Cybercrime Trends 2024

The latest threats and security best practices

sosafe

Contents

In 2023, everything changed. It's time to prepare for what's to come.

The year 2023 was a turning point in our global narrative. Since OpenAI announced the launch of ChatGPT-3 in November 2022, there has been a surge of AI-driven innovation and a **profound shift in how we interact with technology**. This evolution is particularly evident in information security, where AI has emerged as a pivotal force, not only strengthening cyber security defenses but also elevating the sophistication of cyberattacks.

As we head into 2024, fueled by this **unprecedented speed of technological innovation**, we face a confluence of challenges: AI's ever-growing involvement in cyberattacks, the double-edged sword of emerging technologies like 5G and quantum computing, and the maturing of cybercrime into a highly professionalized industry. This context is further complicated by the rise of hacktivism and cyberattacks amid global political crises and the rise of disinformation campaigns, making threats more complex and far-reaching. All this while cyber security professionals are battling burnout in the face of these escalating threats.

With the likelihood of an **attack resulting from human error expected to increase** in this threat landscape, a strong security culture is the only hope we have. That's why this report focuses on the eight cybercrime trends for 2024 and provides security best practices to better prepare against this diverse array of cyber threats.

1 AI's growing role in cyberattacks: A storm on the horizon

The widespread use of AI, which is expected to reach over 300 million users in 2024 and an estimated 700 million by 2030, not only highlights the revolution underway but also raises concerns about its broader implications and security risks.[1] And, inevitably, **deepfakes** and **voice cloning** come into full focus when addressing AI's security challenges.

While bad actors have used both technologies for some time, the recent proliferation of tools capable of producing high-quality deepfake videos has made this technology more accessible, leading to an increase in its use, particularly in **disinformation campaigns and social manipulation** (more about this in the disinformation-as-a-service trend).[2]

Voice cloning is not lagging behind. A recent study confirmed that one in four people have experienced

1 in 4

people have experienced a **voice cloning attack** or know someone who has

Source: McAfee[3]
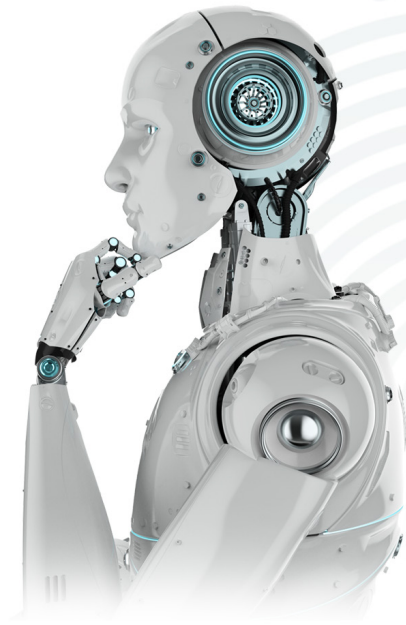
a voice cloning attack or know someone who has.[3] Police in Everett, Washington, have also warned of an increase in financial scams using voice cloning to defraud individuals.[4] But while cybercriminals mostly use these for financial scams, some of them having even faked a young woman's kidnapping, it's now also **undermining MFA systems based on voice recognition**.[5] For example, earlier this year, a journalist successfully accessed her bank account using a recording of her own cloned voice.[6] Although the journalist's experiment posed no personal risk, the broader threat is very real.

---

1   **Statista (2023).** Artificial Intelligence Worldwide.

2   **News abp Live (2023).** Deepfakes To Disinformation: Year 2023 Brought A New Era Of Digital Deception, Driven By AI.

3   **McAfee (2023).** Artificial Imposters—Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam.

4   **Fox 13 Seattle (2023).** Everett Police warn of AI voice-cloning phone scam after case reported in Snohomish County.

5   **CNN (2023).** 'Mom, these bad men have me': She believes scammers cloned her daughter's voice in a fake kidnapping.

6   **The Wall Street Journal (2023).** I Cloned Myself With AI. She Fooled My Bank and My Family.

But this is far from the only use cybercriminals are putting AI to. Advances in generative AI over the past year have brought many new capabilities to key tools. Some of these, such as ChatGPT's recent ability to read images, can be used maliciously. This includes the possibility of **prompt injection**, which means that the tool will follow the instructions or prompts contained in an image instead of the instructions the user gave the tool when submitting the image.[7] While this may seem harmless at first, the possibilities for manipulating users through this tactic are endless.

This image-uploading capability has also raised other concerns, such as the possibility of **bypassing CAPTCHA codes**, one of the most well-known safeguards against the unfair use of technology. Until recently, hackers could not leverage AI technology to read CAPTCHA, mainly due to the ethical restrictions of the tools. However, Bing Chat has proven to be able to decipher these codes when prompted with a reasonable excuse or pretext, raising concerns among companies and websites worldwide about **the need to switch to other security methods**.[8]

And as technology advances, **hackers are also using it to build their own powerful AI tools based on existing language models**. This is how malicious alternatives to ChatGPT, such as FraudGPT and WormGPT, first appeared.[9] However, until the end of 2023, the creation – not the use – of such tools was limited to those with technical knowledge.

Recently, OpenAI introduced the ability to very easily create a GPT – a chatbot that you can train to assist you with a specific task in an even more accessible way than its dark web counterparts – without any coding or technical knowledge needed. While personalized GPTs can be a valuable asset for many, helping them with daily work tasks, we can also expect that **in 2024, attackers will take advantage of their capabilities and create personal hacking assistants**[10] that specialize in creating highly convincing smishing texts, spear phishing emails, and polymorphic malware.[11]

---
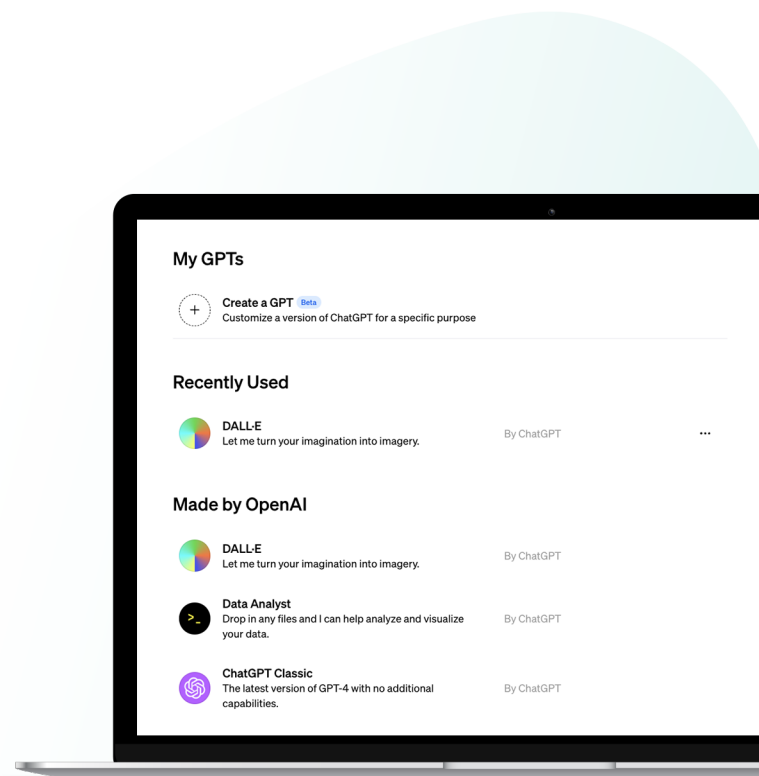
7   **Windows Central (2023).** CGPT-4 Vision: A breakthrough in image deciphering unveils potential for 'prompt injection attacks'.

8   **Digital Trends (2023).** Bing Chat just beat a security check to stop hackers and spammers.

9   **ZDNet (2023).** WormGPT: What to know about ChatGPT's malicious cousin.

10 **BBC (2023).** ChatGPT tool could be abused by scammers and hackers.

11 **HYAS (2023).** Blackmamba: Using AI to generate polymorphic malware.

The risk associated with AI can also stem from its **limitations** rather than its capabilities. The ability of advanced AI models to write code is a significant advancement, widely adopted by up to 92% of developers in and out of the workplace.[12] However, concerns are emerging about **the reliability of AI-generated code**, with experts noting a tendency to prioritize functionality over security, resulting in significantly reduced code reliability.[13] Some of the security flaws include susceptibility to SQL injections, hardcoded credentials, and the use of insecure password hashing algorithms.[14]

But perhaps the most common AI limitation is a phenomenon called **"hallucinations,"** where the AI provides false or fabricated information. **Hackers are now exploiting these hallucinations to infiltrate malicious files**.[15] Upon a user's request, the tool will "hallucinate" and recommend the names of non-existent code libraries. Hackers will then create malicious code libraries or packages under those names and upload them to public repositories. This way, the next time a user is recommended one of these packages, they will download the malicious code library uploaded by the hacker.

Considering the emerging threats from the use of AI and the rapid pace of technological advancement, **it's imperative that we identify and implement robust methods to protect against these threats**. A proactive approach to cyber security is essential to keeping both businesses and individuals safe in an increasingly AI-driven world.

12 **GitHub Blog (2023)**. Survey reveals AI's impact on the developer experience.

13 **The Register (2023)**. Perhaps AI is going to take away coding jobs – of those who trust this tech too much.

14 **Nord Security (2023)**. ChatGPT and secure coding: The good, the bad, and the dangerous.

15 **Infosecurity Magazine (2023)**. New ChatGPT Attack Technique Spreads Malicious Packages.

CHECKLIST

Security
best practices

Check AI-generated code before implementing it: Even if you ask the tool to generate secure code, it is a good idea to test its reliability using automated code review tools or adopting a standardized set of security benchmarks.

Stay on top of the latest AI trends and adjust your security strategy accordingly: Some security measures may no longer be reliable as technology advances, so you need to find alternative solutions to keep your organization well protected. A dedicated task force or intelligence unit within your organization focused on monitoring and analyzing AI-based attacks and their impact on your security posture may be a good place to start.

Leverage AI to strengthen your security: Incorporating AI-powered tools can significantly enhance the analysis of large data sets, leading to better anomaly detection and more efficient real-time threat identification. By integrating AI with SOAR (Security Orchestration, Automation and Response), we can achieve automated, intelligent decision-making and more responsive incident handling. Additionally, using AI in no-code automation allows for quick adaptation of security workflows to keep pace with evolving threats. It's also beneficial to implement AI-based advanced authentication systems, which continuously learn and improve security measures while ensuring they align with your policies and ethical considerations through consistent human oversight.

Use AI tools responsibly: Avoid entering personal details and relying exclusively on the information they provide. Remember that some of their answers may be incorrect or outdated, so it is a good idea to check the integrity of the information.

Be wary of suspicious voice or video messages: Even when they appear authentic, if the content includes unusual requests or suspicious statements, it's advisable to reach out through alternative means to verify their authenticity.

Educate your employees on the security threats that AI can pose: They will be your best line of defense if they know how to protect themselves and your organization from threats. Also, teach them how to use generative AI responsibly, protecting all sensitive data.

2 Beyond AI: All new technologies are being exploited by cybercriminals

Even if it's the innovation of the century, cybercriminals aren't just focusing on artificial intelligence. They're **broadening their horizons** to exploit a range of emerging technologies. The goal is to widen the attack surface and reach as much as possible. That's why each new **technology becomes both a tool and a target** for sophisticated cyber threats.

However, this trend isn't entirely new, as we've seen a similar pattern in the past with other emerging technologies like **cloud technology**. In recent years, companies have shifted billions of dollars to cloud storage and away from traditional data solutions. And, of course, this transition hasn't gone unnoticed by cybercriminals. According to the CrowdStrike Global Threat Report, attacks targeting cloud systems nearly doubled in 2022, and the number of hacking groups capable of launching such attacks has tripled.[1]

The ransomware attack in Sri Lanka in early August 2023 was a stark illustration of this, as malicious actors infiltrated the Sri Lankan government's cloud system by distributing infected links to government employees.[2] The attack wiped out four months of government data because the country's cloud system lacked backup services.

And now, the same fate awaits emerging technologies like **quantum computing**. A critical concept is "harvest now, decrypt later" (HNDL), where cybercriminals accumulate encrypted data today with the expectation that future advances in quantum computing will allow them to decrypt it, potentially leading to unprecedented privacy breaches, intellectual property theft, and exposure of national security secrets.[3]

1   **CrowdStrike (2023).** Global Threat Report.

2   **Infosecurity Magazine (2023).** Ransomware attack wipes out Sri Lankan government data.

3   **Tech Monitor (2023).** Are harvest now, decrypt later cyberattacks actually happening?

Recognizing this issue, the UK's National Cyber Security Centre wrote a white paper as early as 2020 with advice on how to transition to quantum-resistant algorithms and the importance of starting this process early to ensure security against potential quantum computing threats.[4] However, the uncertainty surrounding the timeline for quantum computing breakthroughs creates a complex risk landscape where organizations are balancing the cost of adopting quantum-resistant measures early against the risk of being unprepared for a sudden advance in quantum computing capabilities.

5G technology is another example of how new technologies can be a double-edged sword, promising unprecedented connectivity and speed but also opening up new avenues for cybercriminals to exploit. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) identifies the following risks associated with 5G: increased vulnerabilities due to complex network design and local 5G deployments; supply chain threats from malicious hardware and software; inherited weaknesses from legacy infrastructure and untrusted components; limited market competition leading to reliance on potentially insecure proprietary solutions; and an expanded attack surface introducing new vulnerabilities and increased risk of data breaches.[5]

All these advances underscore a critical point: As these and other **new technologies continue to evolve**, so do the methods and targets of cybercriminals. It's a constant race, with each new technological development providing a new opportunity for exploitation. As a result, cyber security strategies must be agile and adaptive, evolving with these technological advances to mitigate the risks posed by these threats.

---

4   **National Cyber Security Centre (2020).** Preparing for quantum-safe cryptography.

5   **CISA (2023).** 5G Security and Resilience.
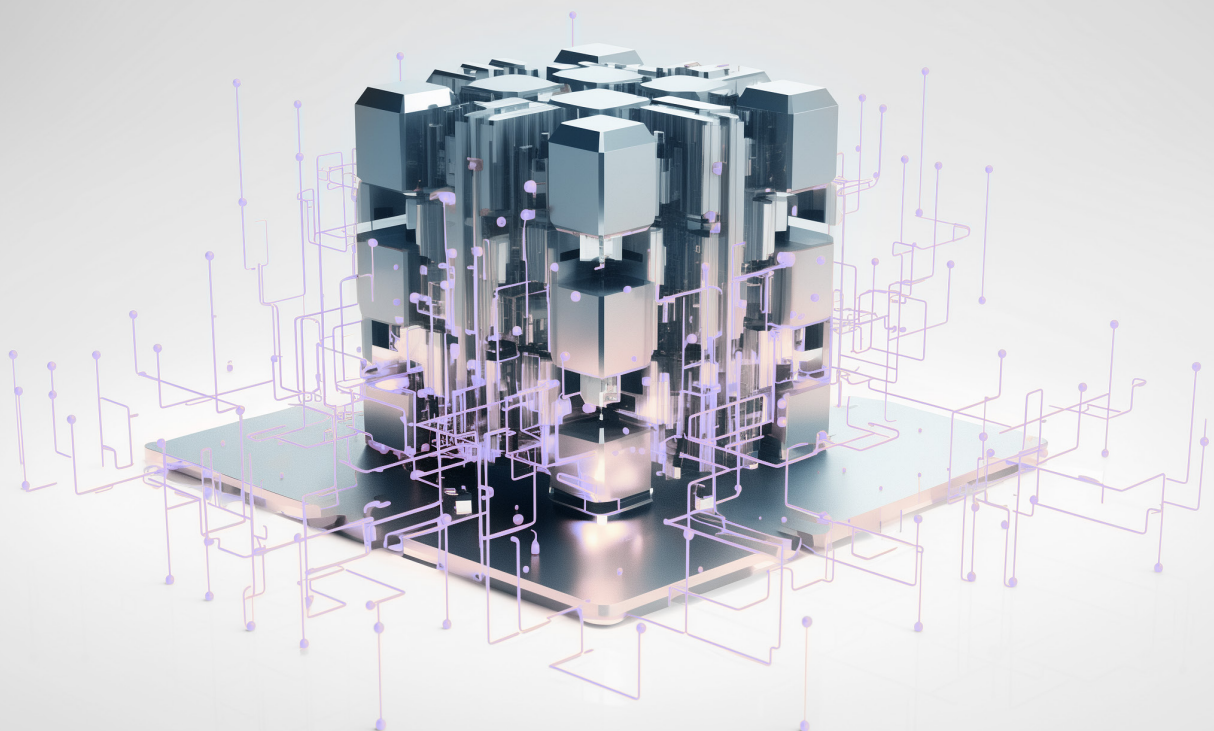
CHECKLIST

Security
best practices

Strengthen cloud security: Invest in comprehensive backup and recovery systems for cloud storage and maintain a routine of regular updates and patches to protect against evolving threats.

Minimize the risk of encrypted data breaches: Use micro-segmentation to protect data, routinely rotate encryption keys based on data classification, and ensure software and security measures are consistently updated.

Adopt a crypto-agile approach: Be prepared to quickly switch algorithms and cryptographic methods as new threats emerge.

Secure 5G networks: Address vulnerabilities in complex network designs and local deployments, and ensure the security of the supply chain, including hardware and software components.

Mitigate legacy infrastructure vulnerabilities: Upgrade or replace legacy systems that may have inherent security flaws, and incorporate security considerations into the design of new technologies.

Monitor and adapt to emerging threats: Stay informed about emerging cyber threats, adapt strategies accordingly, and implement continuous monitoring and real-time threat analysis.

Strengthen your team's cyber security skills: As with the AI trend, providing continuous training and upskilling for both your security team and the rest of your employees will prepare them to rapidly respond and adapt to new threats.

3 Cybercrime will transform into an even more highly professionalized and profitable business

The professionalization of cybercrime continues to make steady progress and will reach a new level of maturity by 2024. This escalation is driven, in part, by the availability and expansion of **ransomware-as-a-service (RaaS)** offerings. Last year, we showed how these sophisticated tools not only lower the barrier of entry for potential cybercriminals but also represent a significant shift in the attack complexity and impact.

Over the last year, this landscape has evolved rapidly, to the extent that in 2023, **the number of ransomware victims doubled** compared to April 2022.[1] This alarming increase underlines that ransomware remains the **most damaging, costly, and prevalent cyber threat to EMEA organizations**.[2]

This development is clearly reflected in the increasing targeting of ransomware attacks. As we will discuss later in the report, there is a clear trend toward **targeted attacks on the public sector and critical infrastructure**, particularly healthcare, education, and government organizations. The reason is they often lack security resources and are more likely to pay a ransom to maintain essential services and protect sensitive information.

A concerning example of this happened in Maine in May 2023, when a ransomware group exploited a vulnerability in MOVEit, a file transfer program used by state authorities. The **attackers stole data from 1.3 million people**, including names, birth dates, insurance numbers, driver's license numbers, and other state and tax identification numbers.[3]

But this sector is not the only one affected. MGM Resorts, one of the world's leading casino hotel chains, was the target of an attack by hackers from ALPHV subgroup Scattered Spider in September 2023.[4] The attackers used social engineering methods by identifying an employee via LinkedIn and then calling the help desk. **A 10-minute conversation was enough to compromise the billion-dollar company**. The cyberattack on MGM Resorts led to major disruptions, paralyzing ATMs, slot machines, and shutting down their website and booking systems. It's expected to lower third-quarter profits by about $100 million, with an additional $10 million spent on recovery, including tech consulting, legal fees, and other external consultant expenses.

1   **Black Kite (2023)**. Ransomware threat landscape report.

2   **Gulf Business (2023)**. Cybersecurity 2023: Threats proliferate but best practice still works.

3   **Mashable (2023)**. An entire state's population just had its data stolen by a ransomware group.

4   **TechCrunch (2023)**. MGM Resorts confirms hackers stole customers' personal data during cyberattack.

"

On average, it takes about 23 days to resume basic operations after a devastating ransomware attack. Restoring the entire system to full functionality can take months.

Inge van der Beijl
Human resilience enabler and threat actor communications expert at Northwave, at the Human Firewall Conference 2023

This growing aggressiveness of cybercriminals is particularly evident in their tendency to intensify ransom tactics. They are **increasingly using double extortion tactics**, in which they encrypt data and threaten to publish it at the same time. Although not new, this method has become more common in the past months.[5] Some hackers are even pursuing **triple extortion**, where they add another layer of attacks like DDoS, and **quadruple extortion**, exerting additional pressure on customers, suppliers, and employees of the attacked company. For example, after hardware vendor Quanta Computer failed to meet the ransom demands of the REvil group, attackers turned their attention to Apple, one of Quanta's customers.[6] The group not only threatened to release Apple's confidential product blueprints taken in the attack but also sought to intensify pressure by timing the disclosure with Apple's product launch, leveraging the public and media attention to maximize the impact.

The professionalization of cybercrime extends beyond RaaS to emerging technologies like voice cloning. **Voice-cloning-as-a-service** (VCaaS) has become a significant threat, as we saw with the AI trend, allowing even low-skilled cybercriminals to engage in sophisticated impersonation schemes.[7] With platforms like ElevenLabs allowing users to create custom voice samples, the barrier to entry in cybercrime continues to drop.

Considering this rise of professional, complex cyberattacks, the importance of supply chain security is clearer than ever. Outsourcing services is increasingly necessary, but it also creates new vulnerabilities as cybercriminals **infiltrate corporate networks through partners or suppliers**. An example of this happened to Airbus in 2023. Hackers compromised one of their customers, Turkish Airlines, leading to a significant loss of data from over 3,000 suppliers.[8] In this context, we are only as strong as our weakest link. Disregarding the security of our suppliers, partners, and customers is no longer an option if we want to stay safe.

The prognosis for the future is clear: **Cybercrime is on the verge of becoming an even more professional and profitable business**. This trend can no longer be ignored or underestimated. Now is the time for organizations to invest in their security as the developments of recent years are just the beginning of an emerging future in which cybercrime will develop ever more sophisticated methods to achieve its goals.

---

5   **TechCrunch (2023)**. Why extortion is the new ransomware threat.

6   **Bloomberg (2021)**. Apple targeted in $50 million ransomware hack of supplier Quanta.

7   **Recorded Future (2023)**. I have no mouth, and I must do crime.

8   **The Register (2023)**. Airbus suffers data leak turbulence to cybercrooks' delight.

CHECKLIST

Security
best practices

Build a resilient infrastructure against ransomware: Develop a comprehensive security posture that includes both preventive measures and robust response plans. This should integrate advanced threat detection systems, such as AI-driven anomaly detection, and adopt a zero-trust architecture to enhance security. Conduct regular security audits and develop effective disaster recovery plans. Also, continually revise backup strategies and ensure you have a tested incident response plan in place to respond effectively and quickly in the event of a breach.

Dealing with zero-day vulnerabilities: Develop strategies to respond quickly to zero-day attacks. This includes setting up patch management to efficiently distribute software updates and close vulnerabilities promptly.

Protection against social engineering and phishing attacks: Train your employees to make them aware of the risks of social engineering attacks, particularly those tactics used by ransomware groups. Ongoing training through micro-modules and phishing simulations can raise awareness and help them recognize potential threats. Incorporating gamified and personalized learning experiences will increase engagement and retention of security knowledge.

Strengthen supply chain security: Review and secure your supply chain. This includes the security protocols of your partners and suppliers and implementing strict access controls and monitoring systems.

Improve data security and integrity: Implement advanced encryption techniques and take a layered approach to data protection by adopting data-centric security frameworks and data loss prevention (DPL) technologies. This helps minimize the risk of data leakage and theft.

Use threat intelligence and analytics: Use threat intelligence to identify and analyze current and emerging threats. This helps to take preventative measures and improve responsiveness in the event of an attack.

INTERVIEW

Ralf Schneider

Allianz Senior Fellow and Head of Cyber Security and NextGenIT Think Tank

Ralf Schneider's impressive career in IT and cyber security spans more than two decades, marked by his long tenure at Allianz, where he served as Group CIO for 13 years. He has also served as a board member for Allianz Managed Operations & Services and recently took on the role of Allianz Senior Fellow and Head of Cybersecurity and NextGenIT Think Tank. He holds a PhD in computer science from the Ludwig Maximilian University in Munich.

> " Criminals need ever fewer skills and organizational power to launch a highly effective attack, and that is going to be a huge problem for us.

What brought you to the field of information security?

I started out in this field when I was appointed Group CIO of Allianz in January 2011. With 3,000 offices and 63 business units around the world, I quickly learned that we needed a communication infrastructure that included video conferences. We had to build our IT such that we could access IT resources with any device worldwide. To do this, you need a network infrastructure, a consolidated data center so that the applications work globally, and a virtualized end workspace – all of which have

to be secure. There was no question that cyber security would become a major topic for us.

When the Snowden disclosures came out in 2013 and Mrs. Merkel's cell phone was hacked, we saw that cyber security was increasingly becoming a hot-button issue. In addition to the infrastructure network, data center, and virtualized workspace, we established the Cyber Security Infrastructure, Global Identity and Access Management, Global Privilege Access Management, and the Allianz Cyber Defense Center on a global scale in 2013.

How do you assess the current threat landscape, and how will it develop in the coming years?

Since the war in Ukraine began, it became clear to us that we're in the midst of a cyber war. In cyber security, we're facing state, military, and highly sophisticated criminal actors. Cybercriminals are constantly honing their skills and becoming more organized. On top of that, they're turning the industrialization of cyberattacks into criminal big business.

Then there's a third component. Cyber security tends to go through cycles. DDoS was a core issue in 2013 before disappearing, and now it's back again. We need to expect the focus to return to activists and hacking kits, including those powered by AI. Criminals need ever fewer skills and organizational power to launch a highly effective attack, and that is going to be a huge problem for us. Instead of focusing on just a few groups, we're looking at hundreds, if not thousands.

The fact that the gap between rich and poor is growing makes the situation even more grave. You don't have to be a professional athlete to earn a lot of money these days. You can also become a hacker. The good thing is that we're always getting better at defending ourselves.

You mentioned the spike in generative AI. Do you think that technology like deep fakes and voice cloning will turn into a mass problem?

Voice cloning and similar methods are very big right now, but I think there's another risk to them as well. It's no longer about finding a security flaw or identifying an individual as a weak point. It's about the response, meaning the disabling and circumvention of detection tools. That's where there will be a big increase in the use of AI.

Besides AI augmented sophisticated attacks, I don't see any major dangers of automatic AI based attacks right now because AI still makes too many mistakes, and it has to be used properly. But we're still in the early stages, and we should be preparing

for the worst-case scenario. Right now, we're benefiting from the fact that this big scaling hasn't happened yet. With each attack – successful or otherwise – we learn and are able to improve our line of defense. But the risk isn't just in the quantity but also in the concurrence that AI allows. Such simultaneous scaling attacks will become the challenge in the future.

How do you feel we can keep pace with the rapid developments in the threat landscape?

In short, proper cyber hygiene and keeping an eye on the latest threats. Cyber hygiene has to be established from the ground up, which is a major challenge. I don't think there's a way around multi-factor authentication. Before you drive off in your car, you have to buckle up. Before you start surfing the web, you have to undergo multi-factor authentication. At Allianz, we implemented multi-factor authentication during the coronavirus pandemic because of the prevalence of remote work.

And the most important way to keep up with the speed at which threats are developing is working well and comprehensively from the very start and then staying on the market. We're currently renewing our Cyber Defense Platform and augment it with AI. Now, the big task is integrating it and using it in the wild, but that's where we're investing. Ultimately, it all comes down to the human factor – finding the right people and giving them the opportunity to learn independently. If you don't have any capabilities or awareness in your company, all the technology in the world will only take you so far.

> "
> Ultimately, it all comes down to the human factor. Finding the right people and giving them the opportunity to learn independently. If you don't have any capabilities or awareness in your company, all the technology in the world will only take you so far.

Another cybercrime trend is digitalization, and everything is becoming more interconnected. What risks do you see here regarding cyber security?

Operating a website without being protected from the fundamental threats by a proxy shield is very risky. Every company needs a good proxy shield, and that comes at a price.

Everything is interconnected and at light speed so to speak. On top of that, it's all operated by software that can perform actions in milliseconds. Monitoring and control aren't possible without automation – but we can't expect AI to do everything for us. We're being attacked by people who use AI, and so we need people who use AI to defend us. These people need to be trained and have the proper understanding and knowledge. In addition, the contact points for the IT systems aren't just machines but are usually people. Each of these contact points has to be monitored and secured against attacks.

The question is, should companies seal up their technical vulnerabilities first and then focus on people or the other way around? Do you have a holistic strategy for including the human factor?

If you run head-first into every battle, you're going to lose. If you know your enemy, you might lose half the time. But if you know both your enemy and yourself, you have a good chance at winning every time. Cyber security is a game of attack and defense. We started in 2013 with two controls that we rolled out on a comprehensive scale. We began with awareness and large-scale coverage against DDoS and securing mobile end devices, followed by all the layers like the Protection, Detection, Response, and Recovery Layer.

Two thousand years of wisdom have taught us in an attack and defense scenario that you have to know the enemy and yourself. So in our days it comes down to knowing the threat landscape and your own IT systems, networks, and vulnerabilities. You can't defend something you aren't aware of.

IT systems are built and operated by people, so you have to know the people and their awareness of secure IT.

> **"**
>
> **We're being attacked by people who use AI, and so we need people who use AI to defend us. These people need to be trained and have the proper understanding and knowledge.**

On the topic of awareness training, how do you view the evolution from a mere compliance requirement to a continuous measure that enables people to become a line of defense?

In our current age of digitalization, IT can no longer be just functional – it also has to be secure and compliant. But not everything that's good for compliance is automatically increasing the security level. Awareness is a good example. You implement an awareness program through web-based training and check off your compliance requirements, and the regulator is satisfied. You still haven't become any more secure if the users are not empowered.

This is when employee enablement comes into play. We learned early on that you have to take an entertaining approach to awareness, and not apply so much pressure. You also have to pick the right time to train them. It's ideal when I've just received a phishing campaign or a real phishing email. The next challenge is keeping people's attention, and SoSafe's Phishing Report Button is an extremely useful tool. If employees are unsure whether they've just received a real phishing email or not, they can use the button to tell them if it's a phishing attack and how to identify it. The learning success here is immense. Plus, there's the fun factor and the motivation that stem from people learning on their own and being able to use the Phishing Report Button as a sort of assistant. Users can directly apply what they have learned, which is an immediate reward.

IT teams are under all sorts of pressure regarding both defense and security awareness training. What do you think could be potential measures for taking some of the onus off of IT teams?

We have to ask where the problems truly lie – conducting crisis drills at every level, up to top-level management and the board. We've been regularly doing that at Allianz for years. Various psychological factors play a role here, starting with the fact that people don't like to show that they are unable to do something. Secondly, the benefits of the time they have invested have to be clear from the start and manifest quickly. After all, awareness training costs money and resources.

One of the core challenges lies in making the urgency of cyber security palpable and tangible for top-level management in all business units. When it comes to business goals, IT has to be functional and secure at the same time. Unless something gravely serious happens, it's hard to tell whether the measures you've implemented have made you more secure than before. Proving the efficacy and removing distrust is very difficult because you can't prove that you're more secure than before – a very convincing way is attack simulations that have to show that you are getting faster, more efficient, and more effective at defending your organization.

Do you think there are KPIs that might be more convincing for top-level management?

At Allianz, we have six cyber security health indicators based on the NIST standard – Govern, Identify, Prevent, Detect, Response, Recover against Cyber Attacks – that we grade with a color system of red, orange, yellow, light green, and green so that we can visibly evaluate the success of our measures. Just like blood pressure, pulse, and cholesterol levels, our eight health indicators have to fall within a certain range.

Two of these indicators have proven particularly effective. One is our zero tolerance against toxic components, where security patches are not available anymore. This led to us tracking down all our outdated, insufficiently protected applications. We also started automating, analyzing all obsolete databases and operating systems, identifying toxic components, and systematically renewing our entire IT system. The zero-tolerance component was implemented for security reasons, but it goes far beyond that. The second effective indicator is our Awareness Score, which we use to measure global phishing campaigns. We log click rates and how many people report a harmful email.

In a past interview, you said that hierarchical structures in companies can impair cyber security. What do you mean by that?

External attacks conducted with tools can only be prevented with experts who have the tools to match. Security experts have to decide what needs to be done. The executive level has to have an eye on everything and provide resources, initiatives and support at the right time. Yet this is done "on site," so autonomy is required as well. Management lays the groundwork, provides the resources for effective cyber defense, and brings security experts together with internal and external partners.

> **Security experts have to decide what needs to be done. The executive level has to have an eye on everything and provide resources, initiatives and support at the right time.**

4 Digital dissent and deception: The dual faces of hacktivism and cybercrime in a fragmented world

The intricate threat landscape extends beyond individuals pursuing financial or personal gain. Escalating political and social tensions are fueling the rise of another significant faction in the digital sphere: **hacktivists**. Motivated by a desire to express dissent or support for causes like armed conflicts or social injustices, these individuals **exploit vulnerabilities and security loopholes to make their statements** – a situation that is intensifying with each passing month.

According to the latest Motorola report, hacktivism increased 27% in the third quarter of 2023.[1] A stark example of this trend is the pro-Russian hacktivist initiative **DDoSia**. They are known for orchestrating attacks against Western entities, which experienced a dramatic surge in participation in 2023, with its membership skyrocketing by 2,400% and amassing 45,000 subscribers on their main Telegram channel.[2]

The ongoing conflict between Russia and Ukraine, now in its second year, is a reminder of how modern conflicts have turned into **hybrid wars fought in both physical and digital arenas**. Within this framework, both hacktivists and state-sponsored entities are leveraging **cyberattacks** as a **key component in their extensive toolkit of modern warfare**. A significant

example of this is the attack by the Ukrainian group Cyber.Anarchy.Squad against Infotel JSC, a critical Russian telecom provider that is integral to the functioning of major Russian banks and financial institutions.[3] This attack had a significant impact, disrupting many Russian banking systems and preventing them from processing online payments for several hours.

The more recent conflict between Israel and Gaza also highlights the escalation and further implications of this threat. Shortly after the conflict started, Anonymous Sudan carried out their first cyberattack, targeting Israel's emergency warning systems and claiming to disable alert applications that notify civilians of incoming rockets.[4]

---

1   **Motorola Solutions (2023).** New Report Outlines Q3 2023 Cyber Threats to Public Safety.

2   **Bleeping Computer (2023).** Pro-Russia DDoSia hacktivist project sees 2,400% membership increase.

3   **Bleeping Computer (2023).** Ukrainian hackers take down service provider for Russian banks.

4   **Security Week (2023).** Hackers Join In on Israel-Hamas War With Disruptive Cyberattacks.

Almost simultaneously, KillNet focused on disrupting several Israeli government websites. As retaliation for these and several other attacks, the Indian-based hacktivist group Indian Cyber Force sided with Israel and brought down the websites of Hamas, Palestine National Bank, Palestine Web Mail Government Services, and Palestine Telecommunications Company.[5]

But hacktivism extends beyond warfare and political tensions to include various **social causes**. For example, Anonymous Sudan launched a cyberattack on Scandinavian Airlines early last year.[6] This was in response to the public burning of the Holy Quran by a far-right nationalist group outside the Turkish embassy in Stockholm. The attack caused significant problems in the airline's online system, exposing passenger data, including contact information, past and future flight details, and partial credit card numbers.

Later in 2023, the VulzSec hacking group claimed to have compromised and leaked sensitive French police data in retaliation for police brutality.[7] This exposed 7,092 branch data records and the profiles of 30 police officers. This incident underscores a broader trend: a significant 28% increase in cyberattacks against law enforcement, with hacktivism as one of the major contributing factors.[8]

However, it's important to remember that hacktivists are not in it for the financial gain. They are committing cybercrime to advance the causes they believe in. On the other side, some cybercriminals take advantage of any social instability for their own ends. For example, mirroring the tactics seen

↗ **28**%

increase in cyberattacks against law enforcement, with **hacktivism** as one of the major contributing factors.

Source: Motorola Solutions[8]

in the Russia-Ukraine conflict, they are now setting up fraudulent charity websites to capitalize on the altruism of individuals who want to help in the Gaza crisis.[9] And this is not all. State-sponsored cybercriminals are adding to the mix, as seen in the 'WildCard' hacking campaign, targeting Israeli institutions with sophisticated malware like 'SysJoker.'[10] All this makes it increasingly difficult for organizations to identify who is targeting them in each attack. It also creates a very complex threat landscape in which different actors, each with their own motives, are operating.

As global tensions continue to escalate with no end in sight, an increase in hacktivist attacks in 2024 appears almost certain. In this context, both hacktivists and cybercriminals are key contributors to the instability of the cyber world. They operate in a sort of adversarial synergy, each exploiting vulnerabilities revealed by the other's actions. This interplay creates a dynamic and perpetually evolving environment of cyber threats, reflecting the complexity and unpredictability of the digital landscape.

5   **CSO (2023).** Israel-Hamas conflict extends to cyberspace.

6   **Bleeping Computer (2023).** Scandinavian Airlines says cyberattack caused passenger data leak.

7   **The Cyber Express (2023).** Cyber Attack on French National Police: VulzSec Hacking Group Claims to Leak Sensitive Data.

8   **Motorola Solutions (2023).** New Report Outlines Q3 2023 Cyber Threats to Public Safety.

9   **InfoSecurity Magazine (2023).** Cyber-Criminals Exploit Gaza Crisis With Fake Charity.

10 **Cyberscoop (2023).** Shadowy hacking group targeting Israel shows outsized capabilities.

CHECKLIST

Security
best practices

Build redundant network infrastructure: Having multiple data paths can help maintain availability even under a DDoS attack. This includes having additional servers, alternative data centers, or cloud services. If one path is compromised or overloaded, the traffic can be rerouted to another, maintaining service continuity.

Regular stress testing: Conduct stress tests on your infrastructure to understand how it behaves under high traffic loads. Using red team exercises to simulate real-world attack scenarios can be very useful in these tests.

Implement rate limiting, scrubbing services, and bandwidth overprovisioning: These strategies allow you to control the amount of traffic a server accepts over a given period, filter out malicious traffic, and maintain a higher bandwidth capacity to handle sudden spikes in traffic.

Regular data backup and off-site storage: Regularly back up critical data and store it off-site or on a cloud platform to reduce the risk of losing it all if the primary site is compromised. It's advisable to adopt the use of immutable backups and to adhere to the 3-2-1 backup rule, which involves maintaining three total copies of data – two local copies on different devices for easy access and recovery and one copy stored off-site for additional security.

Network segmentation: Segment your network to limit the spread of malware. If one segment is compromised, it won't necessarily affect the entire network. Using micro-segmentation is recommended for enhanced granularity and protection of sensitive data within segments.

User privilege restrictions: Implement least privilege access policies, granting users only the permissions necessary for their job roles. This approach, a key component of the Zero Trust network architecture, effectively minimizes the risk of internal threats. Make sure to regularly review and update these permissions.

CHECKLIST

Security
best practices

Web Application Firewall (WAF): Implement a WAF to monitor traffic to and from a web application. This helps prevent unauthorized changes to the website. WAF can be integrated with other security tools and is recommended to create a unified threat management system. Additionally, consider using advanced WAFs that incorporate machine learning since they can provide dynamic adaptation to emerging and evolving cyber threats.

Strong authentication measures: Enforce robust password policies and implement multi-factor authentication (MFA) for an additional layer of security, especially for accessing sensitive systems and the website backend. When possible, use passwordless authentication technologies and biometric verification to further enhance security.

Monitoring and alerting systems: Use monitoring tools to keep an eye on network traffic, system performance, and access logs. Also, use Security Information and Event Management (SIEM) systems and Security Orchestration, Automation, and Response (SOAR) systems for comprehensive monitoring, analysis, and automated responses. Set up alerts for unusual activities or changes, enabling the Security team to respond promptly to potential security incidents.

5 Disinformation-as-a-service: An extremely potent tool in the arsenal of hackers

In the years since the Cambridge Analytica scandal, disinformation campaigns have played a significant role in exacerbating social polarization. This tactic, which involves the **deliberate spread of false information**, is increasingly being used by many different actors to manipulate public opinion, damage reputations, and influence business and political landscapes.[1] However, 2023 marked a turning point in these campaigns, as **the rise of generative AI** raises concerns about a world where manipulative content is so cheap and easy to produce at scale that it becomes **nearly impossible to distinguish between authentic and artificial narratives**.

A key platform to showcase the impact of disinformation campaigns is the US presidential elections. During the 2016 election, misinformation spread widely on social media, fueled by far-right activists, foreign interference, and fake news sites. In 2020, the election was inundated with conspiracy theories and unsubstantiated voter fraud claims, reaching millions and spurring an anti-democratic movement.[2] Looking ahead to the 2024 election, there are escalating concerns about how the latest advances in AI could potentially be used to create **more sophisticated forms of misinformation**, deepfakes, and targeted propaganda campaigns.

In fact, this **potential danger to democracy** was already seen in the Slovakian elections, where an AI-produced deepfake audio was used to spread

disinformation on social media.[3] The audio, which reached thousands of users, featured Monika Tódová, a well-known journalist, and Michal Šimečka, the leader of the Progressive Slovakia party, discussing election fraud. Despite immediate denials of the authenticity of the conversation by those involved, and confirmation of its inauthenticity by several fact-checking organizations, the spread of the video was significant because of its timing. It was released during a 48-hour period of silence before the election, making it difficult for media organizations and politicians to publicly refute it.

---

1   **The New York Times (2021)**. Disinformation for Hire, a Shadow Industry, Is Quietly Booming.

2   **The Guardian (2023)**. Disinformation reimagined: how AI could erode democracy in the 2024 US elections.

3   **Wired (2023)**. Slovakia's Election Deepfakes Show AI Is a Danger to Democracy.

In this context, **disinformation-as-a-service (DaaS)** represents a significant shift in the scale and sophistication of misinformation efforts. This **new model of information warfare** enables individuals and organizations to purchase and disseminate fake news and misinformation campaigns with unprecedented ease. Powered by the rapid advancement of generative AI and a network of professional trolls, bots, and sophisticated online manipulation tools[4], DaaS has democratized the ability to conduct misinformation campaigns in the same way that RaaS has done with ransomware attacks – a revolution that cybercriminals and hacktivists will undoubtedly exploit.

This means that **2024 will experience a surge in both politically and financially motivated disinformation campaigns** that will likely target a wide range of sectors, including healthcare, finance, technology, education, and media. On the one hand, hacktivists and state-sponsored cybercriminals will continue to destabilize governments and political organizations with misinformation to influence public opinion and gain more support for their causes. An example of this happened in 2023 with the spread of a deepfake image showing Atlético de Madrid supporters displaying a Palestinian flag, a misleading narrative that gained significant traction online.[5] Some of these attacks will have even wider economic implications to the extent of even **influencing the stock market**. This already happened in May 2023, when a fake image of an explosion near the Pentagon was widely shared on social media and disseminated by various media outlets, including the Russian state news agency RT, causing a brief market sell-off as fear spread.[6]

On the other hand, financially motivated cybercriminals will seek to destabilize organizations and companies in various ways. At very low cost using DaaS, they **will use disinformation in sophisticated phishing and social engineering attacks**, where they will profit from spreading disturbing news about an organization to exploit individuals' emotions of fear and urgency. But that's not the end of it. Disinformation campaigns by different actors that are widely shared externally can also **damage the reputation of a corporation**. This was evident in the case of Wayfair, where conspiracy theorists linked to QAnon exploited the chaos of the pandemic to tarnish the retailer's reputation.[7] Using platforms like Twitter, Instagram, and Reddit, they spread false claims that Wayfair was involved in child sex trafficking. Despite the company's efforts to refute these allegations, the lies persisted online, demonstrating the significant reputational risks that companies face from such disinformation.

CEOs are also prime targets for deepfakes because maintaining a public profile is part of their job. Since they regularly speak on earnings calls, at shareholder meetings, and in television interviews, it's not hard for cybercriminals to obtain audio and video clips of them. And, we've already seen in the AI trend what they can do with this material.

With the escalation of disinformation campaigns threatening the global information landscape, organizations are becoming increasingly aware of the risks they pose, including significant financial losses and long-term reputational damage. Therefore, as these tactics become more sophisticated and ubiquitous, organizations will need to develop robust countermeasures to protect their integrity and maintain public trust.

4   **Hackernoon (2022).** Disinformation-as-a-Service: Content Marketing's Evil Twin.

5   **Reuters (2023).** Fact Check: Image of Atletico Madrid fans holding giant Palestinian flag is fake.

6   **The Independent (2023).** Fake AI image of Pentagon exploding goes viral on Twitter and causes US markets to plummet.

7   **The Globe and Mail (2023).** Disinformation campaigns, including those using AI deepfakes, are creating risks for corporations.

CHECKLIST

Security
best practices

Evaluate potential threats: It is important for organizations to regularly evaluate their susceptibility to disinformation campaigns. This involves a robust threat modeling approach that not only assesses the likelihood of being targeted but also considers the potential impact such campaigns could have. Additionally, employing tools for sentiment analysis and trend monitoring can help in analyzing public opinion and trends, thereby enabling organizations to anticipate and strategize effectively against potential disinformation threats.

Educate and train employees: Equip employees with knowledge of disinformation campaign tactics and the potential impact on the organization. Teach them how to fact-check information, identify credible sources, and use critical thinking to question the validity of content they encounter. Establishing a culture of skepticism and verification can strengthen the organization against the effects of misleading information.

Enhance internal communication: Strengthen internal communication channels to swiftly address and mitigate the spread of false information. Using communication tools like Sofie Rapid Awareness, SoSafe's integration with MS Teams, enables you to quickly notify your employees whenever you identify a fake disinformation campaign about your company.

Create a crisis communications team: Establish a rapid response team that specializes in crisis communication, capable of countering disinformation quickly with factual information.

Promote vigilance and reporting: Companies need to create an environment where employees are alert and ready to report anything unusual they encounter online, such as misleading news, deepfake images, or altered video or audio content. Also, employees need to feel comfortable reporting these incidents without fear of judgment. For this, implementing an easy-to-use, anonymous reporting system that employees can use to flag instances of disinformation safely and without fear of reprisal is crucial.

Automate the tracking of social media: Keep an eye on social media for traces of DaaS operations, checking for counterfeit news, manipulated images, and fake audio clips. A joint effort with the PR and marketing teams is key to achieving this. There are also AI-driven social media monitoring tools that can detect and flag potential disinformation in real-time, allowing for immediate action.

Collaborate on threat intelligence: Engage with external cyber security networks, including partnerships with industry peers, government entities, and global cybersecurity alliances, for shared insights on disinformation trends and best practices.

6

2024: A year of security challenges for the public sector and critical infrastructure

While hacktivism is a well-known threat to public sector institutions, this is only one aspect of the broader challenges they face. The public sector must also contend with threats from **state-sponsored cybercriminals and independent hackers**, who aim for data destruction, disruption, financial gain, and espionage – all of which have serious consequences. In fact, IBM's Cost of Data Breach 2023 states that **the average cost of a cyberattack in the public sector escalated to an alarming $2.60 million**.[1]

The digitalization of sensitive information in public sector entities, along with the critical services they provide, makes the public sector **an attractive target for cybercriminals seeking sensitive data and service disruption**. In 2022 alone, the number of nation-state **cyberattacks that specifically targeted critical infrastructure increased from 20% to 40%** worldwide.[2] This increase is largely due to state-sponsored attacks coming from Russia's conflict with Ukraine. With the Ukraine conflict still active and other conflicts like the Gaza-Israel war, we expect this trend to continue through 2024, further complicating the threat landscape.

The depth of valuable information these organizations hold is a goldmine for many, and the education

"

Cyber is a geopolitical instrument of power and a new attack vector that states use to pursue their own ends.

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

sector knows this well. Last year, **the cost of a successful data breach in the education sector** was **$3.65 million**.[3] In 2023, we saw how the hacking group Vice Society leaked sensitive information from Pates Grammar School in England, including child passport scans, staff pay scales, and contract details.[4] Several other attacks followed across Europe, with hackers taking down several internal networks and IT infrastructures at French[5] and German[6] universities and even launching a DDoS attack on a Greek high school's online examination platform[7], interrupting the normal functioning of exams.

1   **IBM (2023).** Cost of a Data Breach 2023.

2   **Microsoft (2022).** Digital Defense Report 2022.

3   **IBM (2023).** Cost of a Data Breach 2023.

4   **BBC (2023).** Schools hit by cyber attack and documents leaked.

5   **The Record (2023).** Aix-Marseille, France's largest university, hit by cyberattack.

6   **The Record (2023).** Cyberattack on German university takes 'entire IT infrastructure' offline.

7   **The Record (2023).** Cyberattack disrupts Greek national high school exams.

Public administrations around the world are also under immense pressure from the growing threat of cyberattacks. One notable incident occurred in July 2023, when Kenya's eCitizen portal, a critical digital gateway, was crippled by a cyberattack.[8] This disruption rendered more than 5,000 government services inaccessible online, affecting essential functions like passport applications, visitor visas, driver's licenses, ID cards, and health records. In addition, the attack had a broader impact, disrupting mobile banking and transportation services, which demonstrated how interconnected and vulnerable modern systems are.

This incident underscores a stark reality: In today's complex geopolitical landscape, **governments at all levels** – local, state, and federal – **are vulnerable to cyber threats**. Such attacks can have **far-reaching consequences, compromising not only sensitive data but also public safety.** The potential impact is not limited to service disruptions. It extends to the risk of compromising critical infrastructure, causing economic turmoil and even endangering lives. In addition, the aftermath of these attacks often involves a costly and time-consuming recovery process that strains public resources and trust. This increased vulnerability is particularly evident in the healthcare sector, where data integrity and availability are critical. The ENISA Threat Landscape: Health Sector report reveals that **nearly half of the ransomware attacks on public healthcare organizations result in data breaches or leaks**.[9] One notable example occurred last March at Spain's Hospital Clinic de Barcelona, where a ransomware attack forced the cancellation of 150 non-emergency surgeries and approximately 3,000 patient check-ups in three centers and several external clinics.[10]

8   **BBC (2023).** Kenya cyber-attack: Why is eCitizen down?

9   **ENISA (2023).** ENISA Threat Landscape: Health Sector.

10 **AP News (2023).** Cyberattack hits major hospital in Spanish city of Barcelona.

These **attacks on healthcare organizations have been on the rise across Europe this past year**. In December 2023, the German hospital network Katholische Hospitalvereinigung Ostwestfalen (KHO) was hit by ransomware, causing disruptions at three hospitals.[11] Earlier in the year, a hospital in Brussels was hit by a cyberattack that forced it to divert ambulances to other hospitals.[12] In this case, the hospital's IT operations were fully functional one day after the attack, thanks to the emergency plan the hospital had put in place before the attack. This shows **the importance of prevention and rapid response to these scenarios**.

Unfortunately, **recovering quickly from cyberattacks** is not common but **a challenge** for public sector entities, largely **due to insufficient budgets, outdated technology, and understaffed teams**. Public organizations often do not have the resources to implement sufficient preventative security measures. For example, according to the ENISA report's findings, only 27% of healthcare organizations have a dedicated ransomware defense program, and 40% do not have a security awareness program for non-IT staff.[13] To address this, **it is essential to implement preventative measures** – such as security audits and a Zero Trust Architecture – **and build a security culture through personalized awareness training** that meets the needs of each organization. This is critical not only for their protection but for the security of everyone because these organizations serve and belong to the public.

---

11   **Security Affairs (2023).** Lockbit ransomware attack interrupted medical emergencies gang at a German hospital network.

12   **The Record (2023).** Hospital in Brussels latest victim in spate of European healthcare cyberattacks.

13   **ENISA (2023).** ENISA Threat Landscape: Health Sector.

CHECKLIST

Security
best practices

Analyze and quantify risks: Make risk analysis and risk management a core part of business operations. This should be a regular practice, especially when implementing new technologies or planning business operations. Cyber risk assessments are crucial for establishing a baseline for risks, ensuring compliance, and maintaining data integrity.

Establish leadership in digital transformation: Public sector leaders should consider appointing a department head who understands the importance of digital transformation, such as a Chief Information Security Officer (CISO). This role is pivotal in steering digital security strategies.

Implement a Zero Trust Architecture (ZTA): This approach means not granting implicit trust and rigorously verifying each request as if it were coming from an open network. Adopting a Zero Trust Architecture is especially important in light of the rising number of complex cyberattacks on the public sector.

Learn from incidents and plan ahead: Use the knowledge gained from past incidents to improve the overall security management process. Also, develop and regularly update an incident response plan. This plan should outline the steps to be taken in the event of a cyberattack, ensuring a quick and effective response to minimize damage.

Conduct regular security audits: Conduct frequent and comprehensive security audits to identify and address vulnerabilities within the system. This proactive approach helps uncover potential weaknesses before cybercriminals can exploit them.

Implement personalized training programs: Provide regular training tailored to the organization's specific needs and the roles of its workforce members. For example, provide specific training modules for the healthcare sector that address the social engineering techniques most applied to this sector. Phishing simulations should also be personalized to each sector.

INTERVIEW

John Noble

Non-executive director and chair of the Cyber Security Committee of NHS in England

John Noble was the Director of Incident Management at the National Cyber Security Centre (NCSC) in the UK from 2016 to 2018, where he led responses to nearly 800 significant cyber incidents, contributing to the objective of making the UK the safest place for online business. He is currently a non-executive director at NHS Digital (National Health Service), where he chairs the Information Assurance and Cyber Security Committee.

> By sharing information between governments and fostering collaboration between the private sector and the government, we can better understand emerging threats.

What is the National Cyber Security Center (NCSC) and what is its main goal?

The decision to create the NCSC stemmed from a political judgment by then-Prime Minister Gordon Brown. Recognizing the nation's move towards a digital society built on the inherently insecure internet, the government saw the need for an agency to provide advice and assistance.

Why did you decide to make NCSC part of the GCHQ intelligence agency?

The decision to make NCSC part of the Government Communications Headquarters (GCHQ) intelligence agency was strategic. GCHQ's expertise in network defense and established cyber security agency made it the ideal host for the NCSC.

What is the role of the NCSC?

When we started, we had to figure out how the government could best help and how the NCSC could help make the UK the safest place to do business online. We realized that we had to do it by sharing government experience and building a partnership between the government and the private sector.

Why is it important to have collaboration between the public and private sectors in cyber security efforts?

Both the government and the private sector hold unique strengths in cyber security, so NCSC analyzes how the government can provide means for collaboration between the two. This led to the creation of two initiatives: the Cyber Information Sharing Partnership (CISP), which allows companies to exchange cyber threat information anonymously in real-time, and the Cyber 100, an initiative through which experts from the private sector are brought in to share their knowledge with NCSC.

There's skepticism by organizations to share their vulnerabilities with public entities because they fear that this information will be used against them. How can we convey the message of the government wanting to support and not damage organizations?

Here, the concept of trust and openness is crucial. If an intelligence agency finds a vulnerability in a piece of software and does not disclose it, cyber-criminals can take advantage of it. Agencies like NCSC need to build trust with companies to be able to share evidence of these vulnerabilities. This can result in some very profitable and important relationships with companies.

I also think there has been a mind shift in government towards putting the protection of our digital economy – and digital companies – as the top priority. People need to understand that protecting our digital economy must mean sharing information with governments.

> "
>
> There has been a mind shift in government towards putting the protection of our digital economy – and digital companies as the top priority.

What are some key themes you've observed in the threat landscape over the past decades?

The threat landscape, particularly cybercrime, has significantly changed over the past decades. One prominent aspect is the explosive growth of ransomware, turning it into a sophisticated and specialized ecosystem. Cybercriminal groups like Conti now exhibit business-like structures and hierarchies with distinct departments and job titles. Authorities may stop some of these organizations, but they learn the lesson, reform, and adapt.

There has been an increasing trend where cybercriminals infiltrate systems and do nothing. How can we explain this?

When a vulnerability is exposed, bad actors infiltrate and put down an implant across many different companies. They do this just so they can return later. This is the case with critical infrastructure, where it is important to patch vulnerabilities quickly.

Addressing vulnerabilities can be especially challenging in the public sector because organizations run 24-hour operations. Can you share insights into the NHS's approach to addressing this issue?

The NHS has learned significant lessons from incidents like WannaCry, which exploited a known vulnerability many hospital trusts had not addressed. This incident impacted hospitals not only financially but also affected patient care.

In response to vulnerabilities in healthcare systems, two key strategies have been implemented. The first one is to clearly identify critical vulnerabilities that are actively being exploited and require urgent patching. The second one is to set clear mandatory standards that organizations need to commit to.

What impact has the centralization of healthcare systems, as seen in the UK's NHS, had on addressing cyber security challenges and vulnerabilities?

The centralization of healthcare systems has both positive and negative implications for addressing cyber security challenges. On the positive side, a more centralized system provides clearer standards and expectations, making communicating and enforcing cyber security measures across the entire network easier. This centralized approach also improved patient care and quicker responses to vulnerabilities. However, it also introduces challenges. A centralized system means that a compromise in one part of the system may affect others, which means a failure in one system can have a bigger impact across the system.

What role does geopolitics play in shaping cyber security threats, and how does it impact the interaction between nation-states and private entities?

When we analyze a threat, we need to look at two things: the intent of an actor and their capability. Events like the invasion of Ukraine have led to an intent of nation-states to use attacks to succeed in their war efforts. Regarding capability, we are seeing nation-states developing capabilities that end up being used against us.

What about hacktivism?

The Russian conflict has caused a rise in hacktivism on both sides. We have seen a cyber army of Ukraine carry out attack on Russian companies, on media companies, etc. But we have also seen groups like KillNet, who are very much aligned with the Russian

cause, carrying out DDoS attacks and being very explicit that they want to attack the countries that are supporting Ukraine.

"

The Russian conflict has caused a rise in hacktivism on both sides.

Is there a gray area of interaction between the commercial side of cybercrime and politically motivated cybercrime?

Normally, a state decides not to use cyber because of the consequences that it may have, such as the embarrassment it would cause. However, in a context like the war in Ukraine, states do not really care what others think or the consequences that their actions may have.

We have moved from a situation where we had in place some very effective actions against hacking groups to a position where there is now a collaboration between these groups and the state. There is even now a discussion by leading Russian politicians about legitimizing attacks. It would be terrible to get to a situation where a country legitimizes crime against others. I really hope that we don't go as far as that.

What other strategies do nation-states use in this collaboration?

Deniability is important for countries because it lets them hide their actions. We are seeing these nation-states using many of the tools used by crime groups to allow them to deny their responsibility in these attacks. For example, if a commercially available implant is discovered in a part of a critical national infrastructure, it is very hard to know if a nation-state is behind that or not. Thus, it is very easy for the state to deny it. The availability of these tools allows the nation to use this criminal talent pool.

You mentioned other nations when we talked about Russia. What are other key players in the cyber threat landscape?

When we look at some of the really important strategic issues, we need to talk about China's growing influence, the tensions in the South China Sea, and its attitude towards Taiwan and its other neighbors like the Philippines. China's cyber capabilities have witnessed significant growth, marked by increased sophistication and the utilization of new zero-day attacks. They have reformed their intelligence organizations to avoid conflict, and they have become much more professional. The Chinese have also widened their areas of interest. They always take a long-term view where they build up capabilities over time.

Europe and the UK, on the other side, have a consistent view on cyber, and we have recognized that we need to be more strategic rather than being reactive to the latest events.

What steps can be taken to mitigate cyber threats, particularly those posed by advanced persistent threats (APT)?

By sharing information at an international level between governments and fostering collaboration between the private sector and the government, we can create a more comprehensive understanding of emerging threats. By sharing indicators of compromise (IOCs) and building a trust relationship between both sectors, we can overcome commercial sensitivities. We can establish a united front to detect and respond to emerging threats efficiently.

Did you enjoy the interview?

Human Firewall Podcast

sosafe

Dr. Niklas Hellemann

John Noble

You can listen to the full version in our Human Firewall podcast.

Listen to CEO Dr. Niklas Hellemann's conversation with John Noble and their additional insights on the importance of international cooperation in the field of cyber security.

Listen here →

7 Cyberattacks are becoming more realistic and dangerous due to pretexting and multichannel tactics

Sophisticated social engineering methods like **pretexting** – where hackers impersonate someone the victim trusts and use a fake story to make them fall for the scam – are increasingly being used by cybercriminals to exploit and manipulate victims for financial gain or sensitive data theft. In fact, according to a 2023 report by Verizon, **pretexting attacks account for more than 50% of all social engineering incidents**, showing how attackers continue to rely heavily on deception and manipulation, always capitalizing on human emotions.[1]

In the most sophisticated form of pretexting, **cybercriminals research the victim through multiple channels**, such as social media, blogs, or websites, to gain insight into very specific data about the victim that they can later use in their fabricated story to make it more believable and increase their success rate.[2] This can include information about their workplace, social life, pets, partners, or other personal details that help them create highly convincing and tailored stories that the victim will trust.

However, the channels through which cybercriminals find this data are not only sources of information but also attack vectors. According to our Human Risk Review 2023, email phishing continues to dominate, with a significant 61% of organizations targeted. However, the cyber threat landscape is expanding, with 34% of attacks now using social media.[3] For example, with so many small businesses relying on social media as their primary source of customers, hackers are seizing the opportunity to take over their accounts and bring businesses to their knees. This is what happened to a small business that sold granola through Instagram.[4] Attackers contacted the owner through Instagram, impersonating another business the victim trusted, and asked her to click on a link to vote for the business in a contest. The bad actors then took over her Instagram account and demanded $10,000, which she paid in order to regain control of her business. But this is just one use. Cybercriminals can use social media to target organizations in many ways, including taking over employee accounts to talk to colleagues and solicit sensitive information or making them download malicious attachments disguised as legitimate business documents.

1   **Verizon (2023).** Data Breach Investigation Report.

2   **The Wall Street Journal (2021).** What Hackers Can Learn About You From Your Social-Media Profile.

3   **SoSafe (2023).** Human Risk Review.

4   **CNBC (2023).** Phishing scams targeting small business on social media including Meta are a 'gold mine' for criminals.

Messaging apps like WhatsApp and Microsoft Teams are also some of hackers' favorite channels, both in our private and professional lives. Recently, the Kolkata Police in India warned of a series of WhatsApp attacks where hackers used the pretext of the World Yoga Day to send out messages offering yoga classes and asking people to click on a link and then share a six-digit OTP code, which inadvertently gave the attackers access to the victim's WhatsApp account.[5] After taking over their account, they sent messages to their contacts, creating a sense of urgency and asking for money. In another attack using the professional app Microsoft Teams, attackers sent messages to their victims pretending to be part of the HR team and saying that their vacation schedule had changed.[6] The attacker urged the victim to download a file containing the vacation schedule, which instead loaded a malware called DarkGate.

But cybercriminals haven't stopped there. They are constantly evolving their tactics to make their attacks more convincing. And they are now also orchestrating **highly sophisticated attacks where they contact their victim through multiple channels**, such as SMS, email, or phone calls. For example, in one case where attackers combined SMS and voice phishing, a woman was scammed by attackers who sent her an SMS asking if she had authorized a $7,500 transfer.[7] Shortly thereafter, the attacker took advantage of her fear and called her, posing as a fraud investigator, asking her to change her credentials to prevent a scammer from stealing her money. The attacker ended up stealing $15,000 from both of her bank accounts.

These multichannel attacks become even more convincing and effective when they use AI technology. A stark example of this happened to an employee of Retool.[8] First, the attackers sent a text message to the victim pretending to be the IT team solving a payroll issue. The employee then introduced their credentials on a fake landing page. Since the employee had enabled MFA, the cybercriminals had to call the victim using an AI-generated cloned voice from an IT team member and ask for the OTP token to bypass it. From there, the attackers were able to take over the accounts of 27 customers and steal thousands of dollars worth of cryptocurrency.

With cybercriminals stepping up their game with highly sophisticated and professional tactics, **we must be extra cautious and make sure that secure behavior is ingrained in our DNA**.

5   **The Times of India (2023)**. Police warns netizens about WhatsApp hacking, here's how fraudsters hack accounts.

6   **Decipher (2023)**. Threat actors deliver DarkGate malware via Skype, Teams Chats.

7   **The Guardian (2023)**. Gone in seconds: rising text message scams are draining US bank accounts.

8   **The Hackers News (2023)**. Retool Falls Victim to SMS-Based Phishing Attack Affecting 27 Cloud Clients.

CHECKLIST

Security
best practices

Conduct sender and caller verification training: It's important to train your employees to independently verify the identity of senders and callers. Even if an incoming call appears legitimate, it's safer to contact the person directly through a separate trusted channel if it involves sensitive requests or seems suspicious.

Check external parties: Extend vigilance to include any external parties interacting with your systems. When they require access to sensitive information, confirm they comply with your organization's cyber security standards.

Encourage swift and guilt-free reporting: Foster a culture where employees promptly report any phishing attempts or unusual activities without fearing repercussions. Quick and guilt-free reporting enables security teams to act fast, potentially preventing an attack from worsening.

Update cyber security policies: Continuously revise your cyber security policies to include emerging social engineering tactics like pretexting. Keeping your policies current ensures your defenses stay strong and effective.

Enhance incident response plans: Regularly update your incident response (IR) strategies to lessen the impact of successful pretexting attacks or other methods. Establish clear procedures for detecting, managing, and mitigating attacks to safeguard business continuity and security. Also, make sure that you continuously enhance the IR plans and periodically do tabletop exercises to train the IR muscles.

Train your employees continuously: Provide ongoing training on the latest cyber security threats, including pretexting, and multichannel attacks. Consolidate their learnings through simulations that train them in real-life situations. Educating employees about recognizing and handling suspicious activities is key to creating a vigilant workforce capable of identifying and preventing fraudulent schemes.

# 8 Rising burnout rates challenge cyber security teams like never before

We addressed the issue of security team burnout last year, but the recent global tensions and continued professionalization of cybercrime, now fueled by AI-powered tools, are not only making attacks more complex and difficult to detect but also putting unprecedented pressure on security professionals. In this relentless wave of challenges, our teams' resilience and adaptability are being tested like never before.

A key factor exacerbating this pressure is the shortage of skilled labor in the industry. According to ISC2's latest report, there are 3.9 million unfilled cyber security positions worldwide, up another 12.6% in 2023 compared to 2022, with the largest increases in Asia-Pacific (particularly Japan and India) and North America.[1] Europe isn't lagging behind either, with its cyber security workforce gap up 9.7% from last year. But that's not all. According to a study by ISACA, 59% of organizations have a shortage of cyber security staff, dramatically increasing the workload for existing teams and often **driving security officers to the brink of burnout or even resignation**.[2]

A survey of over a thousand security team members in the US and Europe confirms this: **66% of respondents suffer from significant work stress**, 51% have been prescribed medication for mental health, and 19% consume more than three alcoholic drinks a day as a coping mechanism.[3] But this condition goes far beyond a personal burden. It can also cause **teams to overlook important details, affecting their ability to respond effectively to**

threats and significantly increasing the risk of security breaches in their organizations. This risk is compounded by the fact that cybercriminals are constantly evolving their techniques and becoming more sophisticated in their attacks, as we have already seen in the past sections.

Have you ever been prescribed medication by a doctor for mental health?

49.2%   50.8%

no   yes   Source: Tines[3]
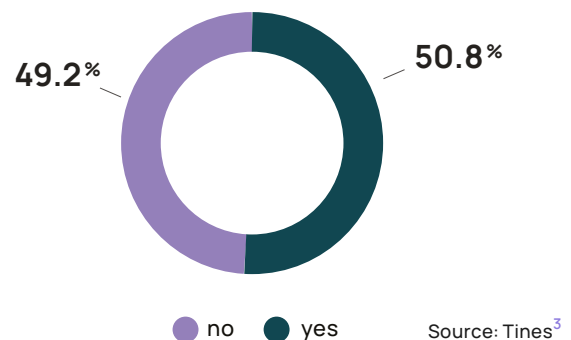
The case of AccessPress illustrates the enormous challenges faced by security teams.[4] As a WordPress plugin provider, AccessPress was the target of a sophisticated cyberattack. Hackers compromised 40 themes and 53 plugins used on over 360,000 active websites, showing the potential reach of software supply chain attacks. This far-reaching compromise, which gave the attackers access to a large number of websites, illustrates the severity and complexity of threats in today's cyber security landscape and reveals not only the technical challenges but also the human aspects of cyber security, particularly the strain on security teams.

---

1   **ISC2 (2023).** How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce.

2   **ISACA (2023).** New ISACA Research: 59 Percent of Cybersecurity Teams are Understaffed.

3   **Tines (2022).** State of Mental Health in Cybersecurity.

"

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 of the CyberPeace Institute

In addition to protecting other departments within the organization and responding quickly to attacks, security teams themselves are among the departments most at risk of falling victim to cyberattacks, according to our Human Risk Review 2023.[5] One of the reasons is that cybercriminals, recognizing that stress can make security personnel more vulnerable, are strategically using team burnout as a pathway for their attacks. By scrutinizing organizations, they identify those whose teams show signs of being overworked or stressed, making them prime targets.

In this dynamic and challenging environment, **it is essential that organizations invest in their security teams** to promote the well-being of their employees. It is important to allocate appropriate budgets and develop retention career plans to alleviate burnout, retain talent, and have enough resources to put in place the right security measures. Only when these steps are taken will teams work effectively to counter cyberattacks and increase security.

4   **The Hacker News (2022).** Hackers Planted Secret Backdoor in Dozens of WordPress Plugins and Themes.

5   **SoSafe (2023).** Human Risk Review.

CHECKLIST

Security
best practices

Prioritize mental health and work-life balance: Develop programs to support the mental health and well-being of security team members. This could include flexible working hours, access to counseling services, and regular breaks to prevent burnout.

Implement effective threat detection tools: Use advanced tools, such as AI-driven threat detection systems, phishing alert buttons, and other tools like SoSafe's email assistant PhishFeedback, to reduce the time and effort required to identify threats.

Automate email analysis: Implement automation tools specifically for Security Operations Center (SOC) teams to analyze reported emails. This can significantly streamline the process of evaluating potential threats from emails, allowing SOC team members to focus on more critical and complex security issues.

Automate routine tasks: Use automation for recurring and routine tasks to allow security professionals to focus on more complex and strategic aspects of cyber security.

Encourage training and upskilling: Provide ongoing training and upskilling programs to improve teams' abilities to deal with the latest cyber threats and technologies. Additionally, facilitate cross-collaborations and establish security champions within other tech teams.

Invest in employee retention: Develop career plans and development programs to retain talent and reduce turnover.

Regular feedback sessions and appraisal interviews: Conduct regular one-to-one meetings to give and receive feedback in order to understand and respond to employees' needs.

Throughout 2024, expect more breaches that involve the human element

All of this year's trends have made one thing clear: **Our cyber security measures will remain incomplete until we focus on people** – just as hackers do. They know that their greatest chance of success lies in playing on human emotions, and that's why social engineering is at the core of their practices, as we've seen repeatedly in this report.

Verizon's Data Breach Investigations Report estimated that up to 74% of breaches involved a human element in 2023, and even tech-focused industry groups now acknowledge the role of humans in exploiting technology.[1] This is just the beginning of what's to come. **In 2024, the percentage of breaches involving a human element will increase even further**, according to Forrester's Predictions 2024 report.[2] With the professionalization of cybercrime and the rise of AI, cybercriminals can now create truly convincing and complex social engineering attacks.This makes it harder to tell the difference between genuine and malicious messages. And with more digital ways to communicate, these threats are spreading faster than ever.

The Allianz Risk Barometer 2024 also estimates that cyber incidents will be the top global business risk in 2024, leaving security leaders no room to ignore the human element in their security strategies.[3] The good news is that there's a powerful countermeasure to this risk: **cyber security awareness and training**. By bringing cyber security to where people are and making secure behavior second nature, we can turn the tide against cyber threats. Remember, it's not just systems but people who are the targets and bear the brunt of cyberattacks. It's also **people who have the power to stop these attacks**. Building a culture of security isn't just a corporate responsibility – it's a personal one, too. Together, we can beat back the looming shadow of sophisticated cybercrime and safeguard our future.

1   **Verizon (2023).** Data Breach Investigations Report.

2   **Forrester (2024).** Predictions 2024: Exploration Generates Progress.

3   **Allianz (2024).** Allianz Risk Barometer 2024.

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 — ## E-learning platform and content

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 — ## Phishing 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 — ## Reporting and analysis

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

CONNECT — ## MS Teams integration

Cyber criminals are moving faster than ever, but so can you. Rapid Awareness enables you to rapidly connect with your employees in MS Teams. Enable rapid micro-learning to address emerging threats, empower your team with instant alerts, and transform them into your strongest defense.

→ Connect directly with your staff in MS Teams

→ Save time and communicate with ease

→ Send bite-sized security alerts that employees can easily digest

→ Track and monitor the number of employees who read the alert
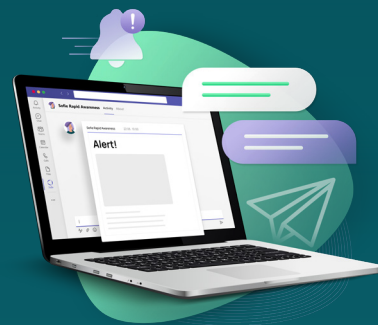
Human Firewall Conference

HuFiCon is a European cyber security event designed to help security professionals transform their teams into cyber heroes. Join us for expert talks, hands-on workshops, and a community committed to putting people at the heart of cyber security.

Will you step up to guide the future of cyber security?

Register now for HuFiCon24

Where? Halle Tor 2, Cologne
When? November 14-15, 2024

Contact

For further questions regarding this report,
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: