IT Security Survey

2025

Table of Contents

Introduction

With its IT Security Survey 2025, the eco Security Competence Group has presented a comprehensive analysis of the current state of IT security in Germany. For over fifteen years, the Competence Group has been dedicated to the security of (IT) infrastructures in the Internet industry. Its areas of focus include personnel and organisational aspects of IT security, the protection of IT systems such as servers and networks, the security of mobile communication technologies (e.g. tablets, smartphones and Wi-Fi), as well as issues relating to security management and employee awareness.

In addition to recurring topics, the annual survey also addresses current developments in the field of IT security. This year's survey focused on the impact of the increasing use of artificial intelligence (AI) on the security situation in companies and organisations.

Data for the 2025 IT Security Survey was collected between September and December 2024. A total of 175 IT security experts were surveyed at live events and through online forms.

Oliver Dehning
Oliver Dehning has been Leader of the Security Competence Group at eco – Association of the Internet Industry since 2014.

General Situation

For 2025, 88 percent of the IT experts surveyed assess the general threat situation as high or very high. Around 11 per cent expect the situation to remain unchanged, while only 1 per cent anticipate a decrease in the threat. Compared to last year's results, there has been a slight shift in the assessment: the proportion of those who expect the threat level to increase has declined, while "no change" was mentioned more frequently.

Despite this decline, the perceived threat level remains very high, comparable to that of 2015, but has fallen below the 90 per cent mark for the first time in years. However, there is no evidence of an actual easing of the IT security situation.

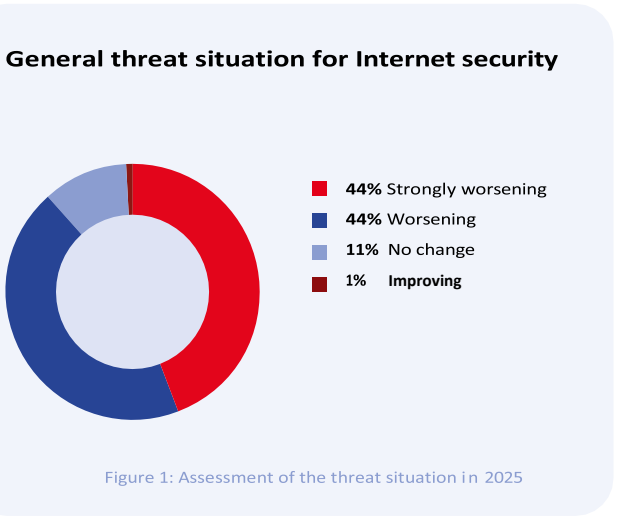


Figure 1: Assessment of the threat situation in 2025

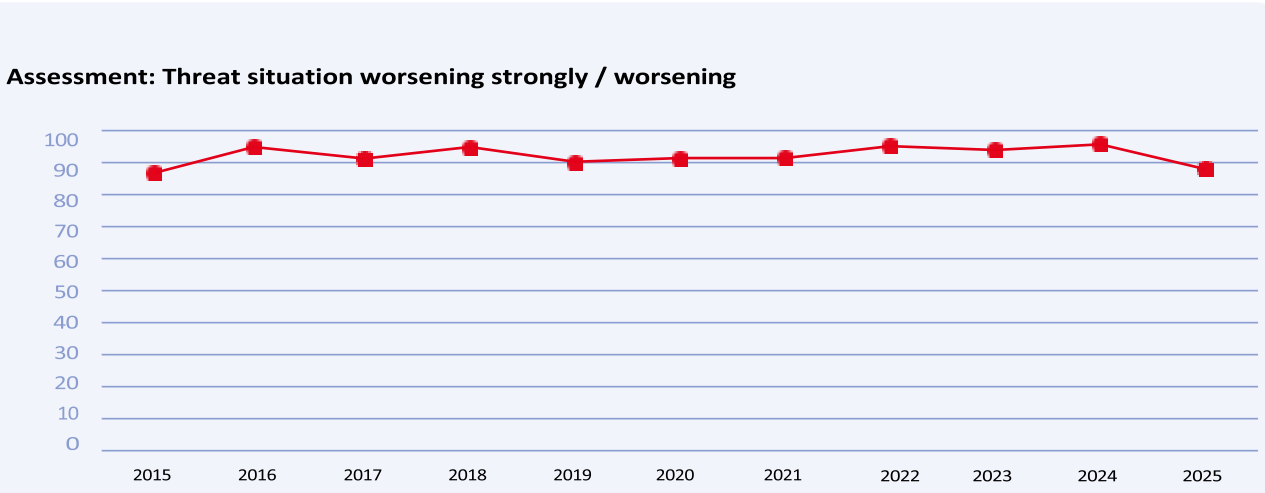


Figure 2: Development of the threat situation 2015-25

The experts surveyed predominantly rate the security of their own companies as stable and at least adequate. Only 12 per cent of participants rate the security of their companies as inadequate. It is striking that the respondents consider their own companies to be significantly better equipped against cyberattacks than the German economy as a whole.

More than half of those surveyed rated the security situation in their own company as "good" or "very good". In contrast, around three-quarters of participants said the German economy as a whole was inadequately prepared for IT security attacks.

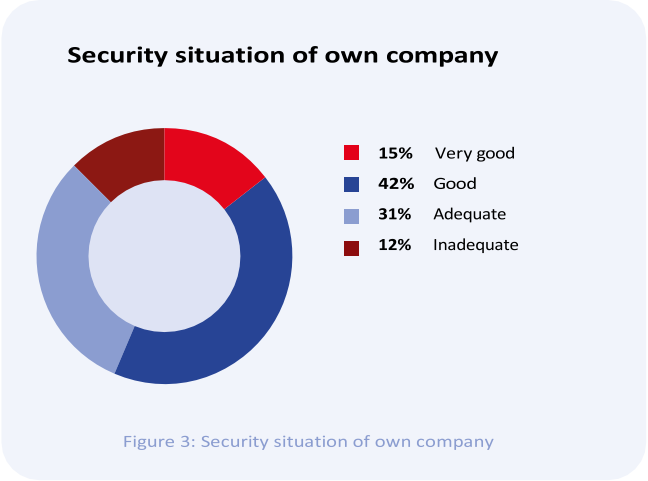


Figure 3: Security situation of own company

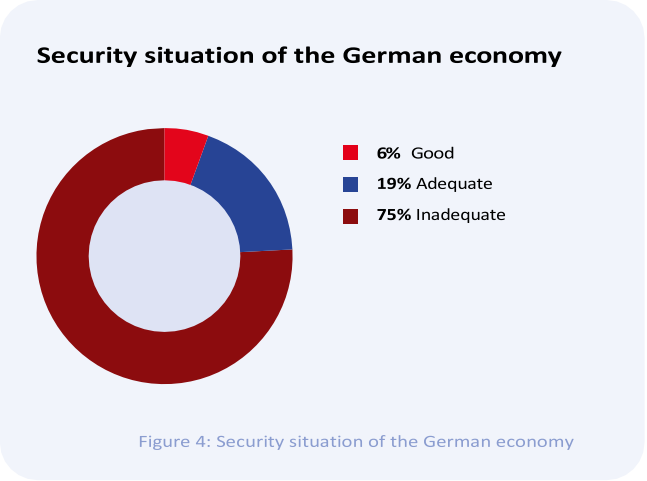
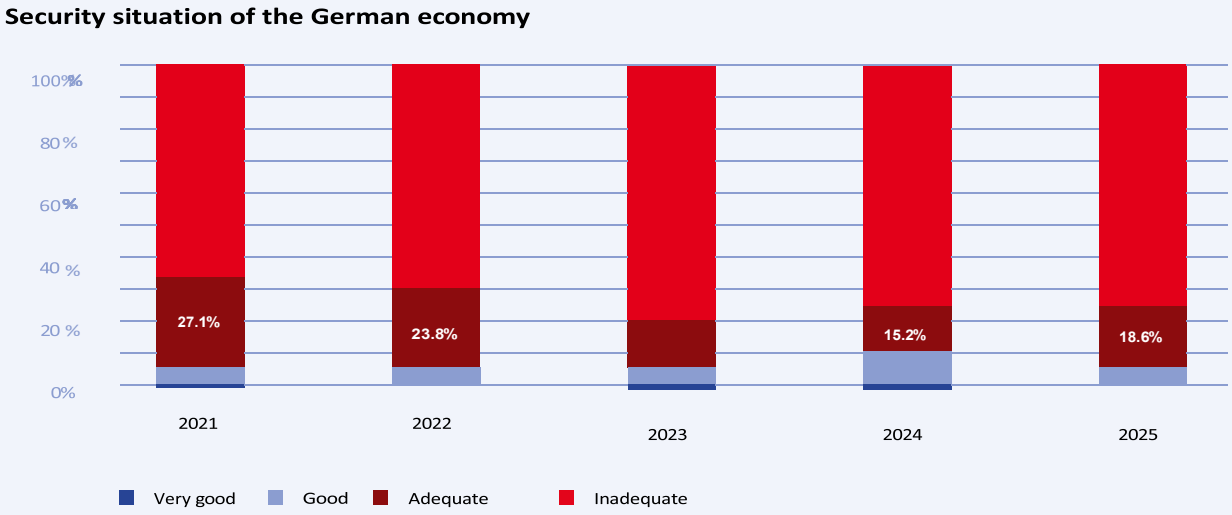


Figure 4: Security situation of the German economy

These assessments have hardly changed over the last three years and point to a continuing discrepancy between individual and macroeconomic risk perception.



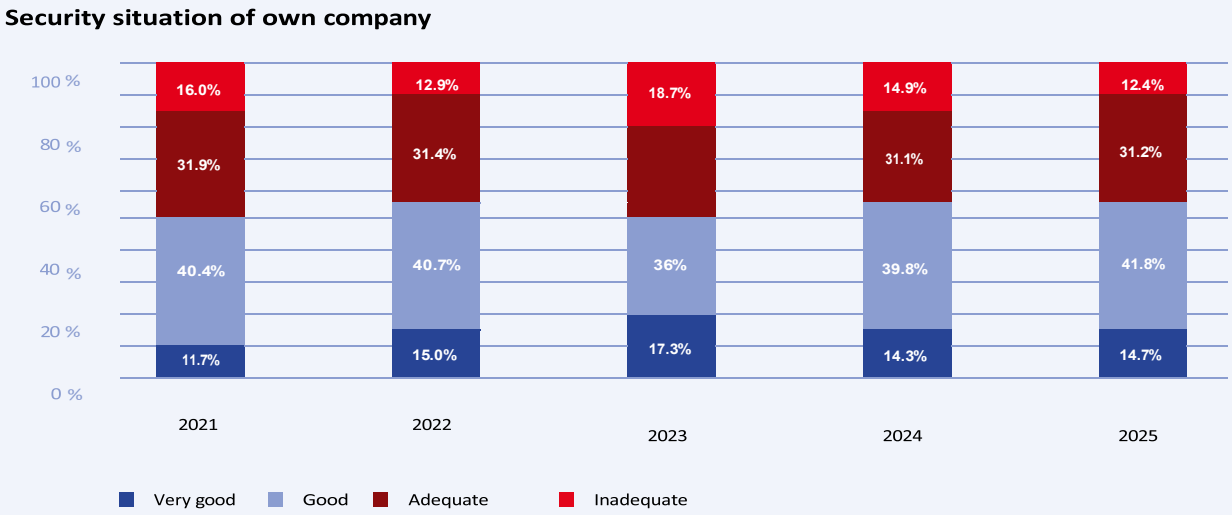


Figure 5: Protection against cybercrime 2021 to 2025

Threat situation still underestimated

"The discrepancy between the assessment of one's own security situation and the security situation in Germany in general shows how difficult it is even for experts to correctly assess the threat," says Oliver Dehning, Leader of the Security Competence Group at eco – Association of the Internet Industry. "Many medium-sized companies are the focus of internationally active cybercrime networks and are unaware of this."

One in six of the companies surveyed had been affected by at least one serious security incident in the past twelve months – 5 per cent had even been affected by several. Compared to the same period last year, there has been a slight increase: in 2024, 7 per cent reported one serious incident and 6 per cent reported several. The current trend indicates that cyberattacks are becoming increasingly widespread, with more and more companies becoming targets.

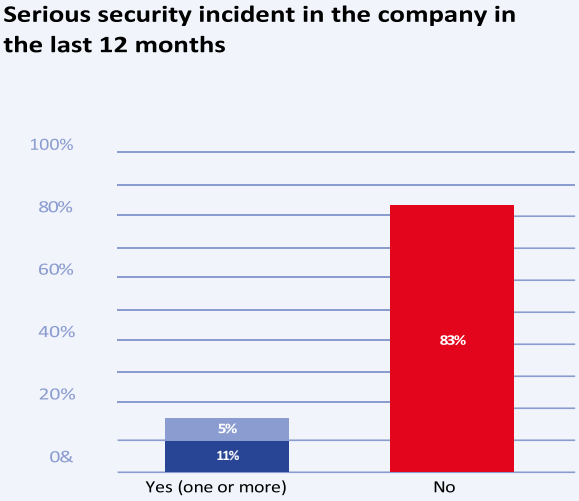


Figure 6: Security incidents in the company

Ransomware remains the most common form of attack on companies, closely followed by CEO fraud. Data theft, website hacking and DDoS attacks are in the middle range.

Around 2 per cent of the companies surveyed discovered an industrial espionage attack last year.

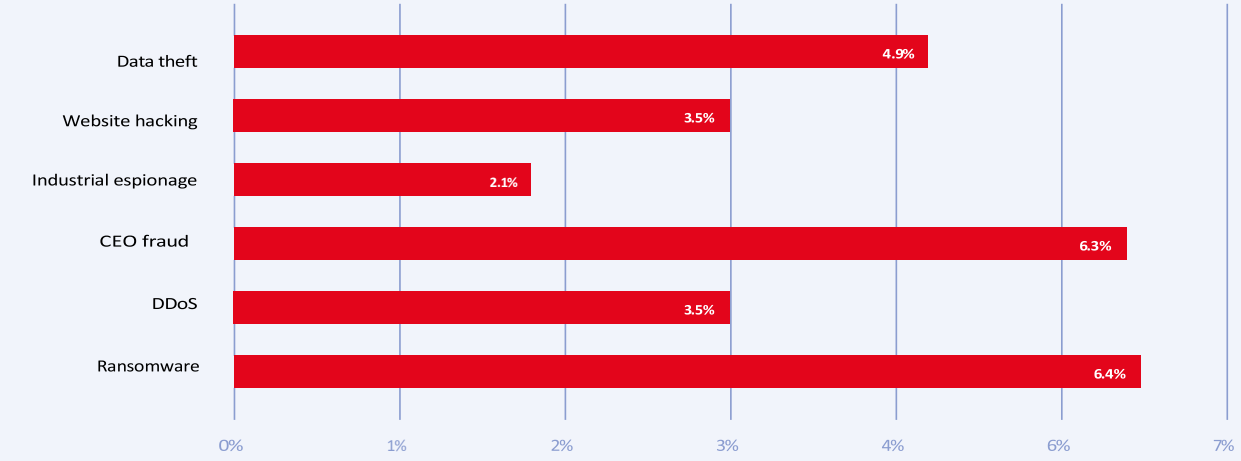


Figure 7: Types of attacks on companies

Compared to previous years, there has been a significant increase in CEO fraud attacks. There has also been a slight increase in ransomware and industrial espionage. Although there has been a slight decline in data theft, this must be viewed in the context of the increasing ransomware threat.

Modern ransomware attacks are no longer limited to encrypting systems and data. Increasingly, sensitive company data is also being copied in the background and transferred to the attackers – with the aim of triggering a second wave of blackmail through so-called double extortion attacks.

What is CEO Fraud?

Explanation of the term

CEO fraud (also known as “boss scam” or “business email compromise”) refers to a form of social engineering in which attackers pose as senior management in order to persuade employees to make fraudulent payments.

Typical procedure

- Information gathering about companies (e.g. via social media, website)
- Fake email or phone call on behalf of management
- Urgent payment request with reference to confidentiality
- Transfer to a fraudulent account

Objectives

- Unnoticed transfer of large amounts of money
- Access to confidential company data

Risk factors

- Lack of security processes for payment approvals
- Lack of awareness among employees
- Public information about company structures

Protective measures

- Training and awareness: Make employees aware of social engineering
- Dual control principle: Establish binding approval processes
- Communication rules: No payment instructions by email without confirmation
- Technical measures: SPF, DKIM, DMARC for email authentication

CEO fraud causes billions in losses worldwide every year. Prevention is significantly cheaper than the potential loss.

Security incidents year-on-year

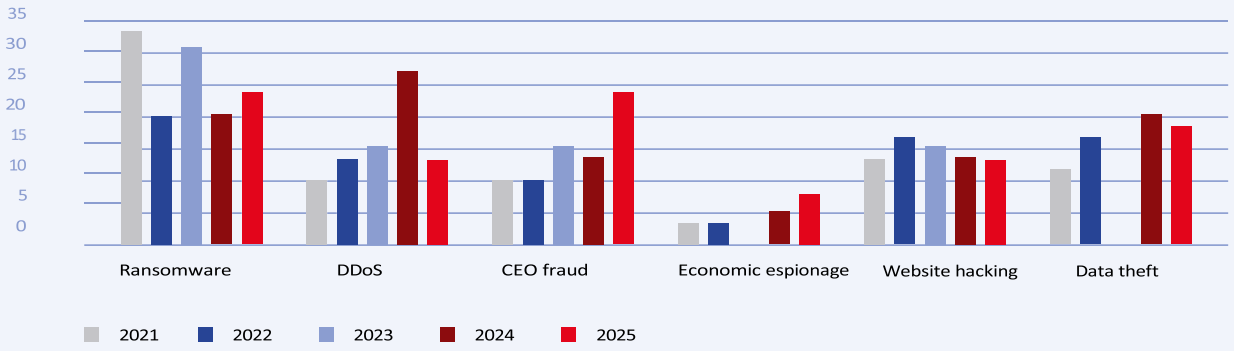


Figure 8: Security incidents and type 2021 - 2025

The economic damage caused by cyberattacks is often difficult to quantify. For many companies, it is a challenge to fully grasp the actual impact. In addition to the immediate defence and forensic investigation of the incident, typical cost factors include the restoration of affected systems, the closure of vulnerabilities, operational expenses and any losses due to data leakage. These costs can be incurred internally or by external service providers – for example, for IT forensics, legal advice or communication. In some cases, fines or reputational damage may also be incurred.

Fortunately, three quarters of the companies surveyed stated that they had not suffered any direct damage as a result of the incident. However, it can be assumed that at least some effort was required to process and secure the data after the attack. In contrast, around one in four companies reported damage, with 6 per cent reporting significant impacts. In the previous year, 79 per cent stated that they had not suffered any damage.

Only 4 per cent reported serious damage at that time. Despite the fundamentally sound cybersecurity position of many companies, the rising number of incidents – both in terms of general damage and particularly serious incidents – indicates a slight deterioration in the overall situation.

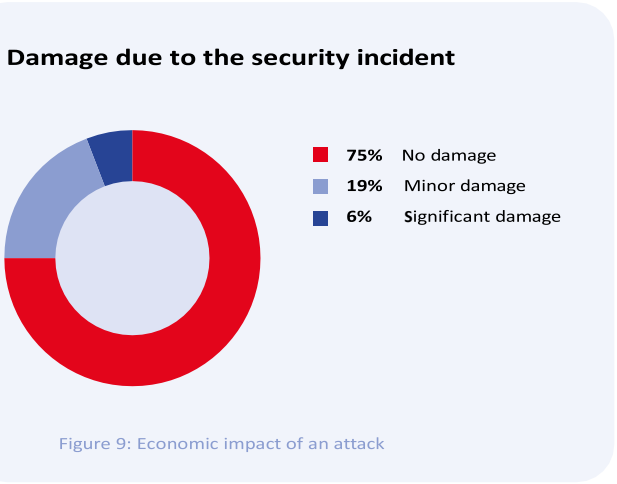


Figure 9: Economic impact of an attack

Just under half of the companies surveyed – predominantly IT-savvy companies – were able to deal with cyberattacks using internal resources. In around one in five cases, external support was called in. In an emergency, however, decisive and swift action is required: companies should not hesitate to seek specialist help at an early stage and to involve the relevant public authorities as they can provide important support.

Last year, around a quarter of all cases involved law enforcement or data protection authorities. It is worth noting that no ransom was paid in any of the cases analysed – in line with the current recommendations of security authorities and experts.

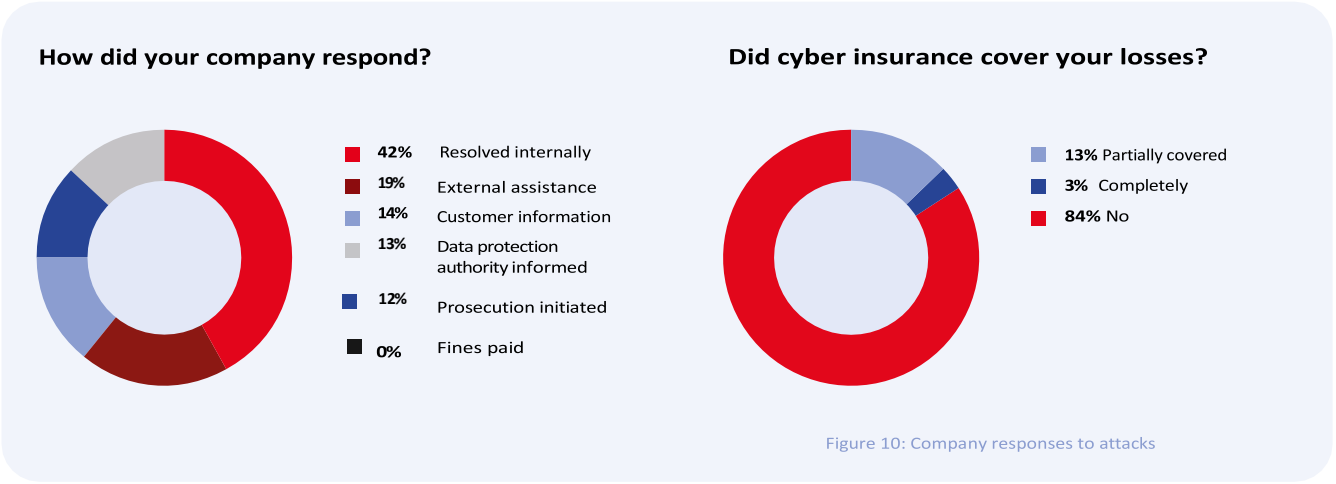


Figure 10: Company responses to attacks

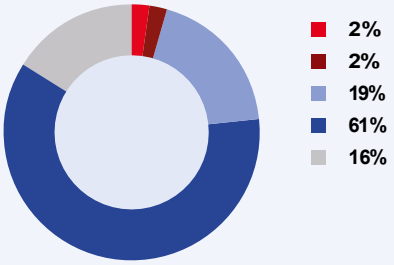
One option for risk management is risk transfer. Financial risks, in particular, can be covered by taking out cyber insurance. In 16 per cent of the survey, it was stated that the damages incurred were at least partially covered by cyber insurance

However, a more nuanced picture emerges when compared to the reported damage cases: in some cases, damage that was covered by insurance was not subsequently recognised as such.

Cyber Resilience / Prevention

A reactive approach to security issues is no longer sufficient. A comprehensive security strategy must also include preventive measures. Employee involvement is a key success factor here. Although they're often considered the 'weakest link', they play a vital role in security. Around 60% of respondents say they provide regular training for employees. Around 19% rely on irregular training, while only 2% do not provide any training at all.

Do you train and raise IT security awareness among your employees about?



Do you train and raise awareness among your employees regarding IT security?

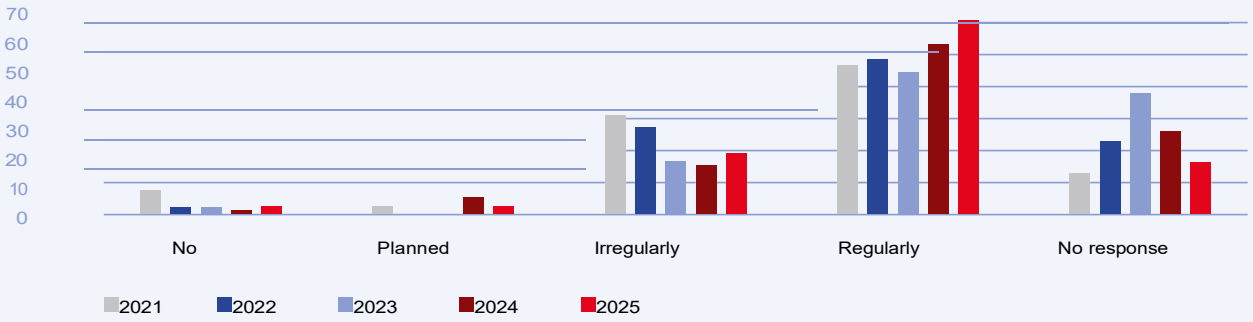


Figure 11: Employee training

Compared to the previous year, there has been a significant increase in both regular and irregular training courses. It can be assumed that many companies that were still in the planning phase last year have now implemented these measures. Encouragingly, the proportion of companies that completely forego this important tool has fallen to a very low single-digit percentage over the past five years.

In addition to training courses to raise employee awareness, emergency planning is currently one of the key security issues for the companies surveyed. Those who have access to prepared processes and relevant information in the event of damage are in a position to significantly limit the impact of an incident. Emergency plans are an essential building block for greater cyber resilience. Around 60 per cent of companies have defined internal processes to defend against cyberattacks and already established emergency plans – a further 16 per cent are planning to introduce them.

Has your company established internal processes or an emergency plan for the event of an IT security incident?

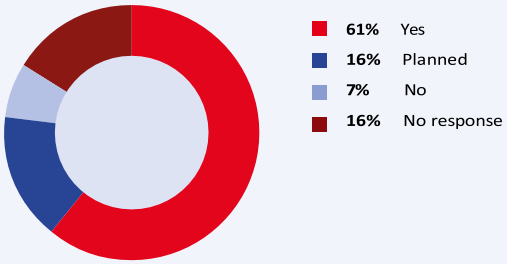


Figure 12: Internal processes and emergency plans

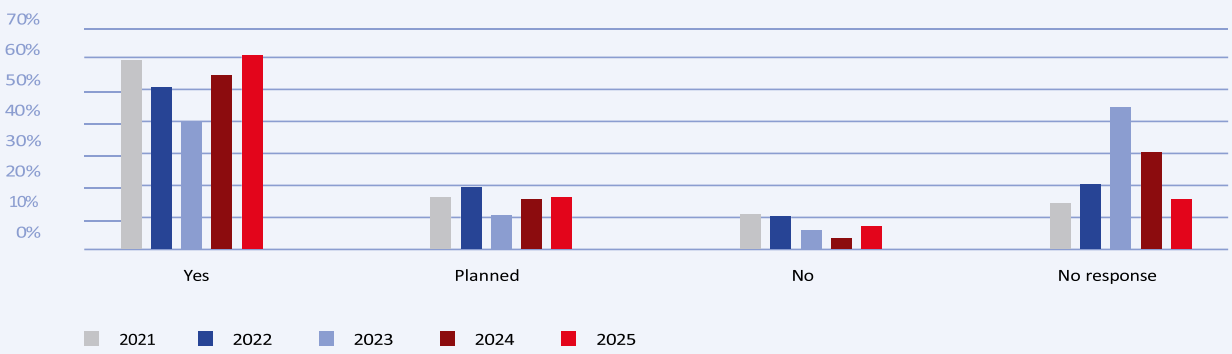


Figure 13: Internal processes and emergency plan

A five-year comparison reveals a mixed picture in the area of emergency management: after a significant decline in 2022 and 2023, the number of companies implementing appropriate measures has reached its highest level to date in 2025. At the same time, in 2025, for the first time in years, more companies stated that they have no defined processes for emergencies – even though this proportion remains at a very low level of just under 7 per cent. While numerous products and providers are available in the area of employee awareness, the development of an individual emergency plan is much more complex.

Investments in IT security are essential to strengthen resilience against cyberattacks. Half of the companies surveyed plan to increase their IT security budget, while around a third will keep it unchanged. Only around 2 per cent expect spending to decline.

Compared to previous years, there has been a steady increase in the proportion of companies increasing their security budgets. Although the record level of 2022, caused by the Covid-19 pandemic and the rise in mobile working, has not yet been reached again, the continuing increase in investment – in response to the growing threat situation – is a positive sign.

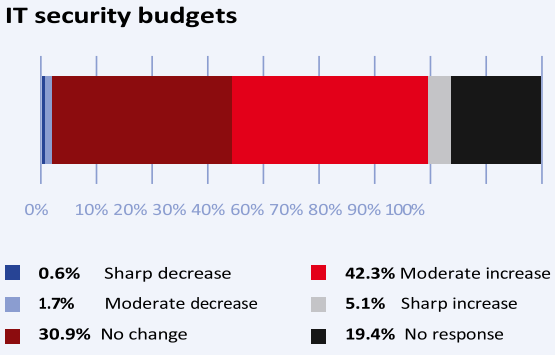


Figure 14: IT security budgets

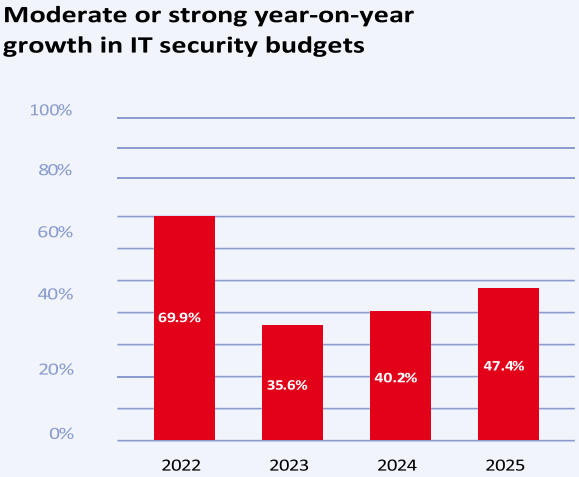


Figure 15: Budgets in annual comparison

Current Topics

The annual survey on the most important security issues for the coming year allows for a high degree of comparability of results over time. At the same time, the authors of the study draw on current events to expand the list of questions in a targeted manner, thus taking into account changing political and societal conditions.

One of the most significant trends currently having a direct impact on IT security is the rapid adoption of artificial intelligence (AI). This technology has the potential to be used by both attackers and defenders. Over 93 per cent of the companies surveyed assume that that AI will further exacerbate the threat situation. At the same time, around 40 per cent of companies are already actively using AI for tasks in the area of IT security.

The main opportunity offered by the use of AI lies in faster detection of and response to threats, for example through automated anomaly detection or support in evaluating large amounts of data. On the other hand, there is a risk that attackers will use AI to carry out more targeted phishing attacks, deepfakes or automated vulnerability scans – at a speed and quality that challenges traditional protection mechanisms.

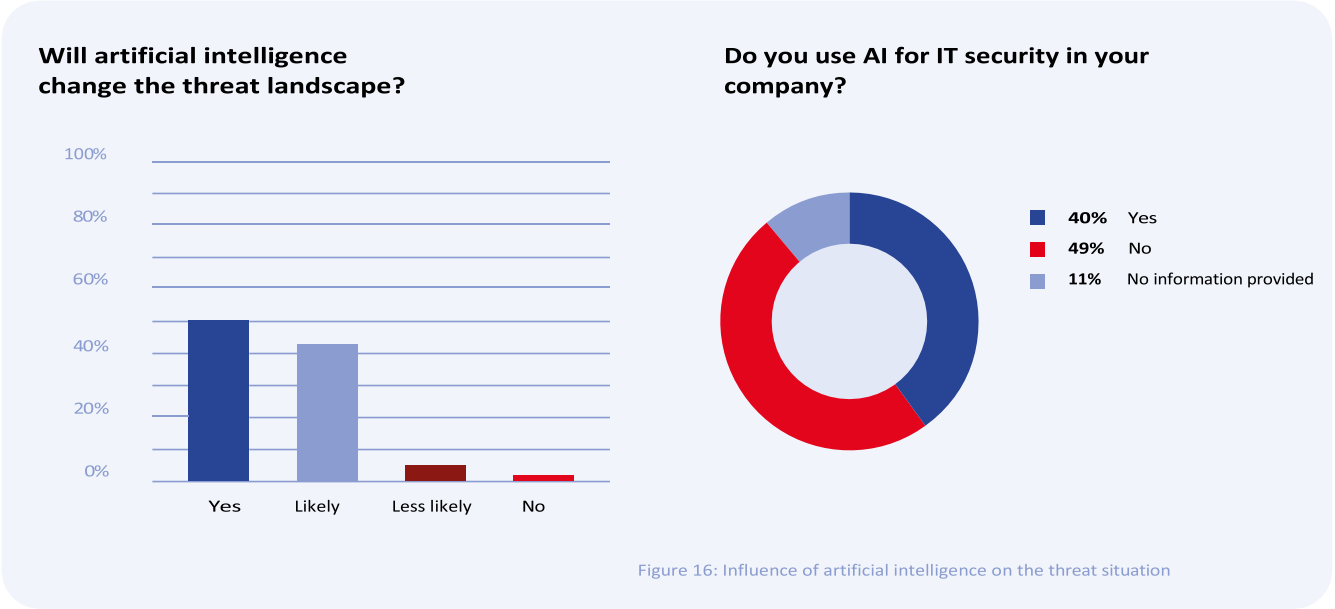


Figure 16: Influence of artificial intelligence on the threat situation

Security issues for 2025

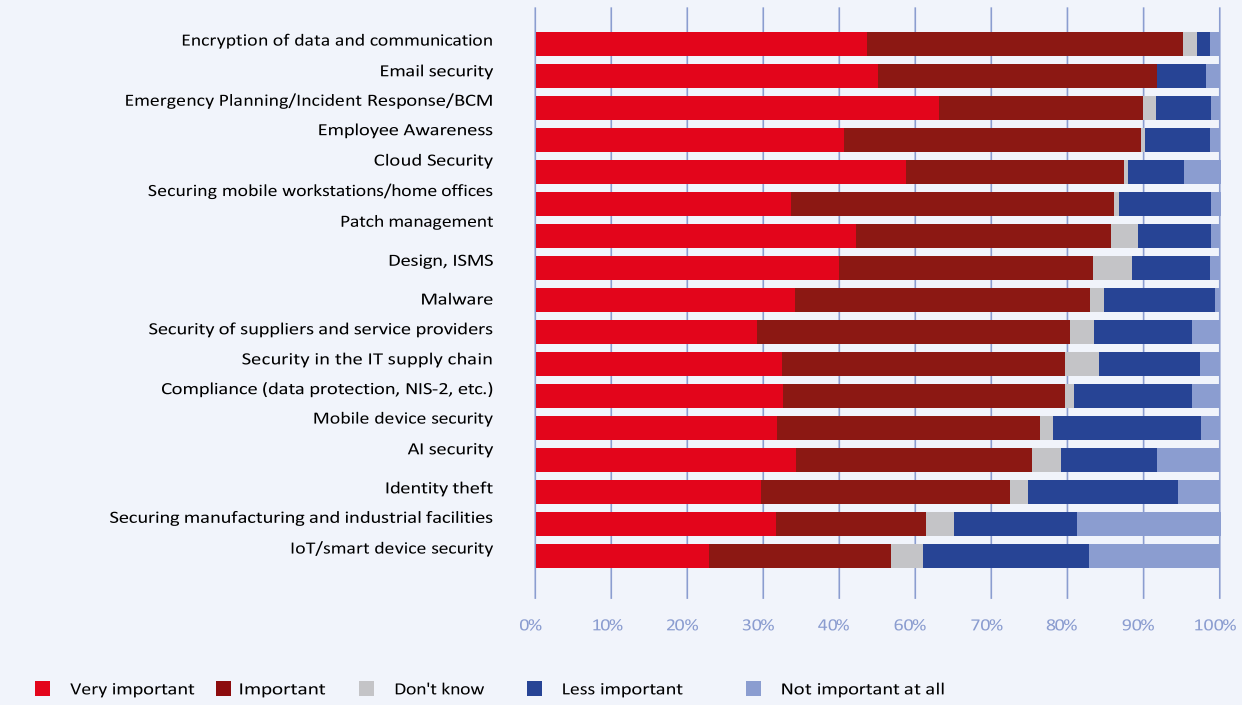


Figure 17: Security issues in 2025

Encryption and email security occupy the top spots among the most important IT security topics in the 2025 survey. Encryption has been a constant focus in recent years and is indispensable in view of increasing cloud usage, international data flows and growing regulatory requirements, such as the EU NIS2 Directive.

Email security has taken a big leap forward. Phishing attacks are becoming even more targeted and credible through the use of artificial intelligence (AI). Thousands of genuine deepfake emails or automatically generated social engineering campaigns make it increasingly difficult for employees to distinguish legitimate messages from fraudulent ones. This is also underlined by the high proportion of CEO fraud attacks.

Close behind are emergency planning and employee awareness, both of which were also among the top priorities in previous years. Emergency planning is becoming increasingly important due to the rise in ransomware attacks and targeted attacks on critical infrastructure. Companies must be able to remain operational even in the event of a successful compromise – not least in order to be able to comply with regulatory reporting requirements quickly and in a structured manner. Employee awareness is more important than ever in light of increasingly sophisticated attack methods. AI-generated phishing emails, deceptively real fake identities and social engineering tricks require growing awareness at all levels of the company – from reception to the executive suite.

IT security requirements are changing. In your opinion, what are the strongest drivers of change over the next five years?

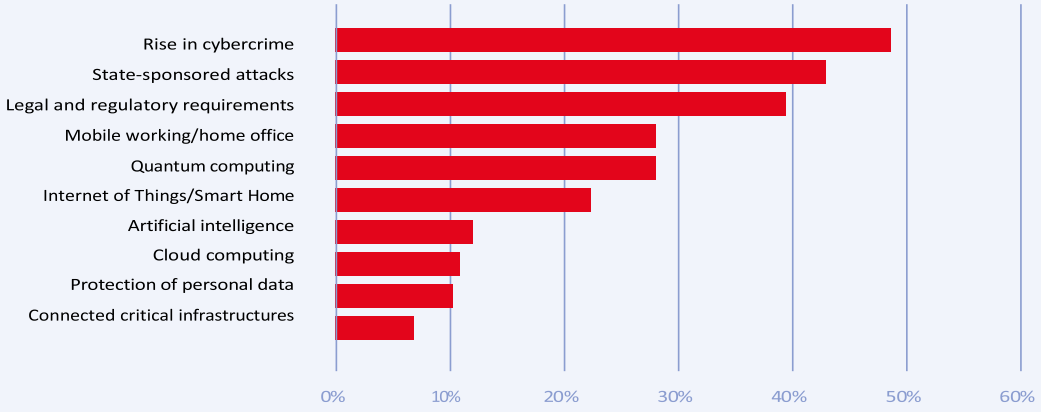


Figure 18: Drivers of change in the area of cybersecurity

The rise in cybercrime continues to be seen as the strongest driver for spending in the area of IT security in the coming years.

As in the previous year, the issue of state-sponsored attacks has also made significant gains. It is becoming increasingly clear that international conflicts are being fought not only on a physical level, but also increasingly on a digital level. Cyberattacks as a means of geopolitical confrontation no longer affect only governments, but also critical infrastructure and companies.

Respondents ranked regulation in third place. In view of current developments such as the NIS2 Directive, the European Cyber Resilience Act (CRA), the Digital Operational Resilience Act (DORA) for the financial sector and other national legislative initiatives, this assessment comes as no surprise. Companies are under increasing pressure to implement regulatory requirements at an early stage and to align their security strategies accordingly.

Drivers of change 2021–2025

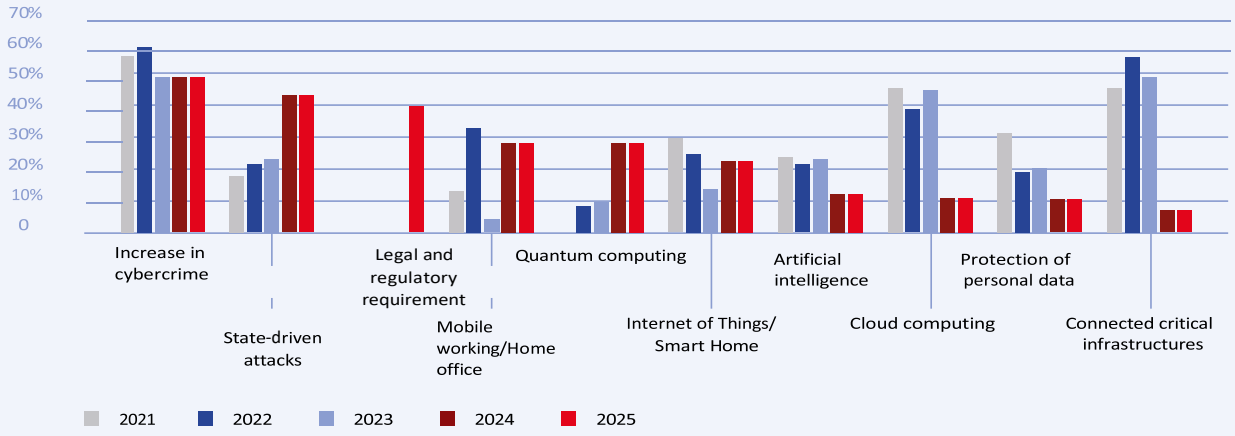


Figure 19: Drivers of change in a year-on-year comparison from 2021 to 2025

Conclusion

The results of the survey make it clear that the IT security situation remains tense. Organised cybercrime and state-sponsored attacks continue to increase and are increasingly targeting companies and public infrastructure. Against this backdrop, it is evident that cybersecurity must be an integral part of every business decision, rather than a marginal issue. This responsibility lies with company management and should not be left solely to the IT department.

At the same time, however, the survey also shows that companies are not defenceless against the growing threats. By making targeted investments in IT security, creating effective emergency plans and raising employee awareness, companies can minimise risks and significantly limit the potential impact of attacks. Companies that act early will not only strengthen their own resilience, but also earn the trust of customers, partners and regulatory authorities.

Your contacts at eco for security issues:

Cornelia Schildt
Senior Project Manager IT Security
eco – Association of the Internet Industry

Cologne Office
43h Lichtstrasse
50825 Cologne
Germany

Telephone: +49 (221) 7000 48 – 175
Email: sicherheit@eco.de

Michael Weirich
Project Manager IT Security
eco – Association of the Internet Industry

Cologne Office
Lichtstrasse 43h
50825 Cologne
Germany

Telephone: +49 (221) 7000 48 – 193
Email: sicherheit@eco.de

eco – Cologne Office

Lichtstrasse 43h
50825
Cologne
Germany

+49 (0)221 700048-0

sicherheit@eco.de
www.eco.de