sosafe

Human Risk Review 2023

Expert insights and strategies for navigating the European cyberthreat landscape

> “ We need to move cyber security to where people are, make awareness permeate all domains of our lives, and act on the fusion of cyber and business.

Dr. Niklas Hellemann
CEO at SoSafe

Editorial

It almost feels needless to say, but it has never been truer than now: The cyber threat landscape is tense and characterized by an incredible speed of innovation.

What we have seen in past years, and 2022 in particular, can only be described as fast-forward evolution. Global tension, geopolitical conflicts, and constant disruptions in business have created a volatile world, massively increasing the attack surface for cybercriminals and leading them to further professionalize their business models. At the same time, technological advancements like generative AI tools have democratized the "art of cybercrime." The result: We see ourselves confronted with countless potential attackers today who have the tools to not only maximize their attacks' reach but also their success rates.

At SoSafe, we have warned for years that cybercriminals might use sophisticated AI-based tactics like deepfake phishing for large-scale attacks. The emergence of more readily available generative AI tools has now brought this possibility into immediate reach. In a small study, we recently found that phishing emails can be created 40 percent faster with the help of ChatGPT – a foretaste of how criminals will use AI to scale their business.

I think we can agree that information security is not a domain where we should rest on our laurels. By definition, security needs to constantly develop and adapt. Adopting new technologies to stand better protected against novel attack tactics is one side of that. But if we can be sure of one thing, it is that attackers will continue to try (and often succeed in) finding ways around even the most sophisticated technological barriers. They are well aware that their biggest chance of success is playing with human emotions. A fact that major breaches like the ones on Uber or Reddit have recently shown. Social engineering is the source that does not cease. The good news is that it is a risk we can very effectively minimize with the right methods.

That is why, perhaps not surprisingly, awareness building now leads the list of security priorities among the organizations surveyed for this report. One of the main influencing factors of whether they can adequately invest resources into their security culture is the extent to which top management is aware of cyber risks. In some respects, that is what we set out to do yearly with our Human Risk Review: We are convinced that our data can bring new perspectives. We are sharing first-hand insights into cybercriminal tactics and the role the human factor plays in that context but also provide resources to enter conversations about information security and awareness, in particular.

A deep dive into data from our platform, an extensive survey among European security professionals, and conversations with C-level experts from various industries confirmed: We need to move cyber security to where people are, make awareness permeate all domains of our lives, and act on the fusion of cyber and business. It's the only way out of the billion-dollar cybercrime misery we are currently in. Just as fast as the threat landscape is evolving, so must we.

Dr. Niklas Hellemann
CEO at SoSafe

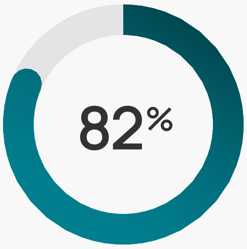
Contents

Executive summary

The threat landscape is tense

1 in 2

organizations experienced a successful cyberattack in the past 3 years.



of organizations don't expect the situation to ease in the next year, either.

> We're living in the age of digitization. Nearly everything is interconnected and can be hacked.
>
> **Dr. Katrin Suder**
> Strategy Expert (digital technologies, business & politics)

Top 3 tactics in successful attacks

1. Malware
2. Phishing
3. Ransomware

Top 3 departments targeted

1. IT
2. Finance
3. Security

And cybercrime is booming – some of the reasons:

3 in **4**

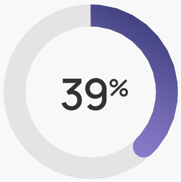
security professionals say their organization's cyber risk has increased due to **geopolitics**, **AI**, and **remote work**.

> The number one challenge in the cyber security industry right now is burnout: There's too much data, too many cases, and not enough time.

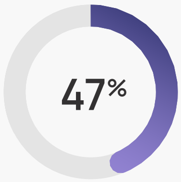
Stéphane Duguin
CEO at CyberPeace Institute

8 in **10**

security professionals say their organization's security is increasingly **dependent on the security of their partners and suppliers**.



In case of a successful ransomware attack **more than a third of companies** paid the ransom.



Among smaller companies, **almost half** were forced to pay.

The dry-powder hypothesis in cybercrime

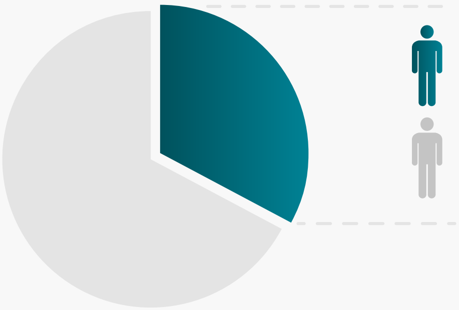
> Cybercriminals have had some very advanced technology at their disposal for quite a while, like voice cloning. Yet, we haven't seen sophisticated social engineering at scale in the wild. One explanation: The simple stuff still works. But with leaks of large language models and exponential development in generative AI across the board, this will very likely change.

Dr. Niklas Hellemann
CEO at SoSafe

80 % of security experts see social engineering and phishing as major risks to their organization:

1 in 3

users click on harmful content in phishing emails, and out of these...



1 in 2

users proceed to enter sensitive information.

In an intensifying tense threat situation, social engineering techniques that leverage pressure or authority to provoke

negative emotions

are increasingly successful.

> We're receiving harmful emails more frequently, and each new wave is more intense than the last.

Sascha Czech
CSO at Uniklinikum Münster

> Many users are less focused when working from home, and it's a more relaxed environment. They mix a lot of personal activities into their workflow, resulting in inattentiveness.

Dr. Stefan Lüders
Computer Security Officer at CERN

Digital natives are

↗ 65 %

more likely to click on phishing emails than older users.

Outlook: Are companies prepared?

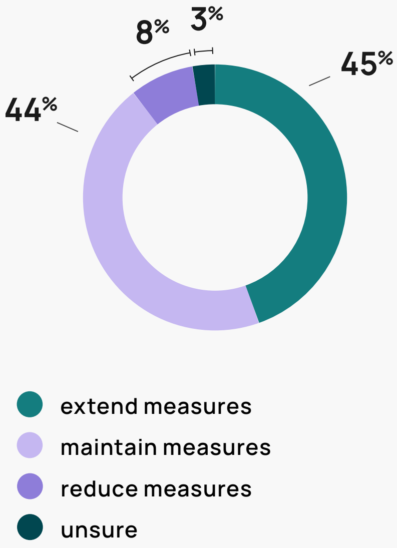
> I often hear the old saying, 'If it's not broken, don't fix it.' But when an attack does happen, the consequences can be severe.

Thomas Tschersich
CSO at Deutsche Telekom

Top 3 priorities for security professionals

1. Improving employees' security awareness
2. Identity and access management
3. Securing hybrid work

9 in 10 organizations plan to maintain or increase their awareness measures in the upcoming year.



> Everything that I can cover through employee awareness makes me more resilient as a company. I save on time, money, and stress, and avoid more risks.

Thomas Schumacher
Managing Director at Accenture Security

The biggest levers for greater security awareness impact according to security professionals:

1. Awareness measures via communication apps
2. Personalized learning
3. Program customization

Methodology and data sources

Survey among security professionals

For this extensive survey on the state of cyber security in organizations, we partnered with Censuswide, an international market research consultancy headquartered in London. More than 1,000 security professionals from 6 European countries (United Kingdom, Germany, Austria, Switzerland, France, and the Netherlands) were surveyed in February 2023. The size of the organizations ranged from 10 to more than 5,000 employees, across all industries.

SoSafe platform data

For the analysis of different social engineering techniques, 8.4 million simulated phishing emails from 3,000 customer organizations from the SoSafe Awareness Platform were analyzed anonymously, giving exclusive insights into human risk levels and the success of different attack tactics in organizations.

Phish Test

In this study on general phishing awareness, over 9,000 simulated phishing emails were sent to users who signed up in 2022. Participants were sent three simulated attacks over the course of a week – all classified as moderate in terms of complexity. The users had to identify these emails. If they clicked, they were forwarded to contextual learning resources.

Cybercrime as the no. 1 business risk – and what human behavior has to do with it

If there is one thing security experts unanimously agree on, it is that cybercrime is a major business risk for companies around the world. For several years, industry reports like the Allianz Risk Barometer and IBM's Cost of a Data Breach have shown that neglecting security precautions can have devastating effects on businesses – both in terms of financial losses and damage to their reputation.

No.1
business risk

Cyber incidents are the greatest risk for companies

Source: Allianz Risk Barometer 2023 [1]

$4.35 million

Average data breach cost

Source: IBM Cost of a Data Breach 2022 [2]

Numerous developments, from geopolitics and artificial intelligence to staff shortages in IT and security, seem to worsen the situation further. And, as cybercriminals become increasingly sophisticated in their schemes and adapt them to these technological and social changes, many organizations struggle to keep up and find the right tools to protect themselves effectively.

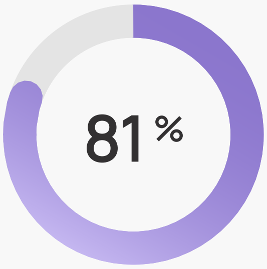
1 in 2

companies have experienced a successful cyberattack in the past 3 years – and 64% assess their risk of falling for another one as high.

The outlook for the upcoming months and years does not necessarily look bright. The security experts surveyed for this report were clear: 82 percent don't expect the situation to ease in the upcoming months.

The unifying element

Despite the complexity of today's threat landscape, there is a common thread: the human factor. No matter how strong technical protection measures are, people still fall prey to clever social engineering tactics. To put this into perspective: Phishing – a prime example of social engineering methods – ranks second on the list of the most successful cyberattack tactics. Only malware and ransomware are ranked similarly high by security professionals in terms of their risk potential. Interestingly, these two attack types also often start with some sort of human interaction, such as an employee unknowingly giving away credentials.



of security professionals say phishing and emotional manipulation of employees pose a significant risk to their organization

This highlights how social engineering techniques remain the top choice for cybercriminals, and they keep innovating in that area because they are simple and cost-effective tools to find a way into company systems. The good news is that organizations can take steps to effectively strengthen their human layer as part of their overall information security and strategy.

Humans as the first and last line of defense

When companies turn the rhetoric around and leverage human behavior and psychology just as much as cybercriminals currently do, they can turn their employees into gatekeepers of their assets and security.

> **Everything that I can cover through employee awareness makes me more resilient as a company. I save on time, money, and stress, and avoid more risks.**
>
> Thomas Schumacher
> Managing Director at Accenture Security

The Reddit incident[3] illustrated this all too well: Early in 2023, the company suffered a data breach, exposing internal documents and source code, caused by a highly sophisticated phishing attack. But what followed was a strong example of a mindful employee and a strong security culture. The employee who clicked on the phishing email realized the attack immediately and promptly reported it to the internal security team, who were then able to restrict the cybercriminal's access. Had they not, the story could have ended differently.

Our greatest chance of countering cybercriminals' attacks is to beat them at their own game – understanding and focusing on our behavioral patterns so that we can proactively respond. In this report, we take a closer look at the state of cyber security and awareness, with a particular focus on Europe, and explore how organizations can leverage insights from behavioral science to protect themselves in the increasingly complex threat landscape we find ourselves in today. We let data speak as much as experts from various industries who share what they think are the biggest priorities for security professionals today.

[1] **Allianz (2023).** Allianz Risk Barometer.

[2] **IBM (2022).** Cost of a data breach 2022. A million-dollar race to detect and respond.

[3] **The Hacker News (2023).** Reddit Suffers Security Breach Exposing Internal Documents and Source Code.

> We're living in the age of digitization. Nearly everything is interconnected and can be hacked.

Dr. Katrin Suder
Strategy Expert (digital technologies, business & politics)

Dr. Katrin Suder is one of the most renowned strategy experts at the interface of digital technologies, business, and politics. She advises different companies, including DAX-listed corporations and large US companies. The physicist and neuro-informatics specialist, who holds a doctorate in artificial intelligence, can draw on many years of experience in politics and business: Until 2021, she headed the Digital Council under Angela Merkel's federal government. From 2014 to 2018, she was State Secretary in the Federal Ministry of Defense. She worked at McKinsey for 14 years, most recently as a director. She holds mandates on German and international supervisory boards, including the board of Cloudflare.

At our Human Firewall Conference, you said that the one thing that keeps you up at night is cyberattacks. Why is that?

Cyber is a dangerous military tool but also a very effective and cost-efficient weapon for criminals because attackers can usually perform their attacks undetected. It's not impossible to find the culprit, but it is extremely time intensive. It's also incredibly affordable if you compare it to, say, a fighter jet. It comes with a low personal risk, too, as nobody has to risk their lives – but this doesn't change the fact that cyberattacks can be potentially devastating. When I was at the Federal Ministry of Defense, the question of security started to increasingly concern security in cyberspace, and as a result we added cyber as a new dimension to our defense strategy. Cyber incidents are one of the greatest risks that I see when working with companies now. Companies are constantly being hacked. The question isn't if you will be attacked, but when, and how quickly you react and how you handle the situation.

The geopolitical situation is becoming increasingly unstable and fragmented. What effect is this having on the dangers already present in cyberspace?

Cyber is a geopolitical instrument of power, and a new attack vector that states use to pursue their own ends. Our new world order has resulted in a continued decrease in general regulatory forces, while national interests become more prevalent, such as espionage or attempts at aggression.

States are investing in weaponized technology by investing in cyber, allowing them to make a small investment with devastating effects. It's not just about data and money, but sometimes even human lives are on the line.

In the current circumstances, is the spike in cyberattacks exclusively (geo)politically motivated?

No, it's not exclusively politically motivated. Many cyberattacks are conducted by parastatal actors, similar to soldiers who aren't allegiant to one particular country. They aren't bound by any laws, you can't hold any specific countries accountable, and you can't claim that they've breached any sort of conventions, and that's what makes the situation so unbelievably complicated. In our new world order, where strong national interests play a major role, these structures can continue to grow. Parastatal hackers are using geopolitical developments to make a profit, such as by supporting political interests or by selling stolen data for massive sums. Geopolitics fuel cybercrime in that geopolitical crises are followed by a rise in not only politically but also criminally motivated cyberattacks.

What other developments are having an impact on our cyber security?

We're living in the age of digitization. Nearly everything is interconnected and can be hacked. Digitization has also made technology more important, and this high level of technologization is opening up new doors for attackers.

How does this affect our critical infrastructure? Power plants didn't use to be online, so does that still apply if we consider decentralized energy distribution?

Of course, there will always be isolated areas that don't rely on the Internet, like for example the German armed forces have. But critical infrastructures are becoming more interconnected, which concerns me. People are increasingly being attacked and manipulated directly at an alarming rate, and these people could in turn have access to isolated networks. There are critical infrastructure legislation and ordinances that aim to regulate this area, but if you look at the decentralized supply network – small, municipal providers, for example – it's harder for them to protect themselves. They lack the financial resources and the personnel to set up the appropriate IT systems.

Can we even maintain an overview of all these developments in the world of cyber security?

People often say that everything in cyber space is new and we've never seen it before. But that's not true: The principles, like safety and security, are the same, password protection is as easy as washing your hands, and so on. I think it's important that we don't act as though everything in the digital space is new, unpredictable, and uncontrollable. That's untrue and makes you feel powerless.

> “Companies have invested more in technology than in people over the past 10 years. They’ve since come to understand that technology isn’t everything, and that social engineering – especially phishing – is a real problem.

Dr. Katrin Suder
Strategy Expert (digital technologies, business & politics)

Let's start talking about defense. You're on the Advisory Board of Cloudfare. Is cyber security a topic of discussion at the board level nowadays?

Absolutely. It's different from one industry to the next because the less digitized an industry is, the less relevant cyber security becomes. But generally, cyber incidents are considered one of the top risks, in my experience. Not every advisory board has a member who's versed in this topic. It's generational, too, because these boards are generally overseen by people with more life experience and often less experience with digitization and cyber issues. Then there's the fact that cyber is a rat race – it's fast-paced, and you always have to learn and keep up. That is why it is so important to develop new models, such as putting younger people with specific expertise in advisory board positions, even if they have never run a company before, or investing more heavily in trainings. The question we all have to ask here is: How high is your company's cyber awareness, and how can you keep it up to date? Many (especially medium-sized) companies are facing this challenge right now.

Are companies doing enough to protect themselves, especially with regard to the human layer?

Companies can't invest enough in security awareness. They first became aware of the matter of the human layer a few years ago, which is why it's going to take some time for companies to develop their best practices and for them to find a way to keep up with the rat race.

Companies have invested more in technology than in people over the past 10 years. They've since come to understand that technology isn't everything, and that social engineering – especially phishing – is a real problem.

"Technology versus people": A common discussion in information security is what should be prioritized, and how. What's your view of this?

It's an artificial contradiction. We're also not asking whether companies should invest in their factory or their employees. Of course, companies can try to seal up any weak spots with technology and achieve scaling with software, and they should. It is imperative that companies also invest in people.

You mention the rat race in information security. Do companies see cyber security as a one-time training measure? Or have they come to understand that we have to continuously invest in this area?

Phishing affects companies now, and most of them understand that constant diligence is key to resolving this problem. Yet, many are having a hard time and keep working with traditional measures: long PowerPoint presentations, "funny" videos, or rigid, in-person seminars that aim to teach employees about this topic.

But if we look at how much information we have to impart to our employees – in addition to cyber, there are topics like compliance, data protection, ESG – then we need to adopt concepts like gamification and some of the methods used in adult education. A lot of companies are still at square one in that respect.

What questions do advisory boards ask in order to evaluate human and technical cyber security within the company?

We on supervisory boards still aren't fully ready and staffed in this regard. Often, questions and discussions focus on control and processes. But instead, we should become even more involved and ask questions like, "What's the potential for danger in our business model? Which data are located where? How much could a cyberattack harm our business model in the current situation? What are our geopolitical attack vectors? What are our contingency measures?" It seems complicated at first, but it's not. In production, for example, specific questions like the costs of a disruption or error rates are also discussed.

How should companies anchor cyber security as an internal requirement?

Cyber is a classic topic of risk management. Either companies integrate cyber into their risk management processes, or they make it an overlapping issue and establish their own cyber risk assessment. I've seen both of these before, and both can work.

Could cyber be seen as a type of digital tax? And do we have to accept that increasing digitization comes with a growing cost pool?

Of course, we have to price in this new dimension of security. The problem is that insurance premiums have risen for health care (COVID), industrial policy, physical security, energy, and cyber security. Companies consequently have high additional expenses, and EBIT margins are also under pressure because of geopolitical developments. Overall, this means that we're losing wealth because the EBIT margins that aren't earned can't be used for investments, employees, and so on. From a geopolitical perspective, I don't see why these insurance premiums would decrease. The state can't make up for or regulate everything, either, and we're seeing that in real time. This is why I think the tax analogy is misleading in this discussion.

What role should the state play when it comes to cyber issues?

One of the most important roles of the state is investing in modern education, and there's not enough of that for IT. Everybody should learn at least the core fundamentals of cyber security and how to work with data in school. In addition to education, we need functioning (digital) law enforcement as well as more support and contact points, which there aren't enough of in the cyber world.

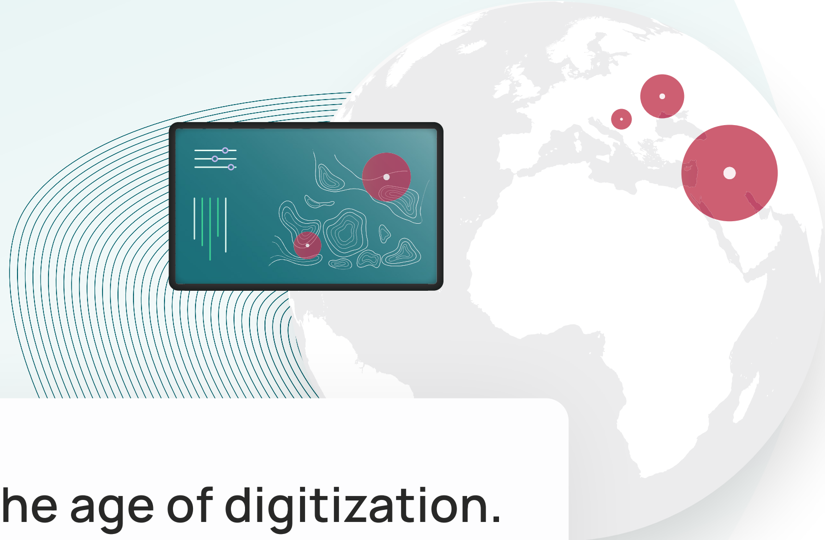
How will we solve the worker shortage in IT?

We have to think well beyond automation in IT if we want to become more secure. We're no longer talking about layoffs and improving efficiency through automation, but rather about whether we can even guarantee cyber security still. The general worker shortage is real, and the consequences are palpable for many, and it's being felt even more in the STEM field. At the same time, demand keeps growing. This situation demands new solutions, such as scaling through automation, and we need to continue to increase our capacity wherever we can, be it with ChatGPT or other technology.

You mention ChatGPT: What influence do you think AI has on cyber security?

I'm less worried about generative AI from a workforce standpoint than from an education and democracy perspective. It's giving us a new educational mandate: If we have more and more generative AI, we have to start addressing how we can categorize innovation or content. How do we evaluate texts? How do we conduct research? These tools' output comes from a machine, and the recipients of the output are lacking a human source that they can assess. Users have to learn how to appraise the answers given by AI tools.

A global battlefield:
How geopolitics are shaping the cybercrime landscape



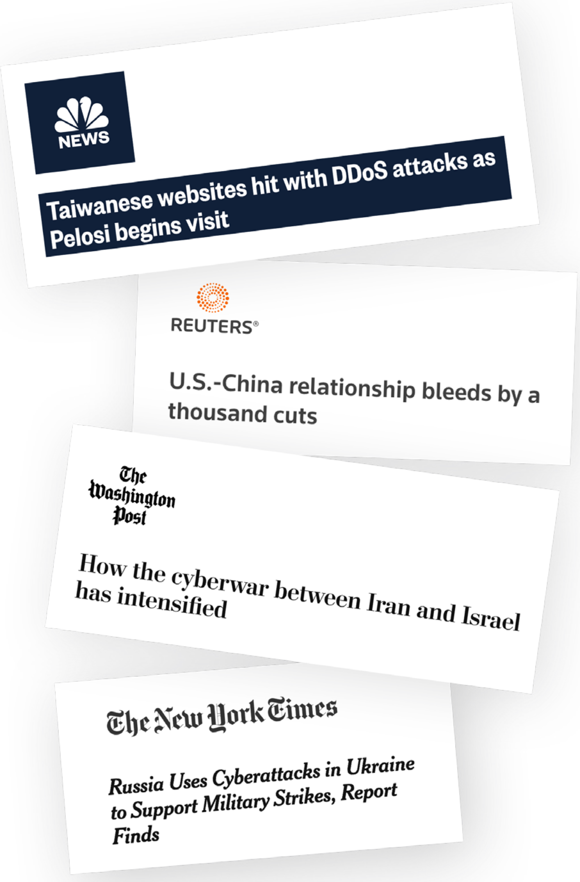
> “We’re living in the age of digitization. Nearly everything is interconnected and can be hacked.
>
> **Dr. Katrin Suder**
> Strategy Expert (digital technologies, business & politics)

Dr. Suder’s quote highlights a momentous truth about our modern world: The rapid advancement of technology and the increasing interconnectedness of our digital devices and systems have led to unprecedented opportunities for communication, trade, and innovation – but it is also putting our cyber resilience to the test.

The **interplay of digitalization and geopolitics** has created a **complex cybercrime industry** where state-sponsored actors, criminal organizations, and individual hackers exploit vulnerabilities in digital infrastructure for political and economic reasons. It’s in the midst of this landscape that cyber security has become a pressing concern for governments, businesses, and individuals alike.

Power at risk: The impact on government cyber security

Paradoxically, after rapid digitalization and decades of increasing globalization, the world is now experiencing a particular geopolitical mega trend: **deglobalization**. Although some initial signs appeared in 2008, this process has recently accelerated because of the strategic competition between the United States and China.[1] These two superpowers have been engaged in tense relations, and their rivalry has spilled over into the realm of cyber security: They have accused each other of participating in state-sponsored cyberattacks, intellectual property theft, and espionage. Last year, for example, official websites in Taiwan were taken down by DDoS attacks, raising concerns about China's involvement due to the timing coinciding with senior US lawmaker Nancy Pelosi's visit.[2]



NEWS

Taiwanese websites hit with DDoS attacks as Pelosi begins visit

REUTERS®

U.S.-China relationship bleeds by a thousand cuts

The Washington Post

How the cyberwar between Iran and Israel has intensified

The New York Times

Russia Uses Cyberattacks in Ukraine to Support Military Strikes, Report Finds

Another example is the ongoing conflict between Israel and Iran, which have a history of engaging in covert cyber operations against each other. After the infamous Stuxnet worm, which targeted Iran's nuclear program, there have been multiple other cyberattacks, such as an attempted breach of Israel's water and sewage infrastructure in April 2020, a cyberattack on Iran's Shahid Rajaee port in May 2020, cyberattacks on Iranian transportation systems in July 2021, and a hack of an Israeli hosting company with personal information of users leaked in October 2021.[3] As cyberattacks like these keep intensifying, also in the context of Russia's war on Ukraine, there are raising concerns that their **objectives have shifted from mostly defense targets to disruptions of critical infrastructure and civilian life** – a fear that is shared by governments globally due to today's increasing political tensions.

[1] **Bruegel (2020).** Deglobalisation in the context of United States-China decoupling.

[2] **NBC News (2022).** Taiwanese websites hit with DDoS attacks as Pelosi begins visit.

[3] **The Washington Post (2022).** How the cyberwar between Iran and Israel has intensified.

> “The number of attempted cyberattacks has increased by approximately 8,000 percent since February 2022.

Sascha Czech
CSO at Uniklinikum Münster

Sascha Czech is CSO at Münster University Hospital (UKM) and, in this role, is responsible for the hospital's corporate security. UKM was the first hospital in Germany to establish a Security Operation Center (SOC) operated by its own specialist staff. For his efforts in the process, Czech was named CISO of the Year by Certification Information Security (CIS) in 2022.

You've held various security leadership roles in the healthcare sector. What have been the biggest challenges in your experience?

We're seeing the threat landscape become more dangerous, and it's been that way for some time now. It's not just that new attack methods are becoming increasingly common, but there's also a spike in the typical, constant “background noise”. I see the combination of cyber and physical perimeter security as the greatest challenge facing the healthcare sector right now.

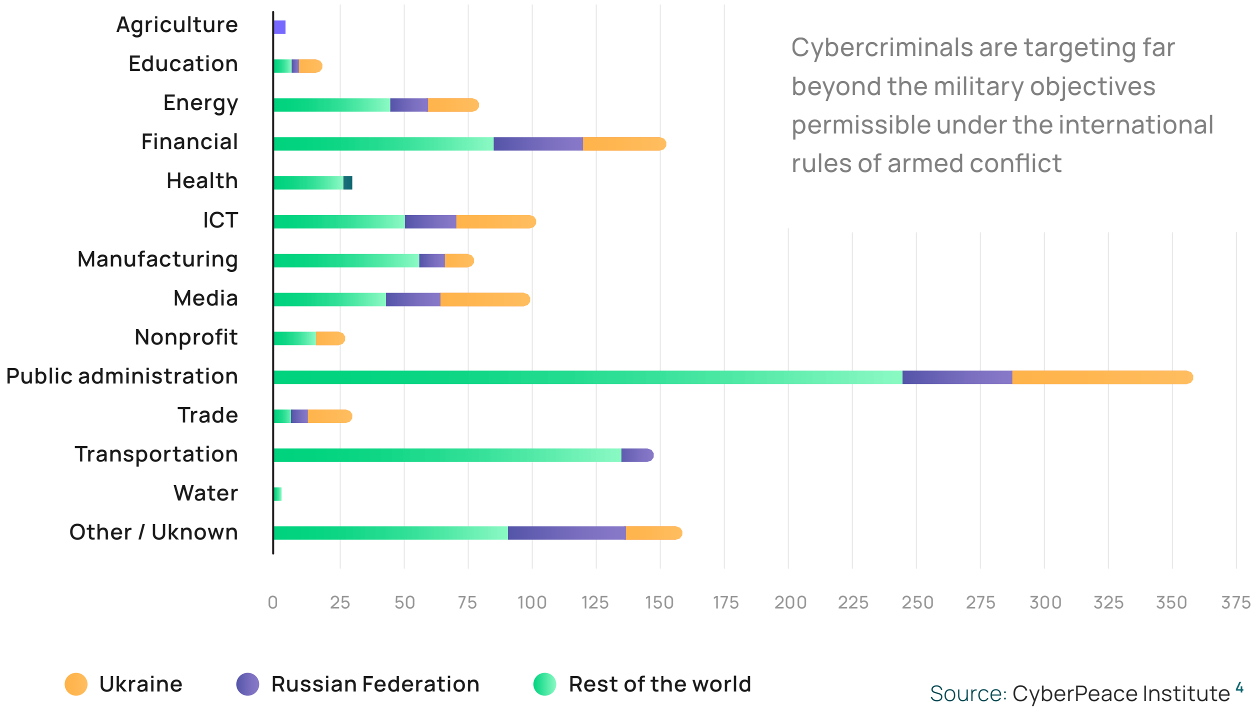
What do you think are the main causes of this?

Definitely the tense political situation, to start. At the Uniklinik Münster we noticed an approximately 8,000% increase in “background noise” since February of last year compared to the previous year. Harmful emails, be they phishing or ransomware, are also becoming more frequent. The individual waves are becoming much more intense, too.

Are you noticing a shift in the general attitude toward information security?

I think that the topic is far more present after being spotlighted in the media. But you still have to find a way to make people aware of their own responsibility, and to ensure that they're open to learning more. The moment that employees no longer think that security is “troublesome” and realize that it's a key to success, your company has won the battle. We first grouped the topic together with other matters of general safety, like fire protection. We also focus on having employees experience a simulated cyberattack so they can see how quickly and easily it can happen, and what the consequences could be. By doing so, we want to reshape their understanding of cyber security: People aren't just another line of defense – they're the most valuable.

Number of cyberattacks by sector depending on their location in the context of the Russia-Ukraine armed conflict



Cybercriminals are targeting far beyond the military objectives permissible under the international rules of armed conflict

Source: CyberPeace Institute [4]

The challenges for companies

> It would be almost naive to assume that criminals haven't known for quite some time now that attacks in the cyber sphere can be very lucrative.

Dr. Stefan Lüders
Computer Security Officer at CERN

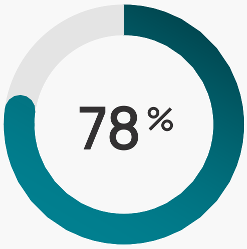
The fact that **geopolitical crises and cyber security have become inextricably linked** doesn't only affect governments and critical infrastructure, but also businesses worldwide. In recent years, we have seen numerous instances where companies were targeted with cyberattacks linked to geopolitical tensions.

For example, the US and UK governments blamed North Korea for the WannaCry attack, which impacted more than 300,000 computers across 150 countries, including hospitals, businesses, and banks, causing billions of dollars in damage.[5] In 2021, the Chinese government was also accused of being behind the Microsoft Exchange hack, affecting at least 30,000 organizations globally.[6] All these attacks showcase that global conflict might trickle down and pose security risks for companies.

[4] **Cyberpeace Institute (2023).** Impact & Harm. How do cyberattacks and operations impact civilians?

[5] **BBC News (2017).** Cyber-attack: US and UK blame North Korea for WannaCry.

[6] **BBC News (2021).** China accused of cyber-attack on Microsoft Exchange servers.



of security professionals say the geopolitical situation has increased the cyber risk of their organization

And geopolitical tensions are far from being the only global events that cybercriminals try to exploit for their own ends. Hours after the collapse of SVB in March this year, threat actors already started registering suspicious domains, building phishing pages, and gearing up for business email compromise (BEC) attacks.[7] As global instability escalates, cybercriminals will keep adjusting their targeting strategies and prioritizing industries and regions that present the most significant vulnerabilities in each given moment.

Weaponizing geopolitical crises: How hackers target individuals

> Civilians are taking part in huge cyberattacks because of a specific crisis or conflict. This is very worrying because it means crowdsourcing cyberattacks, which blurs the limits between who is a civilian, who is in the military, and who is the target.

Stéphane Duguin
CEO at CyberPeace Institute

During times of geopolitical tension, individuals tend to become **more emotionally charged and polarized in their views** – making them more vulnerable to social engineering attacks. Cybercriminals are aware of this and exploit these tensions by spreading misinformation, manipulating the public opinion, or even instigating violence. They also use phishing attacks across multiple channels to create a sense of urgency and fear in people, which can lead them to take hasty and ill-informed decisions.

Russia's war on Ukraine resulted in a sharp increase in coordinated cyberattacks as part of the offensive, impacting organizations and individuals in both these countries and worldwide. Even now, a year into the conflict, online scammers have been reported to use hundreds of fake charity websites to trick people who want to donate to Ukraine.[8]

Considering the high impact geopolitics have on the cyberthreat landscape, it's now up to us to stay informed and put the necessary security measures in place to navigate the complex and ever-evolving cybercrime industry.

> War is being waged in a hybrid manner, and people have turned to cybercrime to support one side or the other. Whenever the conflict is over, there will be high 'unemployment' among these attackers. These 'cyber-unemployed' will then be looking for a new challenge.

Tobias Ludwichowski
CISO at Signal Iduna

[7] **Bleeping Computer (2023).** Cybercriminals exploit SVB collapse to steal money and data.

[8] **BBC News (2022).** Ukraine war: Investigation finds hundreds of fake charity websites.

> “Cyber awareness must become an integral part of everyday routine, just like fastening the seatbelt before driving.

Major General Jürgen Setzer
CISO Bundeswehr

BUNDESWEHR

Major General Jürgen Setzer joined the Bundeswehr as an army officer candidate in 1980. After completing training as a light infantry officer, he studied computer science at the Bundeswehr University in Munich. Major General Jürgen Setzer has held the positions of Vice Chief of the German Cyber and Information Domain Service, Chief Information Security Officer of the Bundeswehr and Space Commissioner of the German Cyber and Information Domain Service Headquarters since April 2018. Major General Jürgen Setzer was born in 1960. He is married and has two children.

The German Cyber and Information Domain Service Headquarters was established in 2017. What was the underlying cause that led to its founding?

In order to face the challenges in cyber and information space as best possible, it was decided not only to establish a new Cyber/IT (CIT) Department in the Federal Ministry of Defence, but also to pool capabilities in the Cyber and Information Domain Service, a new military organizational element that comprises all Bundeswehr forces and assets in the cyber and information domain.

What are the tasks of the Bundeswehr Cyber and Information Domain Service?

The members of this organizational element are responsible for all matters relating to the cyber and information domain. They ensure the protection and operation of the Bundeswehr IT system both in Germany and on operations abroad. They also provide and develop reconnaissance and effects capabilities in cyber and information space.

Furthermore, they support mission accomplishment across all Bundeswehr service branches by providing geospatial information. They also contribute to national security by engaging in exchange and cooperation with other institutions.

How many cyberattacks does the Bundeswehr face every day? And what kind of attacks are these?

Cyberattacks are an everyday risk in today’s increasingly digitized world, and the Bundeswehr is no exception in this regard. Such attacks are nothing out of the ordinary; there are millions each year. Merely looking at the sheer number of attacks and unauthorized access attempts, however, is of little value to the Bundeswehr since the number alone does not allow any conclusions to be drawn as to specific threats.

How did the situation change last year?

There is generally a rising threat in cyberspace from malware attacks, including digital extortion by means of ransomware, as well as from espionage and attempted data and information theft. For years, an increasing trend has been observable towards ever more targeted and technically sophisticated cyberattacks on IT systems belonging to state organizations, critical infrastructures, or industrial and scientific entities.

Being a potential high-value target, the Bundeswehr generally faces the same threats as any other organization, but it must additionally be ready to ward off highly complex, tailored cyberattacks.

In addition, the number of technologically less sophisticated denial-of-service attacks aimed at sabotage has increased considerably since last year. This is clearly related to the Russian war of aggression against Ukraine. It seems plausible that non-state actors use this method to place political messages in cyberspace.

Has there been a shift in the ratio between physical and digital threats?

Cyberspace offers potential enemies an opportunity to inflict heavy physical damage, particularly below the threshold of a conventional conflict. A ransomware attack on a hospital, for example, could disable vital medical equipment, thus threatening human lives.

This explicitly includes state as well as non-state actors. It is particularly the possibility of disguising one's own location and striking covertly that makes cyberspace interesting to potential enemies. There is thus a permanent threat, which is present long before any traditional physical threat emerges.

How did the outbreak of the war in Ukraine affect this trend?

Before the beginning of the Russian war of aggression in February 2022, many experts assumed that the next conflict would take place largely in cyber and information space, expecting cyberattacks, disinformation, and propaganda campaigns as well as small-scale military operations by covert forces. Only very few actually expected battles involving great numbers of conventional armed forces. This, however, is exactly the kind of warfare we are now witnessing, and while it is flanked by an unprecedented number of activities in cyber and information space, these activities do not constitute the main effort. People have obviously realized that, compared to a cyberattack, a missile is still an easier, cheaper, and faster way to neutralize a power station. We have to acknowledge this and draw our conclusions. Nevertheless, we must not make the mistake of believing that this war is a blueprint for future conflicts.

Have you observed hybrid warfare?

Yes. Anyone following media coverage could see that Russia went to great lengths to spread disinformation, for example by promoting the narrative of a special military operation aimed at protecting the security of Russia and parts of the Ukrainian population. One example of a cyberattack would be the attack on the satellite communications system used by Ukraine, which also had an impact on the operation of German wind turbines. Together with traditional military attacks, we have thus observed three elements of an offensive hybrid strategy.

“ The Russian war of aggression is being waged in parallel to an unprecedented number of activities in the cyber and information space.

Do you think that cyber security in Germany should have a similar priority as in other services? Or is this already the case?

Cyber defense (hazard prevention) generally falls within the purview of the Federal Ministry of the Interior, Building and Community and its subordinate agencies as well as the police forces of the individual federal states of Germany.

The Bundeswehr is in close interdepartmental cooperation with domestic security agencies, particularly through the National Cyber Response Centre. In a state of defense or in case of an Article 5 contingency, the Bundeswehr has defensive and offensive capabilities not only for reconnaissance and effects in cyberspace, but also for preventing, detecting, and dealing with cyberattacks against Bundeswehr IT systems in Germany and abroad.

Cyber security is therefore of vital importance in the Bundeswehr. This was made clear with the creation of the Cyber and Information Domain Service as a dedicated major military organizational element on an equal footing with the traditional major services, i.e., Army, Air Force and Navy.

What do you assess as the three most relevant trends on the attackers’ side?

Social engineering, malware attacks (particularly involving ransomware), and denial or distributed denial of service (DoS or DDoS).

What role does the human factor play in (cyber) defense strategy? How do you approach this topic in the Bundeswehr?

Technical network protection measures have become so sophisticated that direct attacks hardly penetrate beyond perimeter protection. For this reason, cyberattacks often target IT end users, achieving their objectives from within. Caution by humans working on end-user devices is critical to enabling a fast and suitable response. In my role as Chief Information Security Officer, it is thus essential for me to educate Bundeswehr staff in cyber awareness and to boost resilience.

In the Bundeswehr, the effectiveness of cyber security measures is evaluated on a regular basis. Our in-house security campaign “Phishing as a Service in the Bundeswehr (PaaSBw)” is also part of this. Our soldiers and civilian staff are literally the last line of defense, and it is important to raise their awareness and increase their resilience. Cyber awareness must become an integral part of everyday routine, just like fastening the seatbelt before driving.

Cyber security requires a whole-of-government approach as well as interdepartmental cooperation. In this spirit, many Bundeswehr agencies show great commitment every year by providing input and conducting awareness measures as part of the European cyber security month in October. This is intended to highlight the risks inherent in the use of information technology and to raise awareness among all personnel for potential enemies who might exploit digital innovations for attacks on the Bundeswehr and its allies.

What measures do you take to make IT security a key issue in the Bundeswehr and establish a security culture?

Information security has become recognized as a crucial command-and-control task in the Bundeswehr. In this regard, we have already taken a great step forward. The key factor for a successful security culture is the interplay between all actors in the Bundeswehr – from the command level down to each individual Bundeswehr member. Since 2020, we have been encouraging external IT security researchers, so-called white-hat hackers, to identify vulnerabilities in Bundeswehr systems and web portals and to report them to us.

With the Vulnerability Disclosure Policy of the Bundeswehr (VDPBw), we have established a legal framework for IT security experts to identify and report those vulnerabilities and thus to offer protection against inadvertent or deliberate misuse. Owing to the reports and extensive documentation these experts provide, we have already managed to improve the IT security level in the Bundeswehr. Thanks to these vulnerability reporting guidelines, the Bundeswehr acts as a pioneer among government authorities in this field.

How has the 100-billion-euro special fund for the Bundeswehr affected your work? What developments are there regarding your cyber defense, where do you invest?

There is not one single major cyber security project. Rather, cyber security plays a vital role in each and every armament project and is always taken into account from the very beginning.

Social engineering:
The source that does not cease

Top 3 tactics in successful cyberattacks

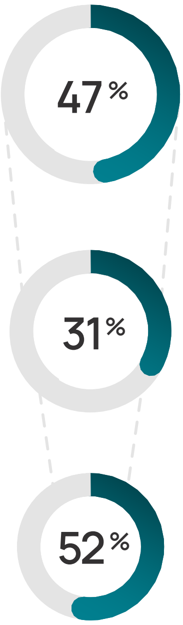
1. Malware
2. Phishing
3. Ransomware

> We don't really see a significant variation of entry points for cyberattacks: infiltration by malware or the stealing of sensitive information, through phishing for example.
>
> Dr. Stefan Lüders
> Computer Security Officer at CERN

While geopolitical upheavals and global crises broaden the attack surface for cybercriminals and technological advancements help them scale their business models, more sophisticated attack tactics are only slowly gaining traction (more on this in the next chapter). Cybercriminals still seem to stick to what they know best: Social engineering – often in the form of phishing. It ranks second on the list of the most successful cyberattack techniques in our survey, in the top three together with malware and ransomware, which also often start with phishing or other types of human manipulation. Moreover, over **61 percent of security professionals say that their companies have been targeted by cybercriminals using emails**, and the trend seems to only accelerate.

> We’re receiving harmful emails more frequently, and each new wave is more intense than the last.
>
> Sascha Czech
> CSO at Uniklinikum Münster

There are reasons for cybercriminals to continue to rely that heavily on phishing: Our platform data shows that it still is a highly effective tool for them as a way to obtain sensitive information and/or access company systems – as evidenced by the fact that one in three users click on harmful content in phishing emails.



Opening rate

Almost 1 in 2 users open phishing emails…

+2 from 2022

Click rate

a third of those click on harmful content in the emails, …

+1 from 2022

Interaction rate

and half of those continue to interact with the content.

-6 from 2022

Although users have become slightly more cautious about interacting with harmful content compared to 2022 (down from 58 to 52 percent), the rates continue to be alarmingly high. We can still see that, when phishing emails manage to trigger a click, they also manage to trigger further interaction in half of those users, for example a data entry in fake login screens. **New technological advancements like generative AI are likely to further boost these KPIs**, giving criminals a chance to enhance their phishing content and scale their overall output (more on this in the next chapter).

But what makes social engineering such an effective attack tactic? To achieve their goals, cybercriminals rely on various vectors that they continuously adjust to current trends to boost their attacks’ impact. A deeper dive into these vectors shows why manipulating human emotions lies at the core of their strategies: They are very successful no matter the technical precautions companies might have already implemented.

Technical adjustments for emotional wins

For cybercriminals, a highly scalable approach to making their phishing attacks more successful is making technical changes to the emails’ format, whether it is in the form of an attachment, link, reference to an input mask, or imitating a reply-/forward-chain. All these vectors continue to work very well, although the overall success rates of technically adjusted phishing emails are on the decrease compared to previous years. Notably, **users seem to have become more careful with attachments**, resulting in an 8 percent click rate decrease from 2022.

Click rates by type of attack (vs 2022)

Attachments	Links	Input masks	Reply/forward
32%	25%	27%	34%
-8	-1	-2	-5

Similarly, different address manipulation techniques are staples in cybercriminals' toolboxes. While simple changes in the target domain only trigger a click in every fifth or sixth person, **subdomain squatting and email address spoofing are more successful in deceiving people**, with click rates of 26 percent and 29 percent.

These developments show that users' awareness of technical manipulation techniques has increased. As more traditional attack methods like attaching a malicious file are starting to lose their relevancy and click rates are dropping, attackers will begin to shift from technical mass manipulation to more sophisticated techniques.

Click rates by attack method

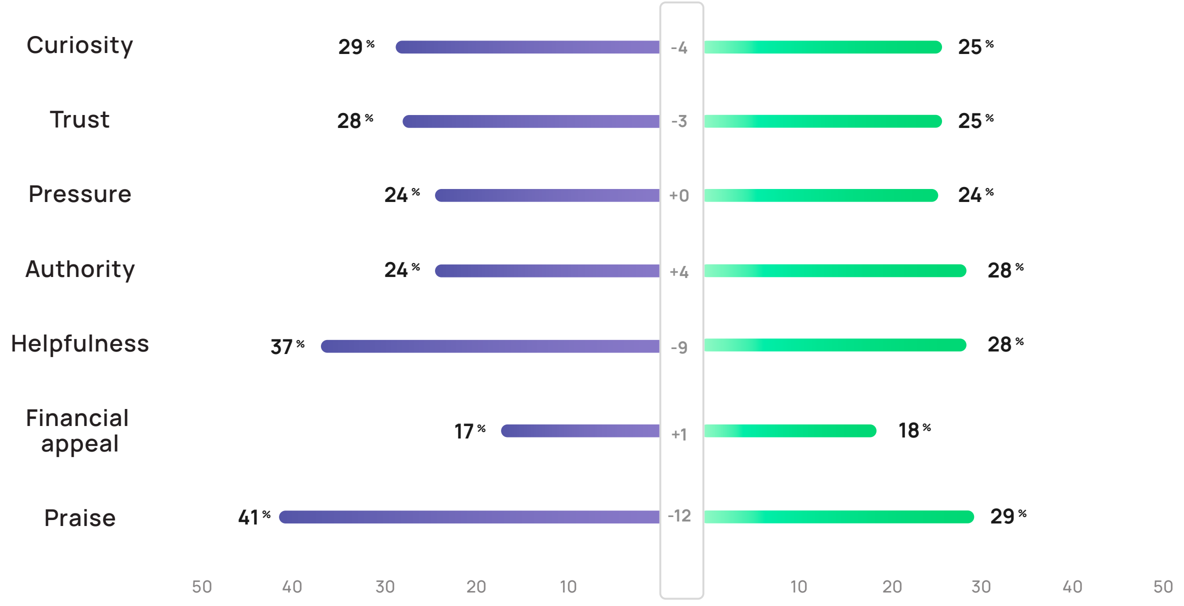
Typo squatting	Subdomain squatting
17%	26%
Email address spoofing	Domain squatting
29%	20%

The psychological aspect: Emotional deceit

Ultimately, the strength of social engineering for cybercriminals lies in its adaptability. It thrives on leveraging new social or political developments to manipulate human emotions – as a closer look at psychological vectors in phishing campaigns impressively illustrates. How convincing the content of a phishing email is and whether it hits a "sweet spot" in terms of emotional persuasiveness plays a decisive role in how many people end up clicking on harmful content.

Compared to 2022, there seems to be a switch regarding which emotions are the most promising for cybercriminals. Although provoking positive emotions through praise and helpfulness generally yields higher click rates, there has been a slight increase in the success of tactics that generate **negative emotions** like imposing authority, pressure, and making financial appeals. This suggests that users have become more susceptible to this kind of emotional manipulation and exploitation. One possible explanation for this trend: Society has seen a massive number of crises and conflicts over the past year, and citizens are anxious and unsettled – making it easier for criminals to evoke negative reactions.

Click rates by emotional trigger ● 2022 vs ● 2023



The top phishing subject lines also show that the most successful phishing campaigns among employees are leveraging negative emotions, with four out of the top five playing with an element of pressure.

Top 5 phishing subject lines 2022

1	Damaged car	Pressure/curiosity
2	Teams invitation	Curiosity
3	Payroll error	Pressure/curiosity
4	Your office password expires today	Pressure
5	Teams missed chat	Pressure/curiosity

The crucial role of modern security awareness training in preventing phishing

The positive news is that employees' awareness of these and other social engineering tactics can be sustainably increased through modern security awareness training. As data from the SoSafe Awareness Platform shows, **a combination of gamified e-learning, phishing simulations, and contextual reporting tools can increase phishing reporting rates up to 80 percent** – significantly contributing to how secure organizations are from cyberattacks and how fast they can react to threats (learn more in the outlook). What is crucial in doing so is a clear focus on the people: Insights from behavioral science can help find the most effective methods to foster secure employee behavior. Approaches like the Behavioral Security Model, which shows synergies between context, knowledge, motivation, and ultimately behavior in organizational settings, can act as guiding principles for security professionals (see also Human Risk Review 2022).

> There is a misconception that the cyberspace is unregulated, which is simply not true. There are many cyber security laws, but they are not properly enforced.

Stéphane Duguin
CEO at CyberPeace Institute

Stéphane Duguin is CEO of CyberPeace Institute and has spent two decades analysing how technology is weaponized against vulnerable communities. He sits on the Board of the Datasphere Initiative, is a member of the Advisory Board of the Global Forum on Cybercrime Expertise (GFCE), and a thought leader in digital transformation and convergence of disruptive technologies. Prior to that, Stéphane Duguin was a Senior Manager at Europol where he led key operational projects to counter both cybercrime and online terrorism.

The CyberPeace Institute has a human-centric approach. In your experience, how can cyberattacks affect individuals?

We should never forget that, in most cases, cyberattacks aim to play with the victim's cognition, meaning there is a manipulation factor. For example, ransomware is one of the few cybercrimes that requires the victim to be an accomplice. When you are hit by ransomware, you must make complicated decisions that have a psychological impact, such as whether to pay the ransom or report the attack.

The second part is the creation of guilt on the part of the victim. NGOs are very heavily affected by CEO frauds. When that happens, the person who fell for the attack, in many cases, is under the scrutiny of the organization.

Another consequence is more systemic: the impact of the attack on the beneficiaries of the entity. We see this in the healthcare system, for example. A Vanderbilt study shows that a cyberattack's impact on hospitals is still evident after several months – or even a year later. Patients with critical conditions received lower-quality healthcare and had a higher chance of having a fatal outcome than before the attack.

We cannot underestimate the long-term psychological impact on victims. An example that illustrates this very well is the ransomware attack on the Vastaamo Clinic in Finland, where they refused to pay the ransom and the criminals decided to extort each and every patient of that clinic, threatening to disclose their private psychological information. In that situation, Finland had to set up an ad-hoc victim support unit to treat more than 25,000 victims.

Looking at the current threat landscape, how do you think it has changed in the last year?

Fundamentally, the cybercrime as a service business model has accelerated. We have seen a very rapid increase in criminal groups using disruptive technology. Cybercriminals are very good at collaborating with each other, and they are now leveraging new technology as attack vectors. We are seeing it with ChatGPT, but we already saw it long ago when deepfakes appeared.

The second aspect that has not improved is how states protect people from cyber threats, which implies ensuring laws, norms, and regulations are properly enforced in the cyberspace. There is a misconception that the cyberspace is unregulated, which is simply not true. There are many cyber security laws, but they are not properly enforced. There aren't enough law enforcement resources to have a systemic response. Another way in which states do not contribute to improving the threat landscape is through surveillance attacks. When states continue to use their resources to conduct surveillance attacks, they are investing in global cyber insecurity, because for that surveillance to work, they need to ensure there are vulnerabilities in the cyberspace.

The third aspect is something we have seen for quite some time, but that is, unfortunately, booming now more than ever in the context of the conflict in Ukraine: the "civilianization" of cyberattacks. This means that civilians are taking part in large cyberattacks because of a specific crisis or conflict. For example, we have seen some Russian criminal groups attacking anyone who is against Russia's interests and volunteer hackers joining the Ukrainian IT Army. This is very worrying because it means crowdsourcing cyberattacks, which blur the lines between who is a civilian, who is in the military, and who is the target.

With the emergence of new tools like ChatGPT, the field of Artificial Intelligence is experiencing a significant boom. In your opinion, how do you think this will affect the cyber threat landscape?

Everything we saw regarding deepfake engineering was a disruption of AI back in 2017. Quite some time has passed, and now criminal groups can generate very convincing and authentic content to manipulate people: a familiar voice, face, or well-crafted email. Another aspect of AI technology is its use to better evaluate your social ecosystem to create very smart social engineering attacks or vectors of attack.

There's also a strategy that is on the rise among criminal groups, and that is AI-generated or AI-assisted attacks to better automate the attack and discover the infrastructure more easily. This means that, on the defense side, we must implement AI tools to be better at defending ourselves.

You mentioned the benefits of using AI as part of our security defenses. What challenges do you foresee in this use of AI?

The big risk here is that AI will generate a lot of data that actual humans will need to go through. The problem with this is that the number one challenge in the cyber security industry right now is burnout: There's too much data, too many cases, and not enough time. Unfortunately, AI is only going to exacerbate this problem because it will multiply the amount of data, which is quite concerning.

Demographic vectors steering social engineering success

Beyond what cybercriminals can influence when rolling out their schemes, there are additional demographic variables that seem to have an impact on their success rates. Surprisingly, age has consistently been a decisive factor in how often people click on harmful content in phishing emails: **Digital natives are 65 percent more likely to click than older users**. One possible explanation for this disparity is that older users, with their accumulated experience and more cautious online behavior, might be better equipped to recognize and avoid potential threats. In contrast, digital natives (in this analysis, people between 18 and 40 years) are more readily trusting digital communication since they grew up with it and tend not to question the legitimacy of what they are confronted with as thoroughly as their older counterparts (people between the ages of 41 and 60).

Younger users (18 - 40 years) are

↗ 65%

more likely to click on phishing emails than older users (41-60).

> From the very start, we have to consider the likelihood of a cyberattack in our culture and our daily work tasks.

Thomas Schumacher
Managing Director at Accenture Security

Industries in the crosshairs

There are also variations across different industries when it comes to social engineering and phishing success. Industries that have been heavily impacted by the latest social developments, such as the logistics, energy, and tourism sectors, show the highest phishing click rates. On the other hand, among those with the lowest click rates are industries with high shares of frontline workers, for example, agriculture, construction, and chemicals and raw materials.

Industry	Click rate
Transport & Logistics	38%
Energy & Environment	35%
Tourism & Gastronomy	35%
Pharma & Health	33%
E-commerce	32%
Education	31%
Services & Craft	29%
Finance, Insurance, & Real Estate	28%
Technology & Telecommunications	27%
Metal & Electronics	26%
Media & Marketing	25%
Consumer & FMCG	25%
Trade	24%
Society	24%
Administration & Defense	24%
Internet	23%
Leisure	23%
Agriculture	20%
Construction	20%
Economy & Politics	20%
Chemicals & Raw Materials	16%

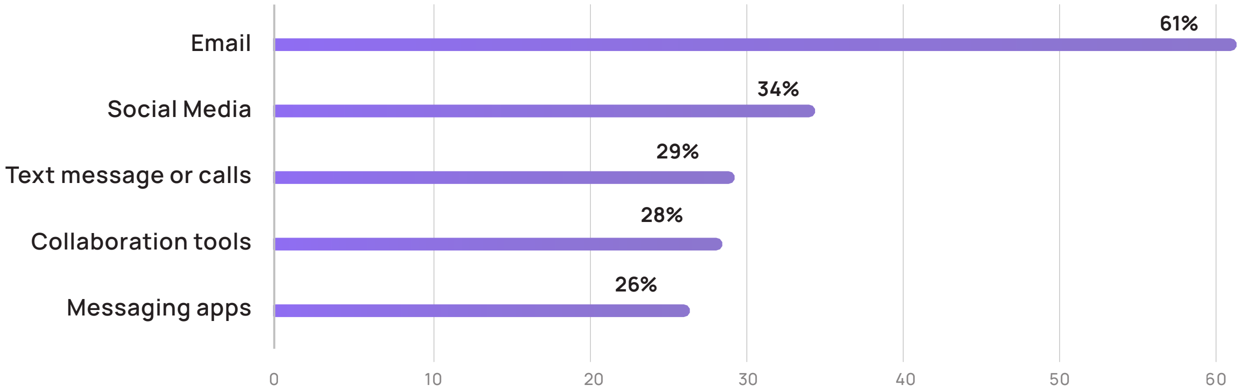
The future of phishing: From email to collaboration tools and social media. What will be next?

Innovation is cybercriminals' best friend – and so they have not only found technical, psychological, or demographic vectors to improve their attacks but also new tools to roll them out in the first place. Whereas email-based attacks are still the most popular, other channels are steadily gaining traction.

Emails are slowly losing their importance as the sole communication channel in companies, and other collaboration and communication tools will most likely only diversify in the upcoming years – a fruitful development for criminals.

In fact, the **first multi-channel attacks have already led to massive damage**, for example, in the case of Uber.[1] The attackers tricked an employee into accepting an MFA notification by pretending to be the internal IT department in a WhatsApp message. Consequently, the company was forced to take large parts of its systems down in order to limit the criminals' access to sensitive information.

Channels that companies have been targeted on in 2022



> When we start working with new types of technology, we must consider the risks from the very start. Otherwise, it will end in disaster.
>
> **Thomas Tschersich**
> CSO at Deutsche Telekom

Companies today stand insufficiently protected against social engineering schemes that will only continue to become better as technological developments are speeding up by the minute – as generative AI is currently illustrating in front of our eyes. That is why many organizations have started to invest more resources into their security culture and now put people at the heart of their strategies.

[1] **Bleeping Computer (2022).** What the Uber Hack can teach us about navigating IT Security.

“A comprehensive security strategy should incorporate the three pillars of technology, people, and processes.

Thomas Schumacher
Managing Director at Accenture Security

accenture

Thomas Schumacher leads Accenture’s security business for Austria, Switzerland, and Germany (ASG). He is also a member of the ASG Leadership Team and the global Accenture Security Leadership Team. Schumacher has advised leading German companies on IT security issues and the operation of secure IT infrastructures for over 20 years. He is an expert in complex transformation projects in various industries, especially in the context of digitalization, post-merger integration, and increasing IT efficiency.

In your opinion, what is the most important point that companies should keep in mind regarding their security strategy?

From my point of view, the topic of cyber security and cyber resilience, as we call it at Accenture, starts strategically. A comprehensive strategy should include the three pillars of technology, people, and processes.

Companies need to be able to answer questions like, “What is my DNA?”, “What do I need to keep my business processes running, no matter what?”, and “What do I want to secure in the first place?” When you’ve completed this exercise, you can start to think about how best to go about it. Many companies still approach this process quite haphazardly. At the latest, this becomes apparent in the case of an attack.

You mention the human factor as one aspect in security strategies. Which role do employees play specifically?

You could always say: Employees will click on something sooner or later. That’s probably true because we can’t protect ourselves from everything. But the question is how quickly all the protective barriers will fall. That is why you have to synchronize the three dimensions of technology, people, and processes. From my point of view, you are ill-advised to rely on technology alone because the costs increase disproportionately. Everything that I can cover through employee awareness and training – supported by the right technology – makes me more resilient as a company. That’s because the human layer protects companies from all types of attack tactics, not only those tailored to a specific use case. I save on time, money, and stress, and avoid more risks.

What is the greatest challenge in relation to the human factor?

I think the biggest challenge is our error culture. If someone does click on a phishing email, we don't want them to think: "I will keep my mouth shut about it and not tell anyone." What really matters in those cases is that we act quickly, report an incident quickly, are aware of what is happening, and how to handle the situation.

Is that a factor influenced by a company's general culture?

To a certain degree, it's comparable to child education. I myself have a big brother – I learned rather early on to deny things when the going gets tough. But that's not very smart in the long run because the problem is likely to explode later. That is why it's extremely important that a reporting culture be created, and to say that it's okay – good, even – when someone quickly reports an incident that they caused. This attitude is not yet common or widespread, especially among SMEs – particularly when there are already financial claims or losses on the table.

How can you influence this culture positively?

I think the first point is to emphasize again: We can't prevent attacks and human error. From the very start, we have to consider the likelihood of a cyberattack in our culture and our daily work tasks. In addition, we should speed up reporting channels or perhaps even make them anonymous so that, in the end, consequences no longer fall on individuals at all. This is easier in large companies, because the connection to the loss and the investment that has to be made is smaller than in the case of a private individual.

If we look at security awareness more specifically: Are you seeing a move away from mandatory training and policies toward continuous training?

I'm still seeing a lot of companies being driven by compliance requirements. But of course, more companies now see the need for employee training. Especially concerning remote employees, basic security knowledge adds real value. We also see that some companies think they have to build their own solutions for this. But there are now many tools on the market that specifically cover this area.

Do large and medium-sized companies approach security awareness differently?

In my view, a fundamental problem with large companies is that they believe they have things under control. But then again, I think that's the case for many companies because cyber resilience is a very complex issue in itself.

Perhaps we need to broaden the scope a bit: We are in a period right now where we have to protect ourselves from cyberattacks, physical threats, a pandemic, and natural disasters. That's a lot of big business risks in one fell swoop. Finding an answer to these is much more difficult than "just" for cyber threats.

But the complexity also adds a whole other dimension to cyber: I have to prepare my employees for completely new scenarios, such as suddenly not being able to work in your company's branches anymore. We have to bring cyber resilience and business resilience closer together.

> “It’s extremely important that a reporting culture be created, and to say that it’s okay – good, even – when someone quickly reports an incident that they caused.

Does this tense situation make continuous awareness training more necessary?

Technology is becoming more advanced, but so are attacks. Therefore, people also have to adapt their daily habits to a certain extent. It’s a classic behavioral pattern: I realize that times have changed, possibly also due to technical developments, but I still carry on as I did 20 years ago. That’s why I believe: We need to move away from telling people what to do and ensure that safe behaviors turn into personal skills. And the reasons for this aren’t even limited to the workplace. If I buy a car today and it has “keyless go” technology, I also have to deal with the fact that things are interconnected and adjust my behavior accordingly. So, we must continue to strengthen this idea of security in our private lives as well and incorporate it more permanently into our everyday lives so that everyone is able to question their own behavior at any time.

The technological innovation you're talking about has been around for a long time, but attackers aren't jumping any higher than they have to. Is that also how you perceive it?

Yes, the attacks are often quite simple and successful, nonetheless. But we also see destructive attacks by attackers who have such high financial resources that anything is possible. I'm pretty sure: The first quantum computer will be with some attacker who uses it to break cryptographic procedures. We must be aware that some attackers have enormous resources, and we need to prepare ourselves accordingly.

That all sounds quite threatening. Is it perhaps also necessary to take away people's fear of the subject?

Fear is always a bad teacher. The question is rather: What can you do? Where can you help? It is not hopeless. You just have to have a few ground rules, a few basic rules of play.

How have security budgets developed? Are they adapting to this development?

Here again, you have to distinguish between large companies and small and medium-sized enterprises – and again, on a sector-specific basis. Since 2014, supervisory authorities have pushed the entire financial industry, i.e., banks and insurers, to take security initiatives. They've passed the phase where "fearmongering" frees up budgets. These companies are very controlled and restrictive in their investments because they have learned to deal with the issue. What still remains unknown in these sectors is: Are they investing properly? I don't think so because there is still too much tool-based buying, and people believe they can eliminate risks completely just by implementing a new tool.

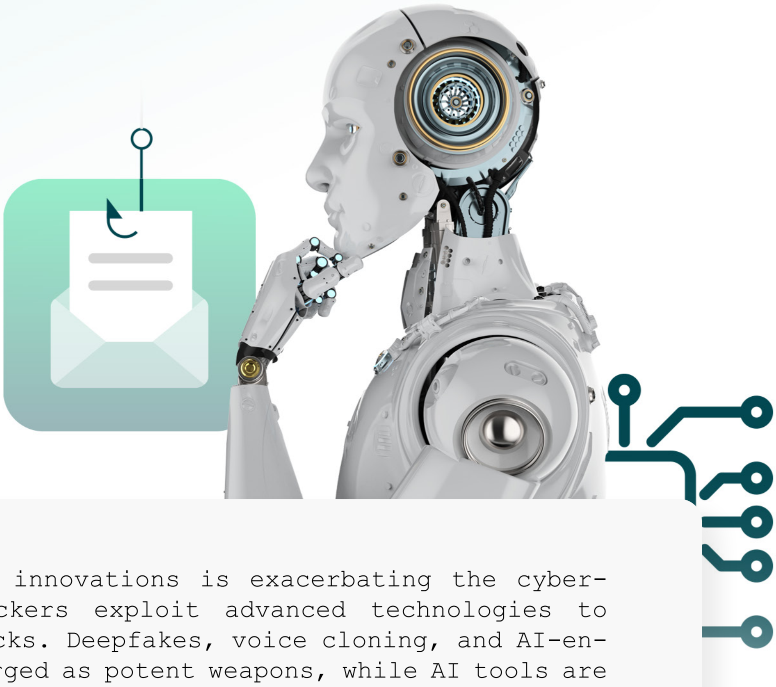
I believe that overall budgets are no longer as readily available. Many mid-sized companies thought that cyber resilience doesn't apply to them, but attacks have taught them otherwise. The great danger here is that things are introduced haphazardly and are to be solved through technology alone. Often, these companies don't even have internal IT departments. So, we need a new generation of companies that can assess cyber risks in addition to market risks.

What would you like to share with other security managers?

The first point is: Cyber resilience is a social problem that has to be solved. That means we all must work together to find a solution – the closer we work together, the more successful we will be.

The second point is: we're not going to win any gold medals for managing risks better than anyone else. It's about "survival." That's perhaps a bit apocalyptic, but it captures the situation quite well. The danger is there, and we need to communicate that more strongly without scaring people.

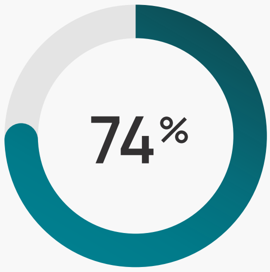
AI meets cybercrime:
The explosive impact of technological innovation



The proliferation of AI innovations is exacerbating the cyber-threat landscape as hackers exploit advanced technologies to create new types of attacks. Deepfakes, voice cloning, and AI-enhanced phishing have emerged as potent weapons, while AI tools are democratizing cybercrime by simplifying the process of crafting malicious emails and software. In parallel, ChatGPT raises substantial data privacy concerns since the potential misuse of sensitive information could lead to further cyber vulnerabilities.

Moreover, AI has the potential to intensify social manipulation and escalate global tensions by leveraging its capabilities for misinformation and propaganda. Biometric authentication systems, once deemed secure, are also under threat as AI tools can bypass such security measures. As the digital and geopolitical realms collide, the implications of AI in cyber warfare necessitate a more proactive approach toward cyber security and a reevaluation of current defense strategies.

These paragraphs were written by ChatGPT-4 ✓



of security professionals say that artificial intelligence will worsen the cyberthreat situation

AI-powered social engineering: Deepfakes and voice cloning

Deepfake technology is not a 2023 innovation, but it's on everyone's minds at the moment for compelling reasons: Hackers are using it for **mass manipulation** and to **scale global tensions**. The deepfake video of Zelensky announcing Ukraine's surrender in 2022 served as a prime example.[1]

But deepfake technology is not only used for political purposes. Cybercriminals also steal data and money from individuals and companies in highly advanced attacks that combine vishing with voice cloning. In a recent example from Arizona, a mother was tricked into believing her 15-year-old daughter had been kidnapped as she heard the girl's desperate cries for help over the phone. The mother eventually discovered her daughter was safe and her voice had been artificially replicated. However, she maintained that she never questioned the authenticity of her daughter's voice.[2] In a different case, attackers impersonated the CEO of a company using deepfake audio and tricked an employee into transferring $35 million to a group of fraudsters.[3] This technology is **even becoming more advanced** with tools like Microsoft's VALL-E, which can generate speech in any voice after only hearing a three-second sample.[4]

With organizations worldwide progressively adopting bypass biometric authentication as a potentially more secure alternative to passwords and PINs, concerns are growing over the use of voice cloning and video deepfakes that could circumvent these advancements. This has led to the ban of facial-recognition software for government use in some regions of the United States.[5] As deepfake technology advances and new uses are uncovered, **both the public and private sectors** will need to work collaboratively to **raise awareness** about the capabilities and limitations of such technology.

Exploiting generative AI: ChatGPT as the attacker

With the advent of new AI tools, cybercriminals are learning how to harness their power to refine and scale their most successful attack tactics, especially social engineering. Even if generative AI tools like ChatGPT explicitly ban fraudulent uses of the application, hackers have found many ways around the restrictions.

[1] **NPR (2022).** Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn.

[2] **Independent (2023).** AI clones child's voice in fake kidnapping scam.

[3] **Dark Reading (2021).** Deepfake audio scores $35M in Corporate Heist.

[4] **Metaverse Post (2023).** VALL-E: Microsoft's new zero-shot text-to-speech model can duplicate everyone's voice in three seconds.

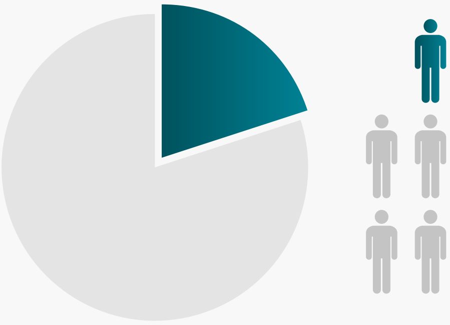
[5] **Built in (2023).** 5 AI trends to watch in 2023.

Phishing emails crafted by ChatGPT and other generative AI tools are skillfully tailored and well-written, making them **less suspicious** than traditional mass phishing attempts. This means it is becoming **increasingly challenging for both spam filters and people to detect them.**

Recent research from SoSafe's social engineering team shows that generative AI tools can help hacker groups compose phishing emails at least 40 percent faster. More significantly: The data, taken from the SoSafe Awareness Platform that anonymously evaluated approximately 1,500 simulated phishing attacks in March 2023, revealed that AI-written phishing emails were opened by 78 percent of people. Among those, one in five people went on to click on malicious content within, such as links or attachments.[6] And this is only the beginning: The test was based on non-personalized phishing emails written by ChatGPT-3.5. However, new AI tools based on enhanced language models are popping up almost daily and the jump from ChatGPT-3 to ChatGPT-4 has already taken scaling personalization to a new level.

However, phishing is only one of the many tactics hackers have refined using AI. With this technology, anyone with minimal technical knowledge can generate sophisticated "polymorphic" malware code that can shapeshift its way around traditional security mechanisms[7], turning these tools into powerful weapons at everyone's fingertips and democratizing cybercrime.

> **The safeguards preventing ChatGPT from providing potentially malicious code only work if the model understands what it is doing. If prompts are broken down into individual steps, it is trivial to bypass these safety measures.**
>
> EUROPOL[8]



1 in 5 users

click on AI-generated phishing emails

[6] **SoSafe (2023).** One in five people click on AI-generated phishing emails, SoSafe data reveals.

[7] **Gizmodo (2023).** ChatGPT is pretty good at writing malware, it turns out.

[8] **EUROPOL (2023).** ChatGPT The impact of Large Language Models on Law Enforcement.

[9] **Bleeping Computer (2023).** OpenAI: ChatGPT payment data leak caused by open-source bug.

[10] **BBC (2023).** ChatGPT banned in Italy over privacy concerns.

[11] **World Economic Forum (2022).** Why artificial intelligence design must prioritize data privacy.

[12] **European Commission (2023).** Intellectual Property in ChatGPT.

ChatGPT – is your data safe?

AI tools require immense data volumes to operate effectively. Inevitably, this raises concerns among individuals and organizations regarding the privacy and security of the information they disclose to prompt the tool.

What are the risks?

Storing massive amounts of data in large servers is not exempt from risks. Earlier this year, we saw how a relatively simple bug in ChatGPT led to many users being able to read other users' queries or even log-in emails and telephone numbers.[9] This incident only exacerbated existing pitfalls around OpenAI storing and using sensitive data. Italy has even taken the step of temporarily banning ChatGPT, arguing a lack of legal justification for collecting sensitive data for algorithm training and highlighting issues about GDPR compliance.[10]

Other attacks, using methods such as reverse engineering to uncover users' sensitive data from the chat's output, could be catastrophic and result in massive data breaches.[11] Experts are also worried about the potential to hack these tools to compromise their output for misinformation or social manipulation, especially in the context of the current global crises.

Intellectual property and copyright infringement is also a troubling aspect of ChatGPT's output. Even though OpenAI's Terms of Use assign to the user the ownership of the output and state that the content it produces is original – although not necessarily unique – the answers it provides derive from content that may be copyrighted by others.[12]

What can we do?

Despite it being a recent development in technology, organizations like the European Union are already passing new laws and regulating the legal aspects of AI tools. However, users can also protect themselves by following some recommendations:

→ **Never enter sensitive personal or professional information.** Your data could be collected for further analyses or improvements of the tool or be exposed in case of a data breach.

→ **Always double-check that the information of the output is true.** AI is not perfect and may make false assumptions or have learned from misleading sources.

→ **Seek legal advice before using the output for commercial purposes.** Ensure you are not infringing on any law or intellectual rights.

> In my opinion, the biggest problem is that we aren’t taking care of the basics.

Thomas Tschersich
CSO at Deutsche Telekom

The dry powder hypothesis

There’s no doubt that technology is progressing at a dizzying rate, with the potential applications of artificial intelligence in cyberattacks evolving equally as swiftly. However, while there have been some cases of sophisticated attacks, **hackers have not yet exploited these tools to their full potential**.

As long as conventional methods like mass phishing or spear phishing emails continue to breach human defenses and infiltrate systems, cybercriminals are unlikely to devote substantial time and resources to orchestrating even more sophisticated attacks at scale. However, as AI tools are continuously improving and democratizing cybercrime, while simultaneously improving the reach and success rates of even the most common cyberattacks, the danger of successful attacks hitting organizations and individuals is greater than ever before.

> Cybercriminals have had some very advanced technology at their disposal for quite a while, like voice cloning. Yet, we haven‘t seen sophisticated social engineering at scale in the wild. One explanation: The simple stuff still works. But with leaks of large language models and exponential development in generative AI across the board, this will very likely change.

Dr. Niklas Hellemann
CEO at SoSafe

Harnessing human defenses against AI-powered cyber attacks

AI has long been used in cyber security to assist professionals with countless tasks, such as attack prediction and detection and automated incident responses. However, recent developments in generative AI tools have allowed attackers to leverage the same technology for unethical purposes, transforming the cyberthreat landscape and **democratizing cybercrime**. While new fraudulent potential uses of AI continue to emerge, law enforcement, international institutions, and AI tool providers are ramping up their efforts to prevent hackers from using AI as an attack vector. But for every law, there’s a loophole, and hackers are constantly finding new ways to target their victims. To avoid sizable damage, security teams must adopt new strategies to adapt to the ever-changing – and now AI-powered – threat landscape. As threats become increasingly harder to detect by technical security controls, the need for a strong security culture that fosters awareness and strengthens the human layer becomes critical.

> Day-to-day work implies that you need to take risks. At one point, you need to open that email and then open that attachment. Despite technology always advancing and taking a big load off your shoulders security-wise, the human risk is still present, and therefore, we have to make sure that our human firewall is well set up.

Stefanie Boem
Data Protection Officer at Sport Thieme

A new era of digital threats:
The professionalization of cybercrime

The rise of generative AI tools has not only democratized cybercrime but also **fueled its increasing professionalization**. In addition, cybercriminals have jumped on cybercrime-as-a-service (CaaS) trends to further professionalize their business models. This confluence of factors has created a fertile breeding ground for them to collaborate, innovate, and launch attacks on vulnerable organizations.

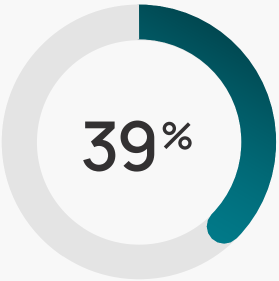
Ransomware, in particular, has emerged as a key component of the CaaS landscape. Since its inception in the late 1980s, **ransomware has remained a prevalent form of cyberattack**, instilling fear in both companies and individuals.

> Ransomware is one of the few cybercrimes that requires the victim to be an accomplice. When you are hit by ransomware, the victim must make complicated decisions that have a psychological impact, such as whether to pay the ransom or to report the attack.
>
> **Stéphane Duguin**
> CEO at CyberPeace Institute

Our survey further underscores this reality: Ransomware continues to be one of the most common cyberattack types, with 1 in 3 companies that experienced a cyberattack in the past 3 years falling victim to ransomware. Moreover, among those targeted by ransomware, an alarming 39 percent admitted having paid the demanded ransom. Among smaller companies, almost half were forced to pay.

31%

of the companies that experienced a cyberattack in the past 3 years were attacked with ransomware, and



admitted having paid the ransom

However, it is in recent years that ransomware has experienced the biggest transformation: The birth of ransomware-as-a-service (RaaS) in the last decade and its continuous growth today illustrate how cybercriminals are adapting and diversifying their business strategies to further enhance their illicit activities.

Ransomware-as-a-Service is a growing pandemic impacting companies worldwide

Cybercriminals now require **minimal IT expertise or hacking abilities** for ransomware attacks. By merely browsing the dark web and making a crypto payment, they can access ransomware-as-a-service (RaaS) platforms with subscription models and dedicated customer support – as impressively shown by the Conti leaks.[1] With recent IBM research indicating that a successful ransomware attack costs companies a staggering average of $4.54 million (the ransom not included)[2], its economic effects continue to wreak havoc among companies – especially now that this accessibility to RaaS platforms has exponentially increased the pool of potential cybercriminals.

$4.54 million

The average cost of a successful ransomware attack per company – ransom not included

Source: IBM [2]

[1] **TechCrunch (2022).** Conti ransomware gang's internal chats leaked online after declaring support for Russian invasion.

[2] **IBM (2022).** Cost of a data breach 2022. A million-dollar race to detect and respond.

As an example, the well-known REvil RaaS operation sent shockwaves through the business world in 2021 with its massive supply chain attack on software provider Kaseya, affecting thousands of companies globally. The incident involved an unprecedented ransom demand of $70 million – the largest to date.[3] Although Kaseya opted not to pay, other high-profile RaaS victims, such as insurance company CNA Financial and Brazilian meat producer JBS, made the news with some of the biggest ransom demands ever paid, amounting to $40 million and $11 million, respectively.[4]

Top 10 ransom payments by companies

Project	Ransom payment	Ransomware Strain	Origin
CNA Financial	$40,000,000	Phoenix	Russia
JBS	$11,000,000	REvil/Sodinokibi	Russia
CWT	$4,500,000	Ragnar Locker	N/A
Brenntag	$4,400,000	Darkside	Eastern Europe
Colonial Pipeline	$4,400,000	Darkside	Eastern Europe
Travelex	$2,300,000	REvil/Sodinokibi	Russia
UCSF	$1,140,895	Netwalker Ransomware	N/A
BRB Bank	$957,245	LockBit	Eastern Europe
Jackson County, Georgia	$400,000	Sam Sam	Iran
University of Maastricht	$218,000	Ciop Ransomware	Russia

Source: Immunefi [5]

The RaaS group HIVE also grabbed headlines last year for their widespread cyberattacks. HIVE didn't just target major IT and oil multinationals but also compromised the data and computer systems of healthcare and public organizations. Since June 2021, HIVE's attacks have impacted over 1,500 companies across 80 countries, resulting in nearly €100 million in ransom payments from its victims.[6]

A new player, Sugar Ransomware, first detected by the Walmart Security Team in November 2021, is now even actively focusing on individual devices rather than large corporate networks.[7] By shifting their focus from high-profile whaling to individual consumers and small businesses with lower ransom demands, these cybercriminals expand their potential victim base while minimizing the risk of law enforcement scrutiny. This demonstrates how cybercriminals are forging alliances, pooling resources, and learning from one another, ultimately paving the way for more **coordinated and effective attacks**.

[3] **The Guardian (2021).** Ransomware hackers demand $70m after attack on US software firm Kaseya.

[4] **Cybernews (2023).** Crooks netted $70m in top 10 ransomware attacks.

[5] **Immunefi (2023).** Top Crypto Ransomware Payments Report.

[6] **BBC News (2023).** US hacks back against Hive ransomware crew.

[7] **BleepingComputer (2022).** A look at the new Sugar ransomware demanding low ransoms.

Navigating a minefield: Building partnerships in a complex global network

The Kaseya attack not only showcases the extreme power of ransomware-as-a-service, but also how the professionalization of cybercrime has led to a dramatic **increase in the scale, impact, and complexity of supply chain attacks** – leaving companies vulnerable in an interconnected digital landscape. In the attack, cybercriminals targeted the company's VSA software, a remote management tool used to monitor and administer IT services for customers.[8] By infiltrating this software, the attackers were able to simultaneously compromise the systems of thousands of companies that relied on Kaseya's services, which is a stark reminder of how much **our security depends on the security of others**.

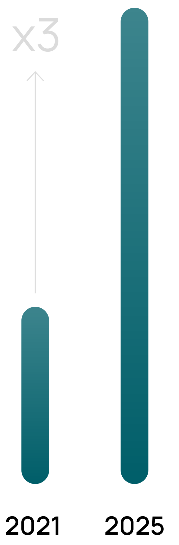
8 in 10

security professionals say their organization's security is increasingly **dependent on the security of their partners and suppliers**

In supply chain attacks, attackers tend to exploit the **weakest links**, often smaller, less-secure suppliers or service providers, to gain entry into their primary target organization. One clear example of this modus-operandi happened early this year, when Nissan North America announced that one of its software development vendors suffered a data breach that exposed full names and dates of birth of thousands of Nissan customers.[9]

A recent active attack targeting 3CX's Desktop Client is also showcasing the potential reach of targeting digital supply chains. 3CX is the developer of a software-based phone system used by more than 600,000 organizations globally, including BMW and McDonald's.[10] The SolarWinds-style attack employs trojanized 3CXDesktopApp installers to infiltrate infostealer malware into corporate networks, harvesting system information and stealing data from popular web browsers.

There are no indications that this trend will relent anytime soon. In fact, Gartner forecasts that by 2025, 45 percent of organizations worldwide will have fallen victim to digital supply chain attacks, a three-fold increase from 2021.



45%

of organizations will have experienced attacks on their digital supply chains by 2025.

Source: Gartner [11]

With organizations finding themselves more reliant on third-party services and software to keep up with the speed of our evolving digital landscape, it's crucial that they ramp up their security strategies to navigate today's complex digital supply chains.

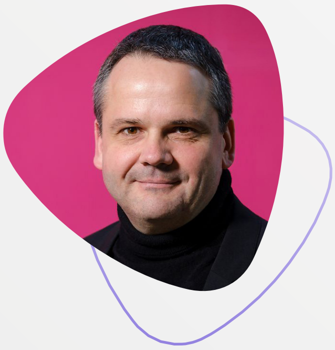
[8] **TechRepublic (2021).** Kaseya supply chain attack impacts more than 1,000 companies.

[9] **Cybernews (2023).** Nissan data breach exposed clients' full names and dates of birth.

[10] **Techcrunch (2023).** There's a new supply chain attack targeting customers of a phone system with 12 million users.

[11] **Gartner (2022).** Gartner Identifies Top Security and Risk Management Trends for 2022.

> “When we start working with new types of technology, we must consider the risks from the very start. Otherwise, it will end in disaster.



Thomas Tschersich
CSO at Deutsche Telekom and CEO at Telekom Security

Thomas Tschersich is Chief Security Officer (CSO) of Deutsche Telekom AG and Chief Executive Officer of Telekom Security. He is in charge of cyber security and all other operative security matters at Telekom. Tschersich, who holds a degree in Electrical Engineering, is Chairman of the Board at the Deutschland sicher im Netz initiative. In addition to his many advisory roles, he is a member of the Cybersicherheitsrat and the UP KRITIS Advisory Council.

Do you think there are problems with how companies interpret security and configure their strategies?

Security has a lot to do with attitude. Many security teams completely prohibit or unnecessarily complicate things. But I think that you must find a compromise between security and convenience every day because if I don’t consider the importance of the latter, users will find a way to circumvent the security measures.

Do you have any examples?

You see it in all sorts of areas. When you force people to constantly change their password, the password will become weaker each time. Even if they’re made to go through complicated multifactor authentication, problems like “MFA fatigue” – when cybercriminals request authentication until the user is too exasperated to continue and finally confirms – will be quick to follow. And if you ban USB sticks, people might send sensitive files to their personal email account so they can copy them from there. This begs the question of which is better: keeping the file on a protected and monitored USB stick or in a personal account?

I firmly believe that security measures need to be transparent and comprehensible. If people understand why certain measures and processes are being implemented, the motivation to abide by them is much greater. If they don’t understand, it becomes more bothersome, and they’ll try to find a way around it.

Many companies have long treated security policies like a checklist of tasks. Do you believe they’re still relevant today?

When I joined Telekom, I was also in charge of policies. Now, I joke that I was writing policies, and 200,000 coworkers were ignoring them. Of course, I have to write certain things down purely for compliance reasons, and that's fine. But I've never accomplished anything with policy alone. And I've never heard of a hacker who was scared off by a company's security policy.

I think that taking only the formal route is one of the biggest mistakes we can make when it comes to security. ISO-27001 certification doesn't make me secure, either – it just shows that I'm capable of being secure. We can't hide behind these regulations and certifications.

What do you rely on instead?

Practicality is more important to me, including things like patch management that lets me quickly repair any vulnerabilities. We keep our policies minimal and use them to describe our general security requirements, giving us more time to actually implement measures. We work out our security needs in our privacy and security assessment process and can immediately take suitable technical and organizational measures accordingly. I think this is much more effective and nips security issues in the bud.

What advice do you have for organizations so that they can devise a good security strategy?

Many companies don't have a security strategy because they're afraid of how complex it might be. I'm a strong advocate for finding simple solutions right away, so we show these companies that there are many individual steps that go into making a security strategy. Let's start with software updates, which already puts you in a good position. Then, they can invest in technical defense systems, such as virus and endpoint detection and response, so that they're better fortified. Next comes employee awareness, but this is a never-ending process.

How can companies improve employees' awareness of security issues?

Security awareness used to be synonymous with web-based training. For me, that means I click through everything quickly and answer a few questions. It gave me a negative impression of the entire idea, and employees found it more annoying than enriching.

How can this be made more effective?

Security awareness should be entertaining and give employees a secondary benefit by applying it to their personal lives as well. Then, they'll view security as an aid, and people will adapt their behavior accordingly. Feedback for learners is especially important because when we simulate phishing attacks, it's pointless if users only learn what's going on weeks after the fact. Users need direct feedback as the situation unfolds, which is when they are most attentive and the learning effect is the strongest.

“Attacks have become extremely sophisticated, and that’s dangerous.

We’re witnessing a range of new attack methods and trends that concern security. What are you seeing in this regard?

I’m always wary of the word “trend.” The big buzzword used to be “blockchain,” and before that, it was “Cloud.” We shouldn’t always be using these fads as our guiding light. In my opinion, the biggest problem is that we aren’t taking care of the basics.

But I see numerous topics that impact security: identity theft (via phishing or CEO fraud calls), DDoS attacks, and ransomware. These are currently the main vectors we need to talk about, and a lack of software updates is often a root cause.

Then, there’s awareness: You click on files out of curiosity or because you want to help someone out, and you’ve opened Pandora’s box. Attacks have become extremely sophisticated, and that’s dangerous. It used to be that we would notice a typo or see that text was machine-generated and would know immediately that it’s not a genuine message. We’ve long since moved past that, and phishing emails aren’t recognizable at first glance anymore.

Machine learning has long been used as a measure of defense. Now, we’re seeing generative AI that makes it easier to conduct new types of voice cloning attacks, among other things. Do you see attacks like these “in the wild”?

We have seen voice manipulation in CEO fraud calls but with artifacts. The greatest challenge lies in the fact that we’re all used to video conferences, and this new technology makes it easier for fake participants to sneak into these calls. As a result, we’ll have to take a different perspective of “digital identities” in the future. We need an “identity of everything,” so to speak, for services, machines, and so on.

Are you seeing a change in how security is viewed at the executive level?

A change in perception, yes, but not necessarily a change in behavior. Security is a main discussion point in every meeting with customers, but I still often hear the old saying, “If it’s not broken, don’t fix it.” But when an attack does happen, the consequences can be severe.

Ultimately, prevention is always the better option. Is this even more pertinent at a company that has been affected in the past?

Unfortunately, it's usually just a short-term effect. The departments often plan and analyze after an attack, but once the plan becomes more detailed and could cost a few million euros, the attack is so far in the past and the pain has diminished to the extent that the money doesn't get invested in security. This is especially common in smaller companies. Awareness looks different in corporations, but they also have entire teams dedicated to it.

Security is often seen as an indirect pool of costs not relevant to productivity. However, a direct pool of costs can form very quickly whenever security is absent. The long-term damages can be immense.

Which top technologies would you recommend to other CIOs/CISOs?

The Cloud has fundamentally changed the world. Security used to be ensured by network integrity, but that doesn't work anymore, and Amazon and Microsoft provide some firewalls. This means that I must focus on the application levels, such as identity management, encryption, and rights management. The trend of working from anywhere is also making the endpoint more important. I always have to be able to check how trustworthy a device is at a given time, requiring a combination of EDR solutions and conditional access. Last but not least, the infrastructure should be patched and monitored regularly. Awareness measures allow companies to tick these technical measures off their list so that they can then focus on specific problems while educating employees at suitable intervals and in a way that's more relevant to them.

> I often hear the old saying, 'If it's not broken, don't fix it.' But when an attack does happen, the consequences can be severe.
>
> **Thomas Tschersich**
> CSO at Deutsche Telekom

Burnout and staff shortages: Security teams' biggest fears amidst rising cyberthreats

While cybercriminals are continuously professionalizing their business models and innovating on new schemes, it's no surprise that excessive workload and burnout drive many security professionals to resign from their positions. A study by the Information Systems Audit and Control Association (ISACA) revealed that in 2022, **60 percent of organizations faced challenges in retaining skilled cyber security professionals**, with stress at work being one of the top reasons to hand in resignations.[1] This situation is aggravated by the 3.5 million worker shortage the cyber security industry is currently experiencing.[2]

3.5 million

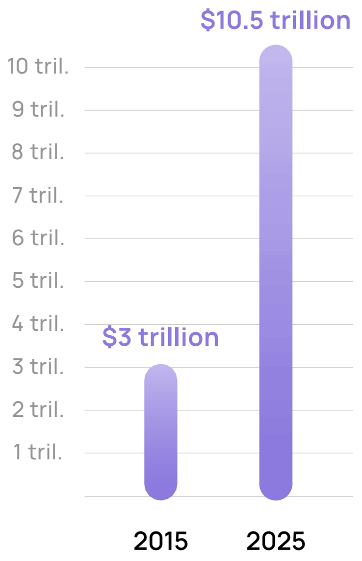
worker shortage in the cyber security industry

Source: Chartered institute of information Security [2]

[1] **ISACA (2022).** State of cybersecurity 2022: cyber workforce challenges.

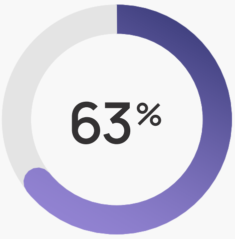
[2] **Chartered Institute of Information Security (2022).** The security profession 2021/2022.

Consequently, the remaining security professionals are finding it increasingly difficult to keep up with the fast-paced evolution of cybercrime – a global industry whose costs are expected to reach $10.5 trillion annually by 2025, up from $3 trillion in 2015.[3]



Source: Security Magazine [3]

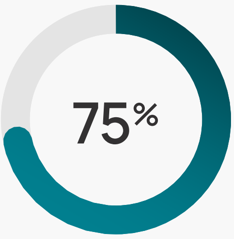
The previous chapters already showed how cybercriminals are constantly developing new strategies and exploiting emerging technologies, further straining the limited resources of already overworked security teams. This creates a vicious cycle where inadequate staffing contributes to burnout, which in turn exacerbates the industry's struggle to stay ahead of evolving cyberthreats.



of security experts say they feel stressed due to the increasing cyber security threats

Hybrid work models are also straining cyber security efforts

Even if some employees across the globe are transitioning back to their offices following two years of remote work, the hybrid work model remains on the rise, with a growing number of organizations adopting this flexible approach to work. However, the convenience and cost-effectiveness of the hybrid work model are accompanied by an elevated risk of cyber security threats.



of security experts believe that remote/hybrid work increases the risk of cyberattacks

Several key factors contributing to this heightened risk include:

- **Vulnerabilities in home networks:** Home Wi-Fi networks are often less secure than corporate ones due to factors like weaker encryption, default settings, and lack of regular updates – which facilitates cybercriminals' access to sensitive data.
- **Reliance on remote connectivity:** Remote workers are more likely to work on the go, such as taking their final calls of the day on a train via public networks – increasing cyber risks significantly.

[3] **Security Magazine (2023).** One of the biggest threats of a cybersecurity team? Employee burnout.

- **Cognitive overload:** Virtual interactions strain our brains, reducing concentration and increasing the effectiveness of phishing scams. Cybercriminals exploit this by targeting individuals when their guard is down, such as at the end of their workday.[4]
- **Expanded use of collaboration tools:** Remote work settings often involve greater reliance on tools like Microsoft Teams, presenting new channels for cybercriminals to exploit.
- **Insufficient employee training:** The rapid shift to hybrid work models has left some employees without sufficient cyber security training.

> Many users are less focused when working from home, and it's a more relaxed environment. They mix a lot of personal activities into their workflow, resulting in inattentiveness.
>
> **Dr. Stefan Lüders**
> Computer Security Officer at CERN

The result: Burnout as a new favorite attack vector

The combination of stress, understaffing, and an increased attack surface due to new work models creates an ideal environment for cybercriminals, who **capitalize on fatigued cybersecurity experts** more prone to missing details and struggling to resolve issues effectively.[5]

> The number one challenge in the cyber security industry right now is burnout: There's too much data, too many cases, and not enough time.
>
> **Stéphane Duguin**
> CEO at CyberPeace Institute

Moreover, security teams must not only ensure the protection of other departments within the company and quickly address attacks aimed at them, but they are also considered to be among the departments with the highest risk of falling victim to cyberattacks themselves, according to our survey respondents.

Top 3 departments that are at the highest risk of being targeted in cyberattacks

1. IT
2. Finance
3. Security

Aware of the vulnerabilities that emerge when security teams are under stress, cybercriminals are using burnout as a new attack vector and are inclined to scrutinize their composition and specifically **target organizations with teams that appear more susceptible** from an external perspective.

This highlights the need for organizations to invest in employee retention, proper resources, and continuous training to empower their security professionals and foster a resilient security culture, effectively navigating the complex threat landscape.

[4] **VentureBeat (2022).** Why hybrid work is leading to cybersecurity mistakes.

[5] **Security Magazine (2023).** One of the biggest threats of a cybersecurity team? Employee burnout.

> It’s important that cyber and information security strategies are always viewed from three perspectives: the people, the technology, and the process.

Tobias Ludwichowski
CISO at Signal Iduna

Tobias Ludwichowski has a background in industrial engineering, and has held a variety of roles at the SIGNAL IDUNA Group since 2015. These have included supervisory roles in risk management and IT governance, his role as head of the Chief Information Security Office since 2022, and serving as CISO for the SIGNAL IDUNA Group’s German insurance companies.

Has the perception of information security changed over the years, especially at the top management and advisory board level?

Regulatory law concerning information security for insurance providers is expanding rapidly, with more laws and regulations being passed over time. The German Federal Financial Supervisory Authority has been taking an active approach to this for some years now.

Altogether, there’s a lot of pressure being placed on top management when it comes to this topic, coupled with an increasingly complex threat situation that we’re facing. This is why cyber security awareness at the top management level has become quite high, and has risen drastically in recent years. Thankfully, the resources that can be invested here have also become more widely available.

Let’s take a closer look at insurance in the cyber world: What market trends can you see in this area as an industry representative?

We’re seeing a tendency for cyber insurance to be geared toward few providers who are prepared to expand their coverage for cyber risks. This is because the cyber risk is difficult for a company to gauge and comprehend when we’re also facing a highly dynamic marketplace of threats. It's extremely difficult to objectively determine how well a company is covered against cyber risks both now and in the future.

The insurance also has to be appealing to the customer. For example, it doesn't do medium-sized companies much good if the coverage is capped at 200,000 euros. We also have to ensure that companies continue to actively combat the risk even with cyber insurance coverage and that they don't get complacent. This makes cyber insurance challenging at this point in time.

How can information security be made less obscure and turned into a joint project that – ideally – everyone wants to take an active role in?

You have to take a two-pronged approach: The first is continuous communication and training to make the potential effects of security incidents visible. For example, it helps to actively inform your employees of the threat situation and certain behaviors. This can also have an impact on security outside of work, which makes the topic all the more palpable, letting them know they need to protect their personal accounts as well.

Secondly, we must ingrain the topics in processes to the extent that employees don't even necessarily know that they're helping to improve security. Processes have to be configured such that employees are automatically compliant, and this feels like less work for the employees in the long run. Sending out guidelines and expecting them to be read, understood, and translated into correct behavior won't work.

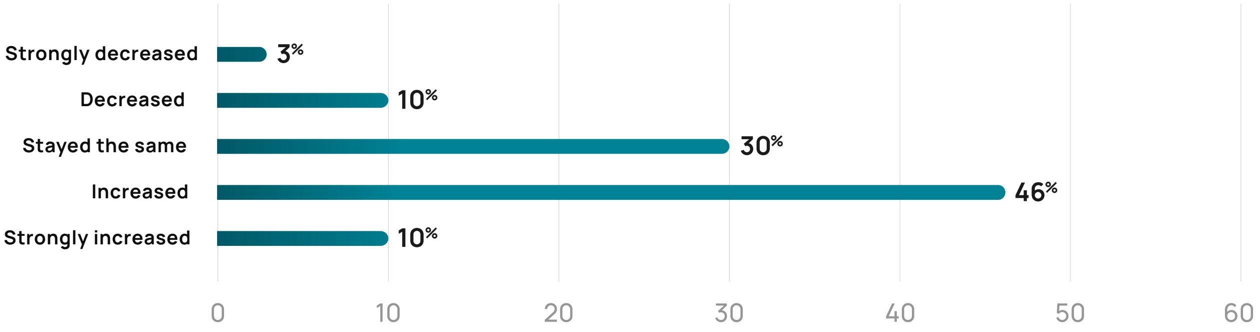
> “The best tools won't do anything if there aren't any suitable processes and if employees aren't able to recognize the risks.
>
> **Tobias Ludwichowski**
> CISO at Signal Iduna

Security as a top management priority: Why security is starting to have a seat at the executive table

In response to all these challenges, organizations are starting to make security a top management priority. In fact, **56 percent of security experts claimed that their top management is focusing more on cyber security** than in the previous year.

This shift in organizational mindset toward treating security as a core component of business strategy, risk management, and long-term business success – rather than just an IT issue – **is leading to significant changes in corporate structures**. By integrating security at the board level, companies can more effectively align their security strategies with business goals, allocate the necessary resources, facilitate change, and establish clear lines of accountability. Our survey also emphasizes the benefits of the growing importance of cyber security in the boardroom.

How, if at all, did your top management's focus on security increase or decrease last year?



Organizations whose top management is aware of cyber risks are

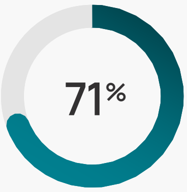
↗ 67 %

more likely to have enough resources to cover their security topics than when top management is unaware.

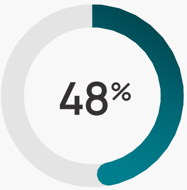
Gartner also forecasts that by 2026, at least **50 percent of C-level executives will have cyber security risk performance requirements** in their employment contracts.[1] This development is bound to influence the speed and quality of information risk decisions, as they will be increasingly made by stakeholders outside IT or security, and prompt a relocation of formal accountability toward other business leaders. Considering this, countries like the US are starting to implement cyber security regulations that affect board members. The SEC (Security and Exchange Commission) proposed a rule in March 2022 that public companies must disclose whether their boards have members with cyber security expertise because investors may find it important when making investment decisions and voting on directors.[2]

This attention from the board to cyber security is considerably impacting the cyber resilience of organizations – also **in the human layer**. According to our survey, the perceived level of security awareness in a company is significantly influenced by the awareness of its top management: 71 percent of security experts that believed their top management is highly aware of cyber risks rated the security awareness in their organization as much higher than those who believed their top management lacks awareness (48 percent).

Perceived level of security awareness depending on top management awareness



of experts say overall awareness in their organization is high when top management is aware



say overall awareness is high when top management is unaware

Surviving the threat landscape: The need for adaptability in the boardroom

> Cyber is a rat race – it's fast-paced, and you always have to learn and keep up. That is why it is so important to develop new models, such as putting younger people with specific expertise in advisory board positions even if they have never run a company before or investing more heavily on trainings.

Dr. Katrin Suder
Strategy Expert (digital technologies, business & politics)

[1] **Gartner (2022).** Gartner Says the Cybersecurity Leader's Role Needs to Be Reframed.

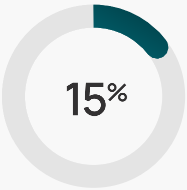
[2] **Harvard Business Review (2022).** Is Your Board Prepared for New Cybersecurity Regulations?

Keeping up with the ever-evolving cyber landscape can feel like running a never-ending race that's constantly picking up speed. While top management – usually more used to relying on their accumulated experience to address situations – is beginning to prioritize cyber security, not all board members have extensive experience with digitalization and cyber issues. That's why it becomes crucial to have an open mind about both **continuously educating and training leaders but also creating new board structures** like adding more specialized positions, even if those individuals have less business acumen. Another option is to regularly invite the security team to board meetings to engage in open and honest discussions about the company's security posture and how it impacts overall risk. Adaptability and collaboration to identify high-risk areas and establish security-related goals that reduce overall risk can significantly enhance cyber resilience.

Cyber security budgets are going up, but that's not enough

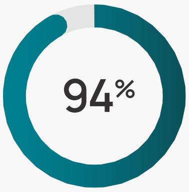
In recent years, there has also been an upward trend in organizations investing in cyber security. Gartner predicts that **global spending on security and risk management is expected to increase by over 11 percent in 2023**, reaching $188 billion, up from $158 billion in 2021.[3] This is a positive development as it aligns with the trend of organizations prioritizing cyber security by often including it in their boardroom agendas. In fact, according to our survey, only 15 percent of companies that don't have enough security resources can make their security culture a priority compared to 94 percent of those with sufficient resources.

However, effective cyber security requires an approach that doesn't only include investment in technology and tools. Aligning security efforts with business goals and making cyber security a priority in the top management are also very impactful initiatives, but all that also needs to be part of a comprehensive strategy.



Among companies lacking adequate security resources only 15% prioritize their security culture

whereas



94% of companies with sufficient resources do so.

As the frequency of cyberattacks increases at a greater pace than the rise in security budgets and attackers recognize the high success rates of exploiting the human element – with over 82 percent of data breaches involving the human factor [4] – the need for **effective cyber security awareness training measures** that effectively foster secure habits in employees is now of paramount importance.

[3] **Gartner (2022).** Gartner Identifies Three Factors Influencing Growth in Security Spending.

[4] **Verizon (2022).** 2022 Data Breach Investigations Report.

Mar 20
Apr 20
Mai 20
Jun 20
Jul 20
Aug 20
Sep 20
21.39%
04.55%
23.98%
65.98%
Q3
Operating Cost:
Making Department
Film Departmeent
Post Department
Compare

> We often talk about IT costs being too high, but IT investments are a lever to enable business growth, improve service quality, and save costs in each business department via automation.

Jens Becker
CIO & CDO at Zurich Gruppe Deutschland

ZURICH

Jens Becker has been Chief Information Officer and Chief Digital Officer of Zurich Group Germany since January 2021 and is driving the “Accelerated Evolution” of Zurich IT in this role. Previously, Becker worked in IT consulting at KPMG and in various IT leadership roles at AXA for more than 12 years. He was responsible for several digitalization projects, introduced DevOps as division head of IT operations and initiated AXA's cloud migration, among other projects.

In your opinion, what needs to happen for top management to become more involved in security awareness?

Most managers understand intellectually that security is or must be a priority. The question is whether this realization will be put into practice, whether it will lead to sustainable security awareness, or whether, in specific situations, it's still more convenient not to lock the computer or encrypt the data.

I believe we shouldn't only focus on the corporate level but also on other levels in order to increase the overall security awareness in society and make people comprehend the real threat situation, the need for cyber resiliency, the correct way to handle sensitive data, and so on. In fact, it should be a mandatory subject for everyone, starting in school. Students need to understand that their passwords and identities can be stolen. We must raise their awareness without scaring them so that they learn to deal competently with attacks.

At the company or corporate level, the expectations are, of course, even higher. Employees must handle their customers' data sensitively and be especially aware of their responsibility in this context. We also discuss this at the Board level and underline that each department is responsible for addressing topics like authorization concepts, business continuity management, and individual data processing.

At a recent event, you talked about the fact that companies should save money with IT and not on IT. Can you elaborate?

Absolutely. We often talk about IT costs being too high, but IT investments are a lever to enable business growth, improve service quality, and save costs in each business department via automation.

We should automate repetitive simple activities so that our customer support team can focus on more valuable tasks. Chatbots are a cost-effective solution for handling calls, legitimating customer requests, and classifying their concerns. This way, the employee in charge can focus on resolving the actual concerns. Automation also helps align response times with customer expectations. We used to wait two weeks for a response to a physical letter, but for an email, we expect a response within two days. Fast processing, or "first time right," increases customer satisfaction and reduces processing costs.

Speaking of digitalization, we should also focus on digitizing our physical output, letters for example. This is still an area where our industry has a lot of work to do and where investments will be rewarded with reduced postage and paper costs and minimized CO2 emissions.

So, is it better to invest today to minimize risks?

Definitely. It's better to install a firewall today than to have to extinguish the fire tomorrow and pay the repair costs. But the question of the "proper balance" remains. Some official guidance says companies should invest 7 percent of their IT budget in security. However, you could ultimately invest your entire budget in security and still not be completely secure. That's why you need a risk-adjusted approach that focuses on the top risks. Standards like NIST and ISO provide orientation. These can also serve as a signal to your partners in that you can prove you have achieved a certain security level. Overall, it's important to continue to invest and never rest on your laurels.

In general, are companies investing sufficiently? Or is security still seen as a project that will supposedly be completed at some point?

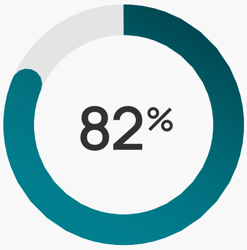
Yes and no. To the first question: I think a lot is being invested, but it's never enough. That's why Zurich follows a so-called "forced ranking approach," which involves creating a risk matrix where we enter our security risks and gradually address them according to this matrix.

Regarding the second question: We have been doing this for several years now, and we will not stop in the future.

> "It's better to install a firewall today than to have to extinguish the fire tomorrow and pay the repair costs.

Outlook:
Why we need to embed cyber security into our everyday lives

The previous chapters have shown how cybercrime has evolved into a highly professionalized and large-scale operation. Attackers exploit vulnerabilities every second and employ innovative and sophisticated tactics at every turn. This ever-evolving landscape poses immense challenges to businesses, governments, and individuals alike as they strive to safeguard their assets in an increasingly interconnected world. The most concerning aspect is that **the situation isn't likely to improve** in the near future: According to our survey, 8 in 10 security professionals predict that the threat landscape will not ease within the next 12 months.



of security experts predict that the threat landscape will not ease in the next 12 months

A deeper dive into the data additionally showed that social engineering remains at the core of cyberattacks, irrespective of the many technical precautions companies already have in place. As email-based attacks are still incredibly popular among cybercriminals and other channels like social media and collaboration tools are progressively gaining momentum, organizations are starting to recognize the value of a strong security culture that places the human factor at the heart of their security strategies.

> Thousands of harmless spam emails come in all the time. The problem is that, despite several security checks, dangerous phishing emails also make it to our inboxes. Employees need to know how to avert the risks – that's why awareness training is so important for us.

Frank Heymann
Senior IT Team Manager at Buhlmann

Effective cyber security awareness training then becomes a key factor for companies to navigate this intensified threat situation and enable employees to proactively protect their organization – extending beyond email to include all newly emerging communication channels.

> Companies have invested more in technology than in people over the past 10 years. They've since come to understand that technology isn't everything, and that social engineering – especially phishing – is a real problem. Many of those companies are on the right path now, but still have some catching up to do.

Dr. Katrin Suder
Strategy Expert (digital technologies, business & politics)

Our best chance lies in security awareness training

> Human behavior is always most easily detected by other people. If you rely 100% on technology and assume that it will catch everything, you're making a big mistake.

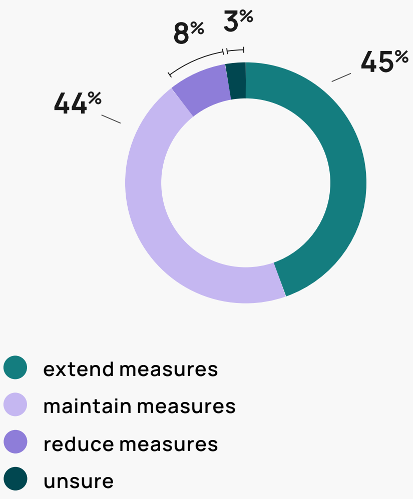
Tobias Ludwichowski
CISO at Signal Iduna

The good news is that many IT and security departments are already aware of the need to address the human factor in their organizations. Our survey shows that the top priority of security experts in organizations is improving the security awareness of employees, followed by identity and access management, and securing hybrid work and existing processes. In addition, 9 out of 10 experts also answered that their company will maintain or increase their security awareness measures.

Top priorities for IT and security departments

1. Improving employees' security awareness
2. Identity and access management
3. Securing hybrid work
4. Securing existing processes

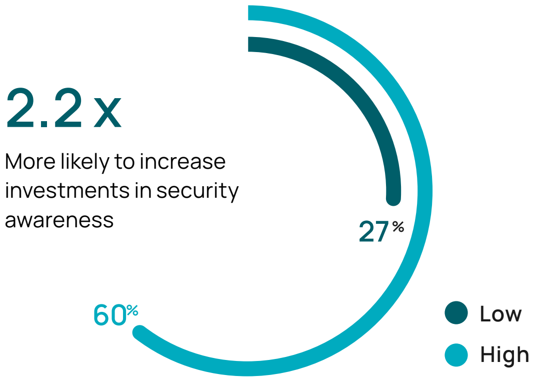
What are your plans in terms of extending or reducing security awareness measures in 2023?



And this requires continuous support from the board

The previous chapter already addressed how relevant it is that security concerns are recognized and discussed at the board level, a point which our survey data strongly supports: There is a direct correlation between top management's awareness of cyber risks and the prioritization of investments in security awareness initiatives.

High top management awareness vs. low top management awareness



Our survey further reveals that **94 percent of companies with adequate resources for cybersecurity consider building a security culture a priority** within their organization. In contrast, of those companies lacking sufficient resources for cybersecurity, only 15 percent prioritize building a security culture. This disparity further underscores the significant impact that resource availability and top management's awareness have on an organization's commitment to cyber security.

That is why it is essential for security and IT teams to continuously communicate with the board and to back up their call for action with success metrics and KPIs. By focusing not only on measuring performance with metrics such as click rates, but also on explaining how behavior changes over time and how it impacts overall security (for example, how having a phishing report button increases reporting rates over time), they can ensure cybersecurity remains a priority in the years to come.

Behavioral science: The present and future of security awareness

Although security awareness might not be a new term in companies of all sizes and industries, it is now witnessing a transformative shift to be able to effectively address all the challenges we are currently seeing. **Traditional training models**, which primarily focus on fulfilling regulatory obligations, **are not enough** to win employees' attention and engagement, and to combat the current threat landscape. Our survey data reflects these limitations:

The top 3 reasons users struggle with security awareness training:

1. Amount of time it takes
2. Information is too generic
3. Training is too repetitive

This shows clearly that organizations need to cultivate a strong security culture by moving beyond mere compliance and instead actively fostering secure habits among employees, while adapting to their work models and busy schedules. To achieve this, **security awareness programs should be completely human-focused** and incorporate **behavioral science-led** methods such as micro-learning, gamification, and nudging to enable employees to make informed decisions not only in their daily work activities, but also in their personal lives.

By moving cyber security to where people are, integrating it seamlessly into their daily lives, organizations will foster widespread awareness across all spheres and achieve an advantageous synergy between cyber security and business operations.

This proactive strategy is crucial to combat the relentless, billion-dollar cybercrime industry that we face today. To stay ahead of the game, we need to adapt and evolve at the same breakneck pace as the constantly shifting threat landscape.

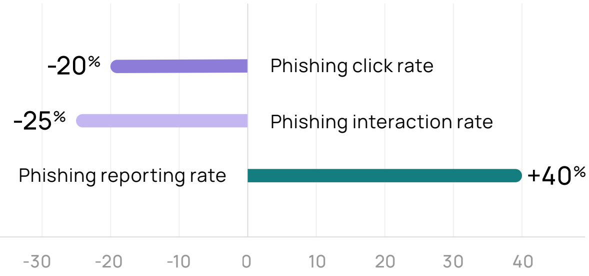
Driving sustainable behavioral change

There are a variety of approaches and methods that help organizations make the most of their awareness initiatives and meet their employees in their individual contexts. For example, **spaced training** consistently delivered via different channels lets users repeat what they have learned at a pace that promotes sustainable learning effects. Another example of such an approach is **nudging** in the form of regular, automated system emails that nurture interactions with users and keep awareness in front of mind. **Micro-learning** is also a powerful approach to reinforce learning and boost retention. On the SoSafe Awareness Platform, this takes the form of snackable and easy-to-follow e-learning content with character-based storylines to improve engagement.

These behavioral science-based approaches in awareness training translate into higher module completion rates that, in turn, reduce phishing click and interaction rates, while increasing reporting rates. This lets organizations move a significant step closer to securing their assets and proactively fending off attacks.

Product usage

Results from users with high module completion rate



To phish or not to phish

Another factor that contributes to the effectiveness of awareness training is whether it is contextual. A successful example of contextual awareness measures are **phishing simulations** that put the behaviors users have learned through micro-modules or other learning activities to the test. This implicit and incidental learning experience makes secure habits stick through realistic threat simulations in daily situations. Many experts agree that the combination of simulations with in-situation learning experiences helps reduce risks effectively:

> In a world where everybody's overwhelmed with information and doesn't have the time to learn, it's essential that employees receive their learning units cut into very small pieces, and then present it at the point of failure, when the motivation to learn is very high. One example is a learning page after you click on a phishing simulation email. Five-minute slices of security awareness training fit perfectly into a very busy workday.
>
> **Martin Schmidt**
> Global Director of Digital Advisory
> at Freudenberg Home and Cleaning Solutions

> It’s especially important that people who are learning receive feedback. When we simulate phishing attacks, users need direct feedback as the situation unfolds. This is when they are most attentive, and the learning effect is the strongest.

Thomas Tschersich
CSO at Deutsche Telekom

> After interacting with a phishing simulation and the subsequent lightbulb moment, most users end up with a better understanding of digital risks and how to handle them.

Dr. Stefan Lüders
Computer Security Officer at CERN

Incorporating **contextual components and tools** within the existing infrastructure can enable employees to take an active stand against cyberattacks. For example, employees who have access to the SoSafe **Phishing Report Button** show a 30 percent lower interaction rate with phishing emails as compared to those that do not have this functionality. That means attacks are less likely to lead to success with this contextual feature, which also offers additional tangible advantages:

Impact of phishing report button

↗ 38%
E-learning adoption rate

↗ 25%
Module completion rate

The call for innovation: Which behavioral features companies are requesting

In our survey among European security professionals, we asked which additional features they thought would have a greater impact on their awareness training. They said:

The biggest levers for greater security awareness impact according to security professionals

1. Awareness measures via communication apps
2. Personalized learning
3. Program customization

This illustrates that security professionals are understanding the need for bringing security closer to the people. **Multichannel awareness** is one way to do this and it trains teams via a more conversational approach. Rapid awareness features that provide alerts about new attack tactics through different communication tools like Microsoft Teams are one method for closely integrating security into everyday work schedules. **Personalized learning** that takes into account the different roles and responsibilities of each employee in order to customize their learning experience to their needs is also perceived as one of the most impactful features for an awareness program – underlining again that security needs to meet employees in their individual contexts.

Finally, **program customization** including features like being able to customize the e-learning to the company brand or adding the company's own information security content and policies, is thought to be an impactful lever for greater awareness success. The underlying message: Security is not a one-size-fits-all approach. It needs to adapt to the people and organizations involved to be successful.

Recommended Actions

The heart of the issue:
Security measures need to align with ever-adapting human behaviors

1

Security should sit on top of everything

If the cybercrime landscape shows us one thing it is that security is something that affects us all. Neither individuals nor organizations can deny anymore that digitalization and technological progress have made us susceptible to all sorts of threats online. To effectively protect ourselves from increasingly advanced attacks, we need to move security best practices to the core of our everyday lives. At the same time, organizations are well-advised to take security issues to the board – and work on finding ways to grow business and cyber even closer together. Because in the end, security measures can only unfold their full potential if they are given sufficient priority in the overall organizational context. Fighting for resources will be a thing of the past if organizations succeed in underlining the extent to which cybercrime affects not only individuals, but also business success.

2

Behavioral change is the key to long-term success

A sensible and tangible way of communicating security and awareness achievements to stakeholders in the entire organization is behavioral metrics. In the past, companies have often relied on performance metrics alone, including phishing click rates or e-learning completion rates. Although these are a first step toward illustrating the awareness levels of employees, what is actually crucial in convincing decision makers of the need for awareness training is how successful security measures are in changing the status quo. In the area of awareness, behavioral metrics like phishing reporting rates and the development of risk scores are prime examples. As data from our survey shows, although 1 in 2 organizations still rely on traditional metrics, behavioral metrics are already used by a third of companies and further gaining importance. With cybercriminals focusing more and more on social engineering, behavioral metrics and human risk scores will be the one thing that can reliably show how well protected companies are against sophisticated threats.

3

Adapt, adapt, adapt

Cyber security is one of the domains that probably has gone through the greatest evolution in the past years and decades. And the reason is all too clear: Technological advancements have made a standstill impossible. But things are accelerating further. This shows how organizations need to be even quicker in adapting their current strategies to new circumstances, including the increasing professionalization of cybercriminals' business models and the evolving complexity of the threat landscape. Not only do security teams need to move from checking off compliance requirements toward making security an integral part of overall business strategy, but they also need to make sure the measures are still in line with what people experience as well as their individual risk contexts. Continuously adapting awareness measures in a situation where security resources are scarce and teams are burnt-out might be a challenge, but it's one that can be overcome by working with the right partners.

4

Place people at the heart of it all

Ultimately, amidst the daunting circumstances we face today, it is essential to focus back on the human factor in security. It's people who are attacked, it's people who suffer from the consequences of attacks, and it's people who can ultimately prevent attacks. Building strong security cultures in organizations – and a strong security mindset in our private lives – is something that will help us all tremendously to avoid the devastating effects professionalized cybercrime might have in the future. Making sure security strategies are aligned to people's needs and making use of insights from behavioral science will be our best chance at protecting ourselves. Because if we can be sure of one thing, it is that criminals will continue to innovate. We must remain alert, adjust to our current reality, and proactively equip individuals for the challenges that lie ahead.

Scale your security culture with ease

With its awareness platform, SoSafe empowers organizations to strengthen their security culture and mitigate human risk. The platform delivers engaging learning experiences and smart attack simulations that help employees become active defenders against online threats – all powered by behavioral science to make the learning journey fun and effective. Comprehensive analytics measure the behavioral change impact and tell organizations exactly where vulnerabilities lie so that they can proactively respond to cyberthreats. The SoSafe platform is easy to deploy and scale, effortlessly fostering secure habits in every employee.

TEACH —

Engaging Micro-Learning

A behavioral science-based learning platform employees love. Strengthen your resilience to cyberthreats and fulfill compliance obligations with dynamic and impactful learning experiences across channels to easily build long-lasting, secure habits.

- → Story-driven, gamified learning content designed to engage and stick
- → Curated and guided content library readily scalable for growth
- → Low-effort customization and content management to fit every organization

TRANSFER —

Smart Attack Simulations

User-centric phishing simulations that foster secure habits. Train your employees on how to recognize cyberattacks with our regular automated spear phishing simulations that create lasting security awareness in their everyday work – to effectively reduce risk and crucial threat detection time.

- Personalized and realistic cyberattack simulations
- Context-based learning walkthroughs to reinforce secure employee behavior
- Easy reporting of threats with a one-click Phishing Report Button

ACT —

Strategic Risk Monitoring

Protect your organization from costly incidents by using our comprehensive human risk assessment solution. Receive a complete overview of your human layer security so that you can stay ahead of potential vulnerabilities. Monitor and interpret the impact of your awareness programs, analyze behavior, and make informed data-driven decisions.

- Contextual insights, including technical and behavioral KPIs
- Industry benchmarking and actionable guidelines
- Built for ISO/IEC-27001 requirements, and on a privacy-by-design approach

Acknowledgements

Thank you to everyone who contributed to this report, especially to all our interview partners for taking the time to share their expertise.

Jens Becker
Chief Information Officer & Chief Digital Officer at Zurich Gruppe Deutschland

Stefanie Boem
Data Protection Officer at Sport-Thieme

Sascha Czech
Chief Security Officer at Uniklinikum Münster

Stéphane Duguin
Chief Executive Officer at CyberPeace Institute

Frank Heymann
Senior IT-Team Manager at Buhlmann

Tobias Ludwichowski
Chief Information Security Officer at Signal Iduna

Dr. Stefan Lüders
Computer Security Officer at CERN

Martin Schmidt
Global Director of Digital Advisory at Freudenberg Home and Cleaning Solutions

Thomas Schumacher
Managing Director at Accenture Security

Major General Jürgen Setzer
Chief Information Security Officer Bundeswehr

Dr. Katrin Suder
Strategy Expert for digital technologies, business & politics

Thomas Tschersich
Chief Security Officer at Deutsche Telekom & Chief Executive Officer at Telekom Security

Contact

For further questions regarding this report and research, please reach out to:

Laura Hartmann
Head of Corporate Communications
press@sosafe-awareness.com

Disclaimer:

Every effort has been made to ensure that the contents of this document are correct. However, we do not accept any liability for the content's accuracy, completeness and currency. SoSafe in particular does not assume any liability for any damages or consequences resulting from direct or indirect use.

Copyright:

(ISC)² | CPE SUBMITTER

Earn (ISC)² CPE credits with this report.

SoSafe offers (ISC)² members the opportunity to earn Continuing Professional Education (CPE) credits. (ISC)² cyber security certifications are recognized worldwide as the highest standard of excellence in cyber security.

If you are interested in collecting your CPE points after reading this report, simply scan the QR code to learn how.

sosafe

SoSafe GmbH
Lichtstrasse 25a
50825 Cologne, Germany

info@sosafe.de
www.sosafe-awareness.com
+49 221 65083800