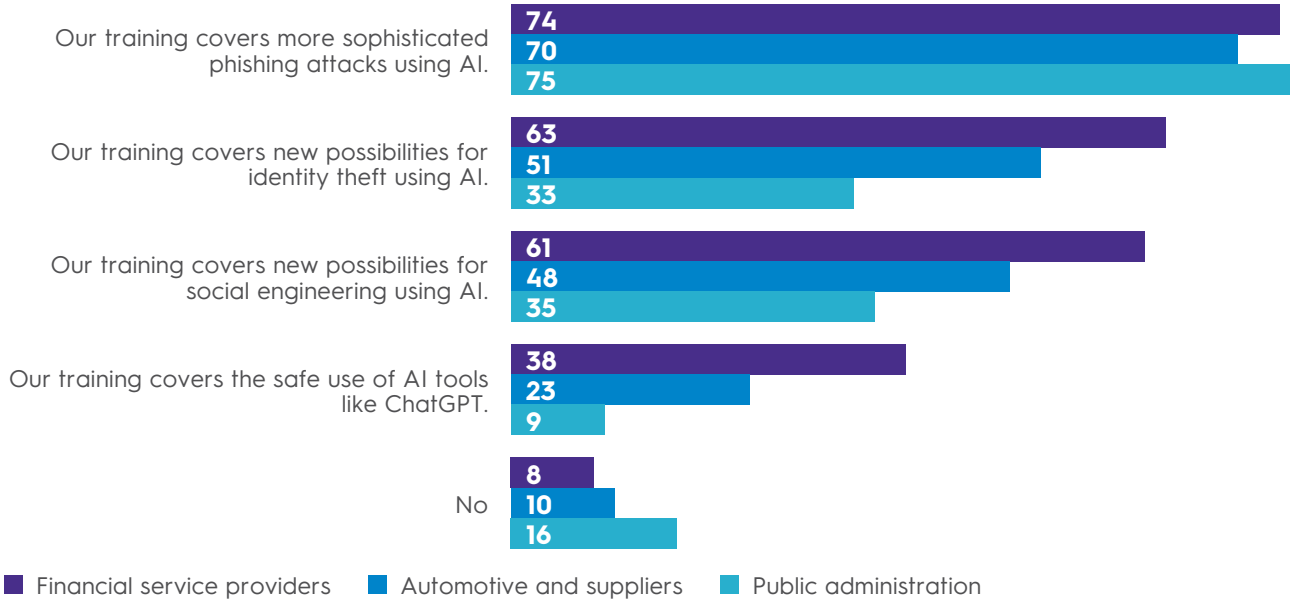
24%

say that their organisation trains employees on the safe use of AI tools like ChatGPT in the work context.

Specialists and managers who previously stated that they regularly train their workforce on cybersecurity; n = 272
Source: F.A.Z.-Institut, Sopra Steria

The financial sector provides the most comprehensive training

Does your organisation also train its workforce regarding the threats and risks of AI?



Multiple answers possible; as a percentage of specialists and managers who previously stated that they regularly train their workforce on cybersecurity; n = 272
Financial service providers n = 104; Automotive and suppliers n = 73; Public administration n = 95; without "Do not know/no answer" (2%)
Source: F.A.Z.-Institut, Sopra Steria

The larger the company or authority the specialists and managers surveyed work for, the more frequently training is provided. The thematic diversity of the training courses also increases with the number of employees. Nevertheless, it is also important for small organisations to make their employees aware of the risks. If an in-house cybersecurity department cannot be set up, basic protection should not be skimped on as well.

Larger organisations are more active

What measures is your organisation currently taking to improve its own cybersecurity?
"We regularly train our workforce on cybersecurity topics."

As a percentage of the 564 specialists and managers
Under 500 employees n = 266; 500 to under 5,000 employees n = 186; 5,000 employees or more n = 112
Source: F.A.Z.-Institut, Sopra Steria

Clear regulations for AI tools are rare

When asked how their employers regulate the use of AI applications, the employee survey provides a mixed picture: Only a little over one in four organisations sets clear guidelines in the form of written rules or verbal recommendations. A quarter, on the other hand, do not have any corresponding regulations at all, although the use of AI is generally permitted. Just under a fifth of companies and public authorities lack transparent regulations. As a result, employees are not aware of whether and which tools they are allowed to use. If employees fill this vacuum themselves by integrating AI applications on their own initiative, this can have far-reaching consequences for data protection and cybersecurity.

AI usage in the workplace

How does your employer regulate the use of AI applications such as ChatGPT, Midjourney, or DeepL?

The use of AI applications is ...

Multiple answers possible; as a percentage of 1,003 employees, without "Do not know/no answer" (18%)
Source: F.A.Z.-Institut, Sopra Steria

INTERVIEW

"Awareness measures must evolve along with the risks"

With customised training, technology and clear processes, organisations can counteract phishing attacks. Cybersecurity expert Stefan Beck explains what this should look like in detail.

Mr Beck, in the era of AI, cybercriminals are specifically targeting poorly informed employees. How should employers respond to this?

We need to raise awareness of a new form of phishing attacks that are becoming increasingly sophisticated thanks to AI. Our survey also shows that AI tools are already very common in everyday office life. Their use also requires regulations and training with continuous updates. In general, the following applies: Awareness measures must evolve along with the risks.

What specific changes can companies or authorities make?

Education and spot checks alone are just as inadequate as generalised measures today. Developers, for example, require different training than employees with administrative tasks. Awareness of security risks can only be raised permanently through individual programmes. In addition, organisations should use technological resources and define processes in such a way that phishing attacks do not succeed. Protection classes for documents are a first step towards preventing, for example that information from emails is loaded into a translation model and subsequently circulated on the internet. Sandbox environments can also be used to intercept malware before it causes damage.

Should organisations use AI to increase awareness?

Absolutely. For example, employers can use AI models to personalise test attacks to close individual awareness gaps in a targeted manner. Not everyone falls for the same tricks. Learning AI tools can also adapt awareness campaigns to new or unknown attack patterns. AI is part of the solution in other areas too, because with conventional methods it is becoming increasingly difficult to analyse enormous amounts of data quickly to find indications of cyberattacks. AI-based solutions can do this. And they can also recognise and fend off previously unknown methods of attack. In the long term, we are on the brink of a battle between machines, similar to some science fiction novels – except that there are also machines that are on the side of humanity.

Stefan Beck
is Senior Manager Cyber Security Public Sector at Sopra Steria.
stefan.beck@soprasteria.com

26%
consider the unregulated use of AI tools as one of the three biggest weaknesses.

564 specialists and managers
Source: F.A.Z.-Institut, Sopra Steria

CHAPTER 3

Combining AI and technical expertise

Not all organisations are up to date when it comes to cyber-security. Why is this? Lack of personnel, lack of expertise and a lack of money. Especially in public administration, these factors jeopardise security.

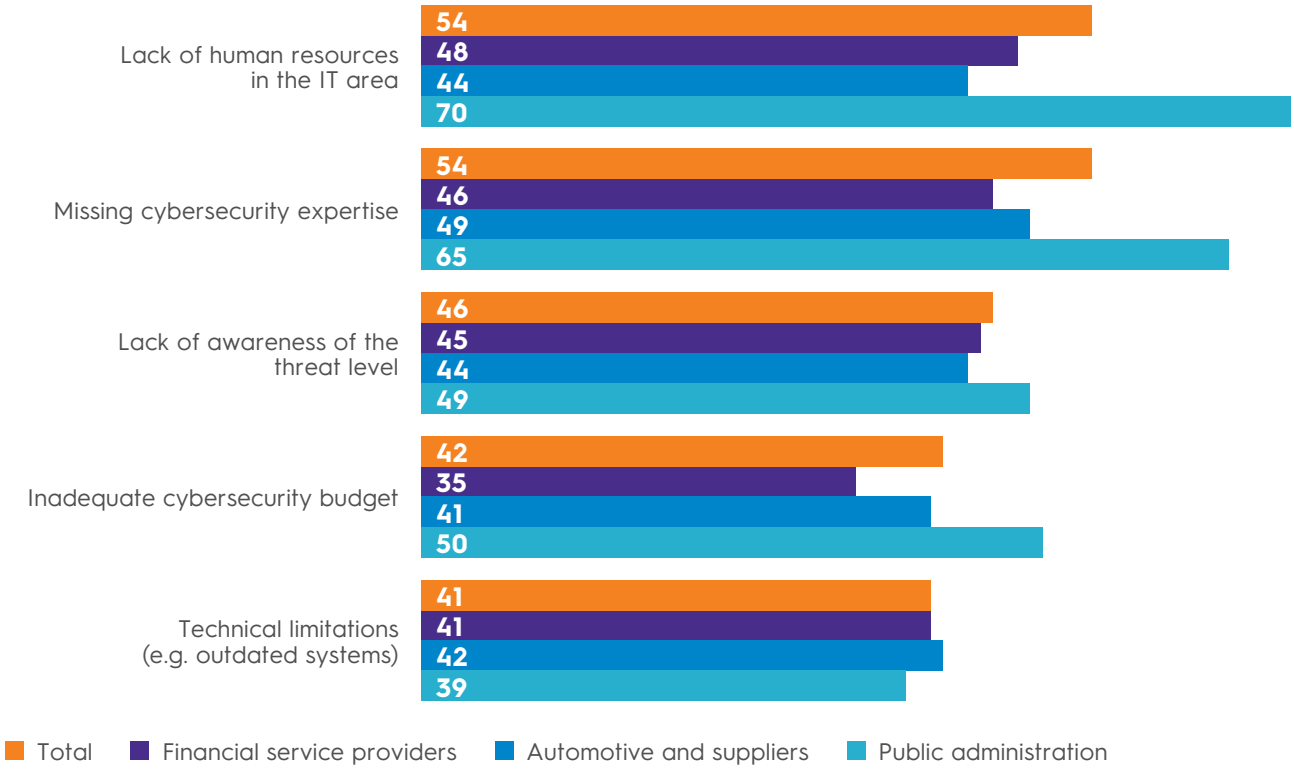
Successful cybersecurity depends on the interplay of many factors. Deficits in just a few areas can quickly jeopardise an organisation's entire security. Currently, the shortage of skilled workers and a lack of expertise are the biggest obstacles on the path to greater cybersecurity. Growing demand for experts is meeting short supply. In addition, 46 per cent of respondents are not aware of the risks associated with insufficient cyber resilience.

The problems are most serious in public administration

Respondents from the public sector in particular report enormous weaknesses in terms of personnel and expertise. Even immediate measures such as the German IT specialist allowance are only a small step and are not sufficient to eliminate such staff shortages. The remaining IT staff have to protect increasingly large areas and investigate more and more incidents.

Personell and expertise for cybersecurity is missing

In your own estimation, what prevents companies and authorities from working on their own cybersecurity?

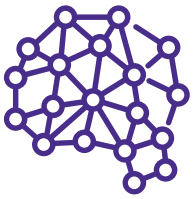


Multiple answers possible; as a percentage of the 564 specialists and managers; depiction of the five most frequent answers
Financial service providers n = 214; Automotive and suppliers n = 153; Public administration n = 197

Source: F.A.Z.-Institut, Sopra Steria

In the finance and automotive sectors, both aspects are less of an issue than in public administration. One possible reason for this is the comparatively less stringent regulatory environment, which often acts as an obstacle to the use of new technologies in the public sector. The differences in budget are similar. Here, too, more decision-makers from public authorities cite inadequate funding than those from companies.

The respondents working at public authorities are aware of their past shortcomings: 30 per cent of those who want to invest in cybersecurity in the next twelve months say they have done too little in this area up to now. In the automotive sector, 22 per cent express this, while only 13 per cent of financial service providers surveyed say it.



34%

cite the new possibilities offered by AI for protecting IT systems as one reason for increasing their cybersecurity.

564 specialists and managers
Source: F.A.Z.-Institut, Sopra Steria

Immediate measures and long-term changes

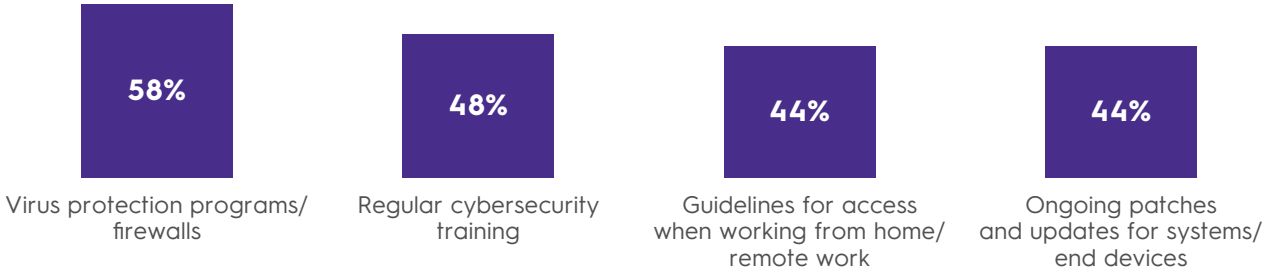
The two most frequently mentioned factors, personnel and expertise, cannot be changed quickly and easily overnight. It takes time to recruit staff and build expertise. It is important to plan for the medium and long term and to pursue a well-thought-out security strategy. This includes integrating AI into one's own security architecture. This means additional effort, but in the long term it will relieve the burden on staff and increase the quality of services.

AI as a catalyst for modernisation

This aspect is recognised by the decisionmakers: Nearly a third of the respondents say they want to improve cybersecurity because AI offers new possibilities for IT protection. In addition to integrating AI into cybersecurity, immediate measures are also important. For example, technical updates and immediate investment in fundamental training can quickly increase basic protection. This creates the necessary security for major changes.

Basic protection often neglected

What measures is your organisation currently taking to improve its own cybersecurity?



Multiple answers possible; 564 specialists and managers; depiction of the four most frequent answers
Source: F.A.Z.-Institut, Sopra Steria

There is even a lack of simple tools

A look at the status quo shows that some organisations have not yet fully recognised the current need for action: Even the simplest IT baseline protection measures, which the Federal Office for Information Security (BSI) in Germany considers to be mandatory, are lacking in many organisations. Less than half of them offer regular cybersecurity training, and only 58 per cent use virus protection programs or firewalls. 44 per cent continuously patch and update all systems and end devices, while 38 per cent actively test their systems for vulnerabilities. This passivity opens the door to potential attackers. To close these security gaps, even low-threshold measures are sufficient.

EMPLOYEE SURVEY

Data protection is a basic expectation

The public expects companies and public authorities to exercise caution and responsibility when handling their data. However, many organisations are still struggling to ensure a high level of cybersecurity. This is shown by the employee survey. These high expectations will certainly not diminish in the future. In the era of AI with an increasing focus on data, the importance of handling data responsibly is likely to increase further.

84%

"When I give my data to a company or public authorities, I expect them to take all the necessary steps to protect my data from criminals."

Agreement rate; 1,003 employees
Quelle: F.A.Z.-Institut; Sopra Steria

INTERVIEW

"Not an annoying add-on"

Budget shortages, a lack of skilled labour, high demands on the workforce. How can all this be overcome in the era of AI? Olaf Janßen, Head of Cyber Security, explains.

In this report, the majority of specialists and managers say that cyber-criminals use GenAI better than companies and authorities. Are the attackers always one step ahead?

For criminals, cyberattacks are their core business. Companies and the public sector generally do other things as well as cyber defence. They often cannot deploy as many resources as they need to for this – unless they are service providers in this area. If they are to do more than just keep up, cybersecurity needs to be more closely integrated into the core business. The best way for organisations to achieve this is by organising themselves into ecosystems and finding joint strategies. It makes no sense to lure specialists away from each other for a task that affects everyone and in which no one is competing with anyone else.

Many cybersecurity organisations are struggling with budget and staff shortages as well as high skills requirements. How can these challenges be overcome?

First of all, it is important not to view cybersecurity as an annoying add-on that only costs money. This new perspective raises the importance of the topic, including in the distribution of resources. The much-cited shortage of skilled labour is clearly exacerbated in cybersecurity. Cooperative approaches between industry and the public sector are needed here to address the staff shortage, promote skilled labour and, as a result, have more skilled workers available. Sharing models should not be taboo either. After all, despite all the opportunities for automation, highly qualified people are essential to train and monitor AI models and integrate them into the security system. A third strategic lever is outsourcing, i.e. the use of managed security services, where external experts take over security monitoring and management.

Which cybersecurity tools can be improved with the help of AI?

Security operations centres (SOC) and endpoint detection and response (EDR) solutions are already working with AI components in many cases. There is great potential in AI for prevention, i.e. in recognising threats before they cause damage. In addition, the mapping of regulatory requirements can be automated in order to implement requirements more promptly and close existing regulatory gaps faster. This facilitates compliance with regulations and improves safety measures.

Olaf Janßen
is Head of Cyber Security at Sopra Steria.
olafjanssen@soprasteria.com

80%

"To protect themselves effectively against cyberattacks, organisations should work together."

Agreement rate;
564 specialists and managers

Source: F.A.Z.-Institut, Sopra Steria

CHAPTER 4

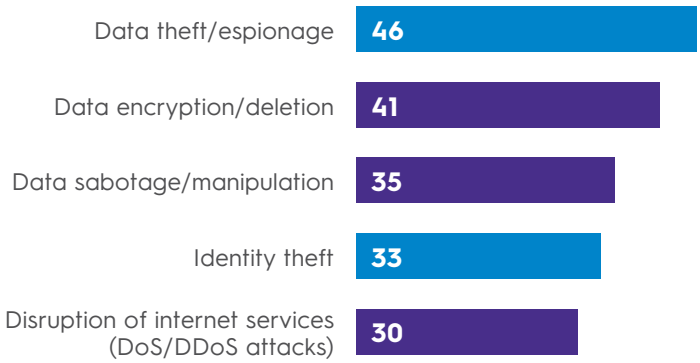
Counteracting dangers

Companies and authorities are exposed to many different sources of danger – from data espionage to identity theft. To respond adequately, there needs to be a rethink towards targeted cyber resilience.

Data is a valuable treasure trove for organisations and therefore attractive prey for hackers. With regard to the most damaging criminal activities in cyberspace, respondents cite data-related scenarios including theft/espionage, encryption/deletion and sabotage/manipulation most frequently. No scenario stands out. The threat is multifaceted, the number of potential attackers high. Protecting against individual sources of danger is therefore no longer enough, organisations must have broadly based cybersecurity.

Concerns about data and identity theft

In your opinion, which three scenarios in the digital space are currently causing the most damage to organisations in your industry?



Multiple answers possible with a maximum of three, as a percentage of the 564 specialists and managers, depiction of the five most frequent answers

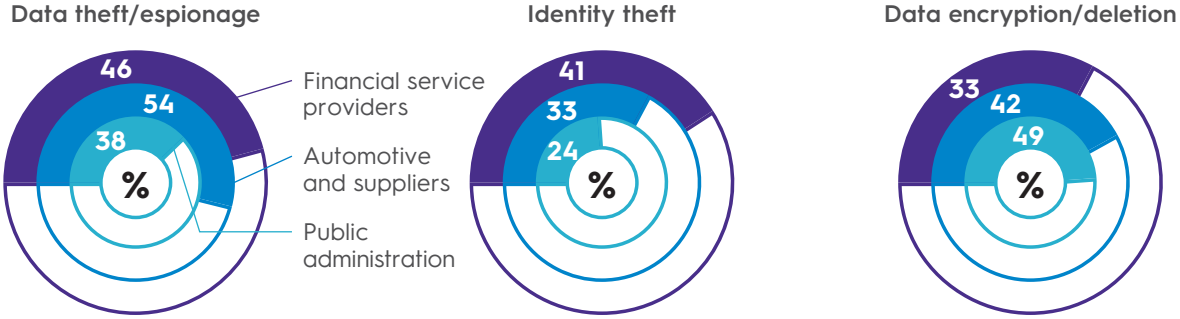
Source: F.A.Z.-Institut, Sopra Steria

Industries struggle with different risks

Data theft and espionage as well as identity theft are the biggest problems. For example, AI tools that are used for voice cloning or deepfake videos are pushing existing identification methods to their limits. On the other hand, financial service providers can also use IT tools to identify anomalies in payment transactions, and thus detect cybercrime. Among car manufacturers and suppliers, more than half of those surveyed cited data theft and espionage as the biggest damage scenario. Public administration cites data encryption and deletion of data as damaging to their sector.

Identity theft is threatening the financial sector

In your opinion, which three scenarios in cyberspace are currently causing the greatest damage for organisations in your industry?



Multiple answers possible with a maximum of three answers; selection of response options
564 specialists and managers: Financial service providers n = 214; Automotive and suppliers n = 153; Public administration n = 197

Source: F.A.Z.-Institut, Sopra Steria

Prepare for more and new damage scenarios

93 per cent of the specialists and managers surveyed assume that there will be an increase in damage scenarios due to the use of AI in the next twelve months. The strongest increase is expected in the area of data theft/espionage, where the respondents already report the greatest damage caused by cybercriminals. With AI, hackers now have another weapon to attack organisations more precisely. In view of the new technological possibilities, respondents also expect an increase in identity theft.

Digital theft using AI on the rise

In your opinion, which three scenarios will increase the most over the next twelve months due to the use of AI by cybercriminals?

Multiple answers possible with a maximum of three; selection of response options; as a percentage of the 564 specialists and managers, depiction of the three most frequent answers

Source: F.A.Z.-Institut, Sopra Steria

Intelligence services as role models

To counteract the numerous threats in cyberspace, companies and public administration need to broaden their perspective and capabilities. A new mindset is needed, one that is partially inspired by the mindset of the intelligence services. Organisations should keep a watchful eye on how the threat level develops and put themselves in the shoes of potential attackers. Increasingly, this must also take into account actors from foreign states who have an interest in (economic) espionage and sabotage.

External expertise to aid the transition

Cooperation with external experts helps against well-organised and specialised attackers: Service providers often have a better overview of the dangers and can categorise them on a cross-industry and comparative basis. They monitor the regulatory requirements for cybersecurity for all their customers on an ongoing basis, which enables them to implement regulations much more efficiently and ensure better quality. Service providers also have measures at hand to firmly integrate cybersecurity into the DNA of the respective

31%

say that their organisation has commissioned an external service provider for cybersecurity.

564 specialists and managers

Source: F.A.Z.-Institut, Sopra Steria

organisation and to embed the necessary awareness among all employees – to utilise the full technological potential for greater security.

Furthermore, experts help to meet the respective challenges – as threatening as they may be – with the necessary calm and foresight. At present, just under a third of organisations have external service providers for cyber-security. 27 per cent of organisations surveyed are considering working with an external cybersecurity consultancy in the next twelve months.

72%

"Cybersecurity is a strategic issue that we consider every time we set up a new process in our organisation."

Agreement rate;
564 specialists and managers

Source: F.A.Z.-Institut, Sopra Steria

Prudent action with a clear strategy

The importance of cybersecurity has increased in recent years. Around seven out of ten respondents say that they consider cybersecurity right from the start in new processes and products. In certain areas regulatory requirements mandate this anyway, for example in the context of critical infrastructures (KRITIS) or the Digital Operational Resilience Act (DORA). In practice, however, the strategy shift is often still sluggish.

Paradigm shift in cybersecurity

Overall – and particularly in view of the growing threat posed by cybercrime – the following applies: Companies and authorities must act proactively instead of responding reactively to attacks. To do this, they need a security strategy that has tactical and operational mechanisms to ensure that the organisation, processes and technology can adapt to changing risks. Threats must be recognised in the context of high-quality threat intelligence before damage occurs.

In future, this will require a real-time picture of the situation, for which the respective organisation is continuously scanned for risks. This will only be possible if all available (data) sources are constantly consulted and collated. AI will play a decisive role in this context. It will help to get ahead of the situation.

INTERVIEW

"We are in a race"

IT systems are exposed to many threats. A successful hacker attack has massive consequences for the affected organisation and can also have an impact on society. Timo Kob, Professor of Cybersecurity and Business Protection, explains where companies and authorities need to act now and in the future.

Professor Kob, how has the threat situation in the cyberspace for companies and public administrations developed in recent years?

The general situation has been getting worse for years. There are several reasons for this. Firstly, everyone is becoming increasingly dependent on IT systems. We live and work in a world that is shifting more and more towards the digital realm. In addition, the circle of attackers and potential targets has been growing for years. Cybercrime is becoming increasingly profitable due to growing professionalisation and new technologies. At the same time, the risk of state espionage and sabotage has increased significantly due to geopolitical tensions. This automatically increases the threat level.

© Kühnapfel Fotografie

Prof Timo Kob
is a Professor of Cybersecurity and Business Protection at FH Campus Wien and a member of the Management Board of HiSolutions AG.

"Cybercrime is becoming increasingly profitable due to growing professionalisation and new technologies."

What role does artificial intelligence play in this?

AI is a topic that keeps us very busy in cybersecurity. We are in a race between attackers and defenders. AI is giving both sides new weapons. The situation is unlikely to change fundamentally if both sides take action. But this balance will only exist if organisations focus on using AI as part of their defence. If they say: "Nothing will happen," this can quickly end in disaster.

Who are the attackers targeting?

Anyone with money or knowledge is an attractive victim. And those who do not protect themselves all the more so. The cybercriminal is a homo oeconomicus. If they cannot get in after a few attempts, they will try another address. But some companies leave their front door virtually unlocked due to a lack of basic protection. The groups that hackers target ranges from corporations to local authorities and doctors' surgeries.

Technologies such as AI bring a new dynamic to cybersecurity and have an impact on large areas of IT security architecture.

In ransomware campaigns, multiple targets are attacked in order to increase the chances of success.

Which sectors and organisations are particularly at risk?

Germany sees itself as a country of hidden champions, but that does not mean that these companies are invisible to potential attackers. There is a lot of valuable expertise, but also a lot of naivety in dealing with it. Many are not aware that they are a relevant target for espionage, and their cybersecurity is correspondingly inadequate.

Another aspect is the risk of deliberate sabotage by state or state-funded actors, with the main focus here being critical infrastructures such as financial service providers, telecommunications and energy suppliers. Since the war in Ukraine began, this dimension has gained significantly in importance. It is central that companies examine their own cybersecurity in relation to state threats.

"It is central that companies examine their own cybersecurity in relation to state threats."

What consequences can a successful hacker attack have on an organisation?

After an incident, the functioning of an organisation can break down partially or completely for months. It can quickly threaten an organisation's existence, even for larger players. Additionally, in the event of a ransomware attack, organisations often no longer know which systems and data they can trust. Even if they pay the ransom, in most cases they have to replace and rebuild their entire IT. No PC remains untouched.

Do you have a specific example of this?

The district of Anhalt-Bitterfeld is a striking case in point. In 2021, the administration was the first local authority to be forced to declare a state of emergency due to a hacker attack. In the first few days of the attack, the administration's ability to act was massively restricted. For example, no social welfare and

75%

say that the threat will continue to increase as long as organisations only try to combat existing dangers and do not anticipate new ones.

564 specialists and managers

Source: F.A.Z.-Institut, Sopra Steria

maintenance payments could be paid out. Normality was not restored until several months later and with help from the federal government.

To what extent does an emergency plan help to minimise damage?

Preparations for emergencies are crucial. It is a classic mistake that companies focus their entire attention on keeping attackers out. No matter how high you build the firewall on the technical side, if an attacker gets into the system through human error, further protection mechanisms have to trigger. Otherwise, the hacker can just walk right in.

Additional resilience is required: The key term here is zero trust security, but very few implement it consistently. In practice, resilience means that IT systems are divided into several segments that can be isolated if necessary. It means that regular back-ups of important data are made to avoid data loss and outages lasting several months. In addition, clear emergency processes and quick access to an incident response team should be guaranteed. With these steps, the consequences can be minimised.

"AI is not just a tool; AI systems themselves can become targets for hackers too."

What will organisations need to prepare for in the future?

Many processes will need a rethink. I have been working in IT security for 30 years. In the beginning, it was a niche topic for IT administrators. While much has changed, many board members still underestimate the significance of cybersecurity for other areas of the business. We need more holistic thinking.

For example, more and more organisations are developing and integrating AI applications into their business processes. However, AI is not just a tool; AI systems themselves can become targets for hackers too. The outcomes of AI applications are already difficult to trace. If an attacker succeeds in introducing bias, the distorted results could lead organisations astray. Manipulated training data or parameters in AI systems present a new potential risk.

But this is just one aspect of future cybersecurity. Organisations must evolve continuously if they want to maintain their current security level. At the same time, it is crucial not to neglect basic protection.

Contacts

Sopra Steria SE
Corporate Communications
Birgit Eckmüller
Hans-Henny-Jahnn-Weg 29
22085 Hamburg
Germany
Tel.: +49 40 22703 0
E-Mail: birgit.eckmueller@soprasteria.com

F.A.Z. Institut
Jacqueline Preußer
Pariser Straße 1
60486 Frankfurt/Main
Germany
Tel.: +49 69 7591 1961
E-Mail: j.preusser@faz-institut.de

F.A.Z. INSTITUT

sopra steria