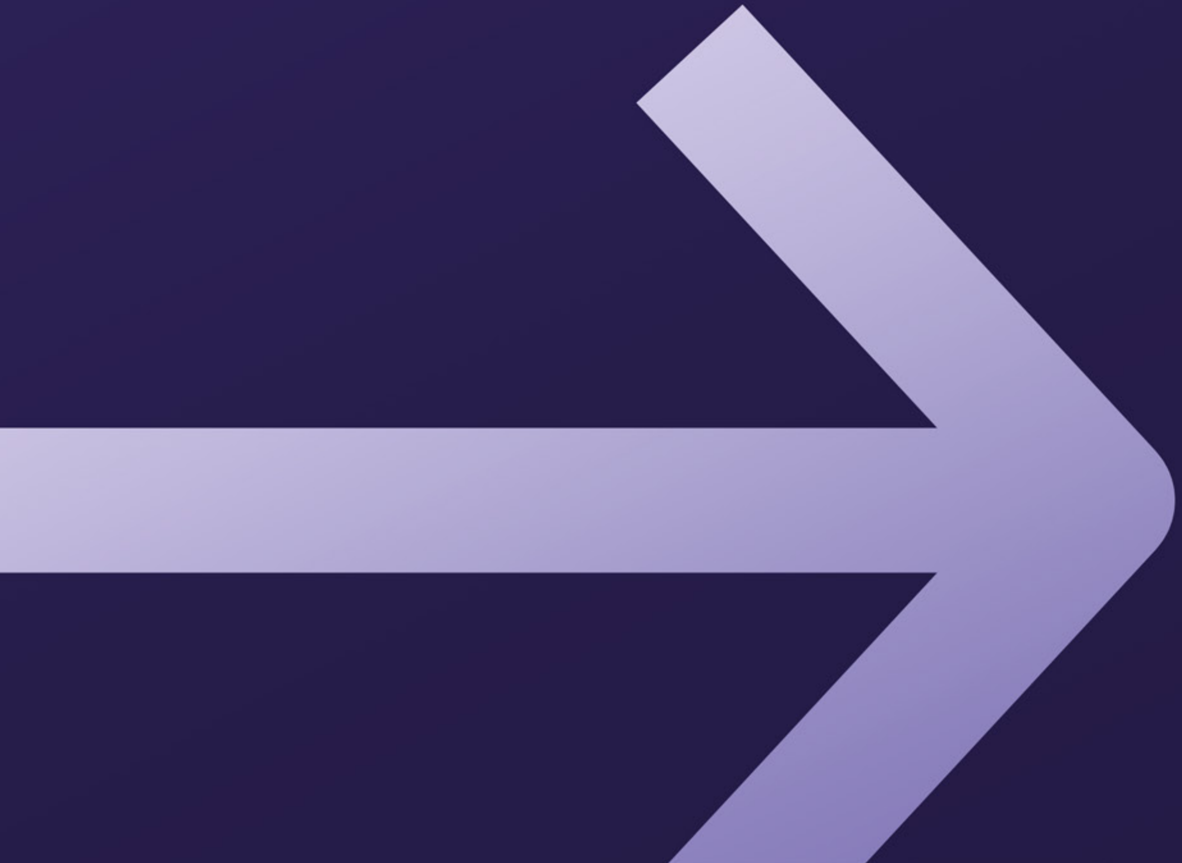
sosafe

Human Risk Review 2022

An analysis of the European cyberthreat landscape

The professionalization of cybercrime has reached a dangerous high.



Editorial

Innovative and highly professional – The new generation of cybercrime

From global crises and geopolitical challenges to the COVID-19 pandemic, the past year has given us no time to rest. Unfortunately, we also witnessed dramatic developments in the field of information security: Cybercriminals did not hesitate to take advantage of dynamic societal events for their own unscrupulous ends.

Coupled with this is an increasing professionalization of cybercrime. Organizations are now facing an innovative dark economy in which cybercrime-as-a-service is a common business model. Tactics are evolving almost by the minute. The IT landscape is also broadening, as hybrid work methods have come to entail new means of communication that offer cybercriminals further opportunities to launch insidious attacks on company systems.

The interface between person and machine is still the primary gateway for cybercriminals, with more than 85 percent of all attacks originating in the human factor. This is no surprise, because even when the person behind the screen is using a wide range of tools, they are still vulnerable to one common type of attack: emotional manipulation. Supply chain and ransomware attacks – many striking instances of which we have seen in the past year, including in the case of Kaseya and Kronos – often begin with phishing.

Yet, such incidents also illustrate that employees are an active part of the solution to the trillion-dollar problem that is cybercrime. If they know how to handle and avert the risks, they can proactively defend their organization against costly incidents. This is why organizations should use sound awareness measures so that they do not fall victim to cybercriminals. Our Behavioral Security Model (page 50) shows how a strong security culture can be established for the long term.

As drastic as the situation is in many regards, there is a silver lining: Awareness of cybersecurity is finally increasing. The rise in cybercrime has led to a reinforcement of security budgets, and organizations are better able to protect themselves. Now is the time to counteract professional cybercriminals, and to ensure the security of data and systems through the minimization of human security risks!

Dr. Niklas Hellemann
Managing Director SoSafe

Contents

Executive Summary

9 out of 10 IT and cybersecurity specialists say:

The cyberthreat landscape has worsened. Every third organization experienced a successful cyber-attack in 2021.

The most successful phishing subject lines in 2021...

...were based on hybrid work processes and emotional manipulation by means of pressure and authority.

66%	You must complete the following task: distribution of documents and assessment of tasks
66%	You have 2 mentions
57%	Important: CORONAVIRUS update

The top 5 cybercrime trends in 2022

01 3 out of 4 survey respondents say that hybrid work models have expanded the range of attacks and success rate of cybercriminals. More than 80% believe that this can be resolved through a combination of technical and organizational measures.

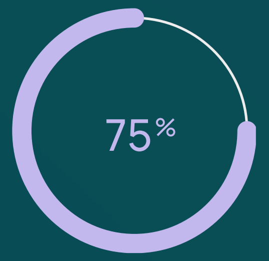
02 ENISA speaks of a “golden era of ransomware”. Complex tactics like multiple extortion increase the risk of data misuse by about 800%. The AV-Test 2021 revealed that the amount of malware has reached a new high, as over 150 million harmful program variants were recognized (59% of which are Trojans).

03 Large-scale supply chain attacks target vulnerable links in supply chains and bring entire supply systems to a standstill.

04 The expansion of AI-as-a-service makes it possible for cybercriminals to utilize new, insidious attack tactics such as deepfakes, voice cloning, and automated, large-scale spear phishing.

05 Phishing and social engineering remain preferred attack methods and are adapted in line with current events. Global issues that affect us all are taken advantage of to create new phishing emails. Every third user clicks on harmful content in phishing emails.

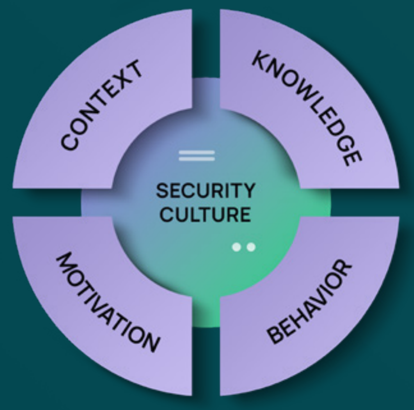
Stricter cybersecurity regulations across Europe increase the liability risks for managers.



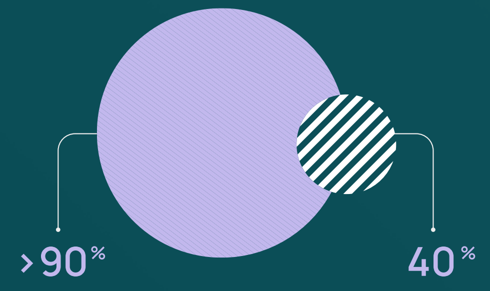
Gartner predicts that 75% of CEOs will be personally liable for cyber-physical incidents as early as 2024.

> “We require decisive and guiding figures at the management level.”
>
> **Achim Berg,** President of Bitkom

The Behavioral Security Model: Psychologically sound awareness measures minimize human risks by up to 90 percent.



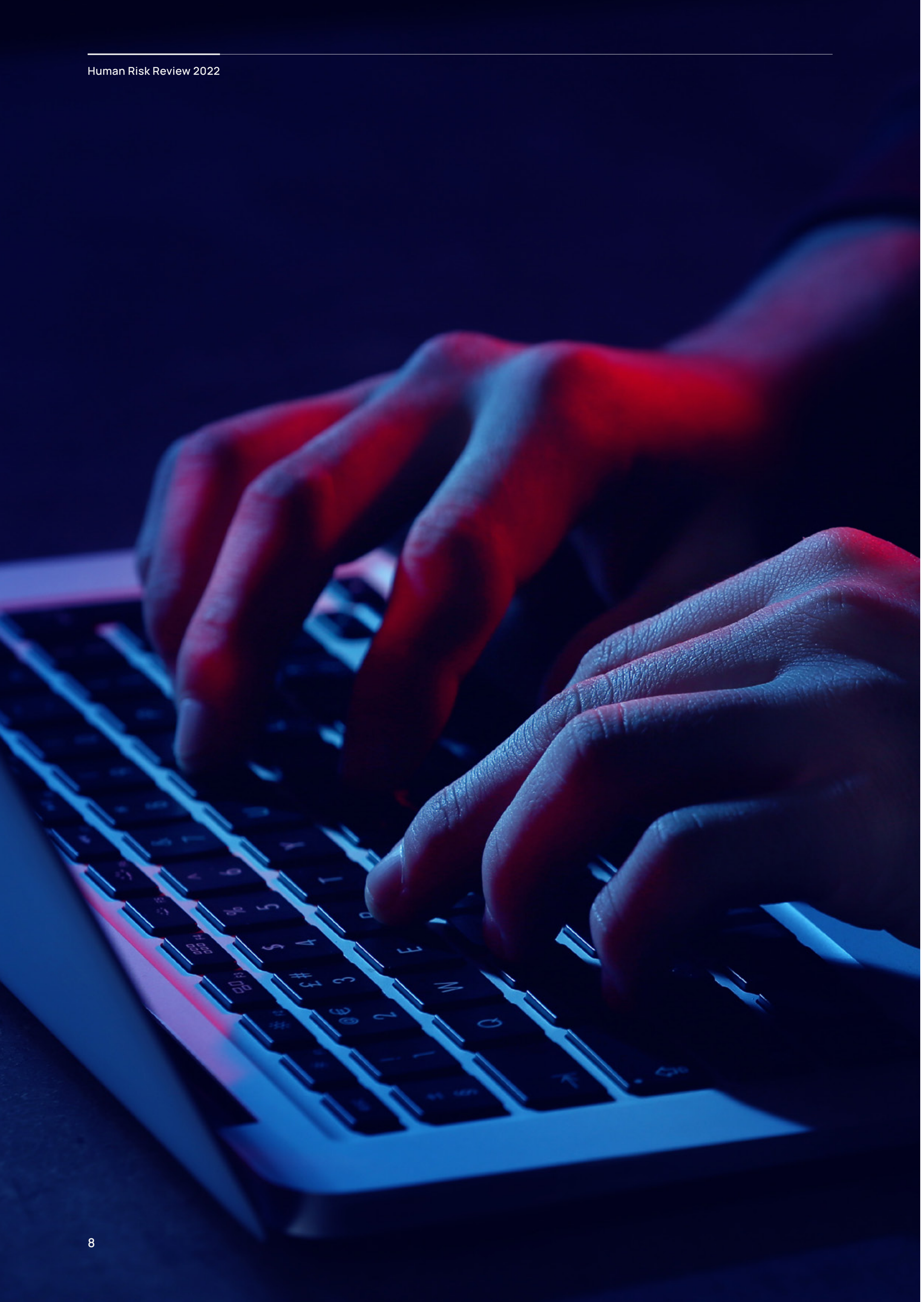
More than 90% of IT and cybersecurity specialists say:



Awareness is important in their respective organization, yet 40% of these organizations state that employee awareness is low. Over two thirds of survey respondents thus plan to expand their awareness measures in the coming year.

99% of respondents say that the strength of organizations’ security cultures will be important in the coming year.

> “Humans are the most important factor in cyber resilience.”
>
> **Vivien Bilquez,** Principal Cyber Risk Engineer at Zurich Resilience Solutions



01 The cyberthreat landscape: familiar tactics and new extremes

An overview of some alarming facts and figures from the past year

2021 left us no time to rest with regard to cybersecurity. Cybercriminals have been increasingly professionalizing for years as they hone their methods. Many of their tactics have long since become unique business models, and cybercrime-as-a-service is booming.[1]

Cybercrime is the world's top business risk, costing trillions of dollars in damage

A poll released by Allianz-Versicherung during the second year of the pandemic revealed that cyber incidents have become the most important business risk.[2] The previous year's report showed that cyberattacks cost an incredible 1 trillion dollars for the global economy, equating to a 50 percent increase from the figure two years prior.[3] Other sources report even higher damages. Cisco CEO Chuck Robbins spoke of 6 trillion dollars in damages per year at the RSA Conference 2021.[4]

Risk of data misuse via ransomware increased by over 800%

Ransomware attacks have become considerably more prevalent, in particular those with the aim of multiple extortion. The risk of stolen data being released due to ransomware attacks increased from 8.7 percent in 2020 to 81 percent in the second

[1] Forbes (2021). The Destructive Rise of Ransomware-As-A-Service.

[2] Allianz (2022). Allianz Risk Barometer 2022: Cyber perils outrank Covid-19 and broken supply chains as top global business risk.

[3] Allianz (2021). Allianz Risk Barometer – Identifying the major business risks for 2021.

[4] SDX Central (2021). Cisco CEO: Cybercrime Damages Hit $6 Trillion.

quarter of 2021 as a result of this tactic.[5] At the same time, the average costs of a data protection violation in 2021 was 4.24 million US dollars greater than ever before, according to IBM.[6] Geopolitical conflicts will drive the advancement of ransomware even further, and the tactic will cause conflicts to be waged in cyberspace as well. In the context of Russia's attack on Ukraine, for example, ransomware group Conti sided with the Kremlin in order to attack Ukrainian critical infrastructure organizations, among other things (see page 22).[7]

Unexpected vulnerability in Java logging framework causes millions in damages

Not even 72 hours after discovery of the Log4j security flaw in December 2021, 800,000 cyberattacks that exploited the Log4j security flaw were recorded not even 72 hours after the flaw was discovered.[8] CISA Director Jen Easterly referred to it as "the most severe that [she has] seen in [her] career".[9] The President of the German Federal Office for Information Security (BSI) Arne Schönbohm predicted millions in damages for the German economy alone.[10]

The "King of Malware" Emotet is back – and stronger than ever

After international authorities working with Europol were able to take down the dangerous malware Emotet in early 2021, it returned with full force not one year later. The Trojan has been active since November 2021, using the infrastructure of the banking Trojan Trickbot to access systems via spam emails and compromised Excel files, for example. International authorities agree that there will be waves of attacks in the coming months.[11]

[5] European Union Agency for Cybersecurity (ENISA) (2021). ENISA Threat Landscape 2021.

[6] IBM (2021). How much does a data breach cost?

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

[8] Ars Technica (2021). Hackers launch over 840,000 attacks through Log4J flaw.

[9] National Security Agency (2021). CISA, FBI, NSA, and International Partners Issue Advisory to Mitigate Apache Log4J Vulnerabilities.

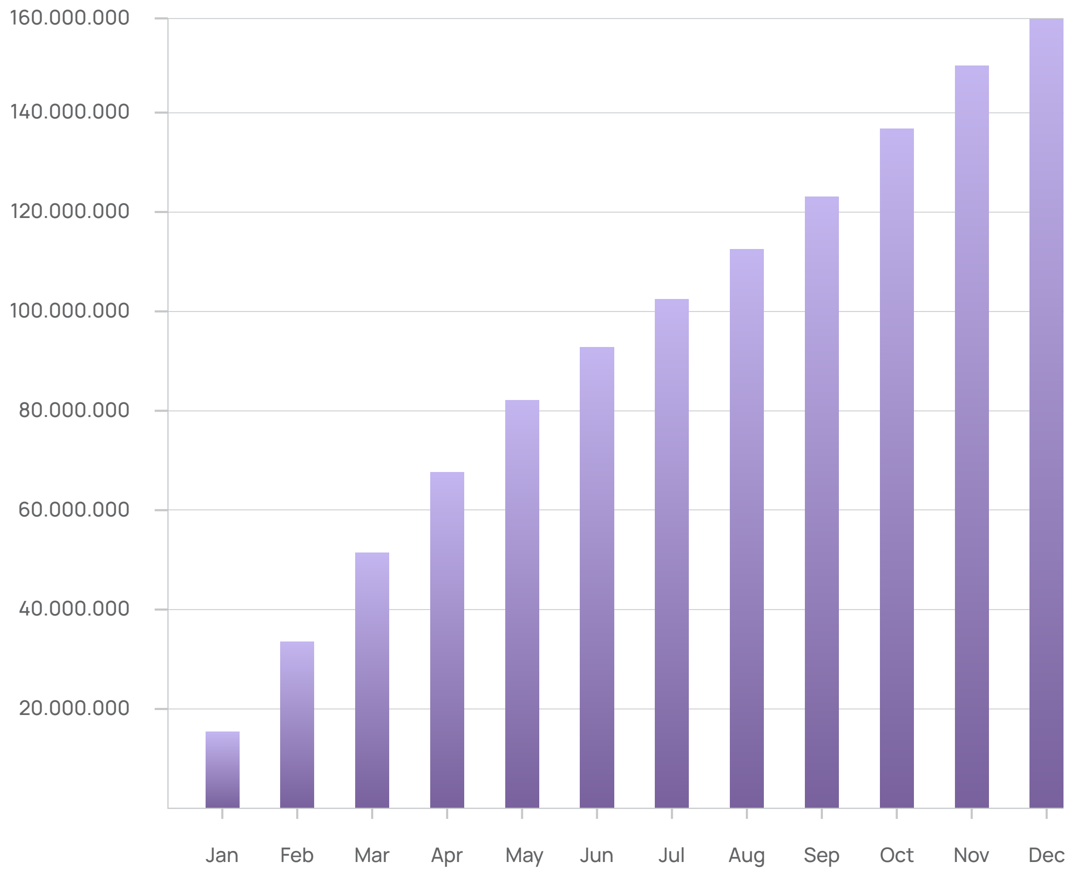
[10] Wirtschaftswoche (2021). BSI-Chef: "Deutscher Wirtschaft drohen enorme Schäden durch neue Sicherheitslücke".

[11] Dark Reading (2022). Emotet is Back and More Dangerous than Before.

1.1 Malware on a continuous ascent

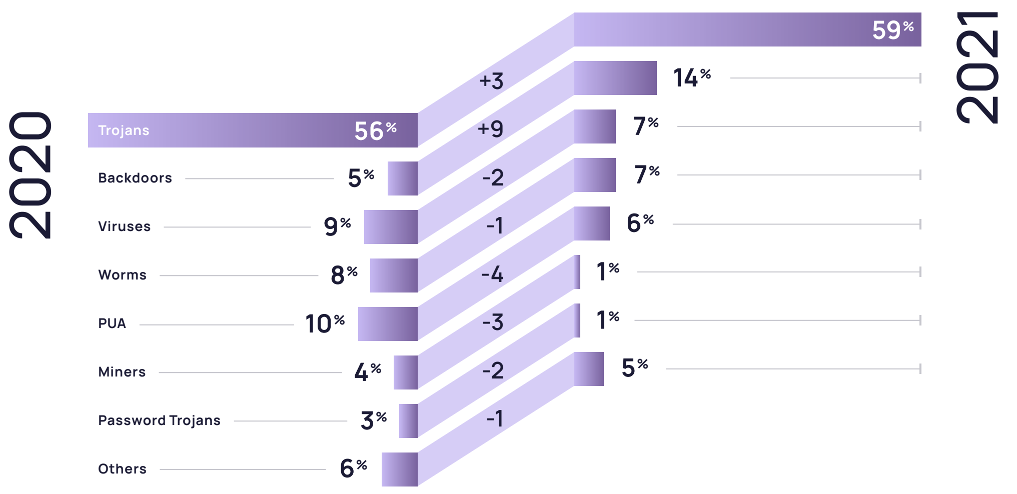
This analysis is based on data from the AV-ATLAS Threat Intelligence Platform from AV-TEST GmbH, which conducts fully automated analyses and classifications of malware, thereby facilitating comprehensive comparative test.[12]

Number of newly identified types of malware in 2021



More than 160 million new types of malware were identified in 2021, with sharp increases between January and April with over 15 million new malware programs each. Overall, the total is now at over one billion recognized types of malware since 2008, or more than twice the total from five years ago.

Frequency of different types of malware in 2020 vs. 2021



Most of the known malware programs are Trojans, which make up nearly two thirds of the total. There is also a considerable and proportional increase in backdoor attacks, which at 14 percent are now nearly three times as common as the previous year. These are often disseminated via Trojans or phishing emails and enter systems unbeknownst to the user. On the other hand, the number of potentially unwanted applications (PUA), like adware, has decreased.

Malware attacks thus remain a dangerous risk to organizations, and the advancement of malware types makes purely technical prevention difficult, if not impossible. Most of the known malware types such as Trojans (including the “King of Malware”, Emotet[13]) and backdoors use people as a gateway to sensitive information and systems. As stated above, criminals are increasingly making use of extortion Trojans known as ransomware. The ransomware group Conti leaked internal chats and sensitive data in early 2022. It was revealed that the parties involved allegedly achieved nearly 200 million US dollars in profit with such attacks the previous year.[14] Employees are thus the most important line of defense for organizations, as they are the primary target of professionalized cybercrime business models.

[12] AV-TEST – The independent IT-Security Institute (2022). AV-ATLAS.

[13] Bundesamt für Sicherheit in der Informationstechnik (2021). Emotet-Infrastruktur zerschlagen – BSI informiert Betroffene.

[14] Krebs on Security (2022). Conti Ransomware Group Diaries, Part III: Weaponry.

1.2 The major cybercrime trends in 2022

1.2.1 Waves of current event-based phishing attacks: unscrupulous deceit

Phishing is the constant among cybercriminals' tactics. They are drawing on current events and developments with increasing speed to conduct targeted attacks, especially when they can use fear as motivation. For example, the beginning of the pandemic in 2020 provided an ideal opportunity for this method. Cybercriminals were also active in 2021, attacking their victims in highly sensitive situations without hesitation.

Just a few weeks after the COVID-19 Omicron variant became global news, a phishing attempt based on this development occurred. Passing themselves off as the National Health Service (NHS), the cybercriminals were offering supposedly free PCR tests in December 2021 that were, according to them, specially developed to detect the Omicron variant. Residents throughout Great Britain were contacted via text message, email, and even telephone and manipulated into disclosing personal information. A fabricated screen for ordering the tests asked the victims to provide their names, addresses, and bank accounts, and to answer highly sensitive security questions.[15]

In one extreme case of such phishing attacks based on topical developments, Russia's attack on Ukraine is resulting in an unprecedented increase in cybercrime activity (see page 22). Entities in support of both the Russian and Ukrainian governments have been attacked. Criminals have also taken advantage of residents who are hoping to aid those affected by the situation. For example, fraudulent charity drives have been disseminated on social media and via phishing emails.[16] SoSafe warns of a particularly nefarious scheme in which links presumably used to conduct DDoS attacks on Russian servers and services were shared. Clicks on these links allowed cybercriminals to install viruses and Trojans into individuals' systems.[17]

These incidents illustrate how important it is for users to anticipate and understand emotionally manipulative tricks so that they can protect themselves from often costly consequences in both their personal and work lives.

1.2.2 Supply chain attacks: maximization of profit via targeted attacks on service providers

Attacks on supply chains became more frequent in 2020. There was a further increase in these attacks in 2021, in which supposed vulnerabilities in the supply chain of multiple companies are attacked, sometimes with far-reaching consequences. For example, groups like REvil, BlackMatter, or DarkSide conducted large-scale attacks on the HR platform Kronos, the oil pipeline system Colonial Pipeline, and meat producer JBS. The Chinese cyber espionage group APT27, also known as LuckyMouse or EmissaryPanda, frequently attacked smaller companies. Further victims were then targeted via the supply chain, in particular organizations from the pharmaceutical and technology industries.[18]

The ransomware attack on IT service provider Kaseya exemplified the scope of these complex attack methods, affecting an estimated 1500 companies worldwide, including in the USA, Germany, and the Netherlands.[19] Via a supposed software update, the perpetrators not only gained access to Kaseya's systems, but were also able to spread the infected software to the IT systems of Kaseya's customers and the entire supply chain. Companies without any direct affiliation to Kaseya were also affected. Organizations find themselves in an increasingly precarious position as they select their partners and weigh the associated risks. This is because all parties within a network must maintain a strong security culture in order to effectively prevent risks. In the future, such connected (human) resilience will be of massive importance.

[15] The Independent (2021). Scam warning over fake omicron testing text messages.

[16] Fortune (2022). Scammers are pretending to raise money for Ukraine. Here's how to make sure your donation goes to the right place.

[17] SoSafe (2022). SoSafe warnt vor Social-Engineering-Angriffen im Kontext des Angriffskrieges auf die Ukraine.

[18] Bleeping Computer (2022). German govt warns of APT27 hackers backdooring business networks.

[19] The Washington Post (2021). Ransomware attack struck between 800 and 1,500 businesses, says company at center of hack.

1.2.3 Multiple extortion: expanded ransomware scams

ENISA refers to the current situation as a "golden era of ransomware".[20] Attacks with incredible sums gained through extortion are dominating headlines around the world. Simple extortion and purely technical attacks are a thing of the past. Cybercriminals have long since utilized sophisticated and psychologically advanced extortion techniques in conjunction with other methods. This is known as multiple extortion, and has also entailed additional DDoS attacks, crypto-minding, and botnets.

Yet, in addition to the initial theft and encryption of sensitive information (and the threat of releasing this information in the event of non-payment), attackers are now also demanding ransom claims from the customers or partners of the actual victim if the victim does not cooperate. In April 2021, for example, REvil attacked computer manufacturer Quanta Computer. When the company did not meet the ransom demands, the attackers contacted Apple – a client of Quanta Computer – and threatened to release the information on the latest MacBook Pro that had been stolen from the manufacturer. It remains uncertain whether Apple paid the ransom of 50 million dollars.[21]

1.2.4 Artificial intelligence and deepfakes: new technology escalates frequency of attacks

Artificial intelligence (AI) is becoming ever more common. Famous examples like Amazon's virtual assistant Alexa show how smart technology is integrating into our everyday lives and becoming an invaluable aid. According to a prediction by the International Data Corporation, companies around the world will pay more than 204 billion US dollars for AI software in 2025. This equates to an annual increase of 24.5 percent between 2021 and 2025.[22] AI-based tools are also being increasingly used in the field of cybersecurity to protect against attacks. However, cybercriminals quickly learned that this technology can also be used for social engineering and phishing and can allow them to maximize their profits (see info box on page 19).

[20] European Union Agency for Cybersecurity (ENISA) (2021). ENISA Threat Landscape 2021.

[21] Bloomberg (2021). Apple Targeted in $50 Million Ransomware Hack of Supplier Quanta.

[22] International Data Corporation (2021). Investment in Artificial Intelligence Solutions Will Accelerate as Businesses Seek Insights, Efficiency, and Innovation, According to a New IDC Spending Guide.

Voice phishing (vishing), to name one example, is being successfully combined with deepfake technology and used to legitimize phishing emails in advance. Another method, voice cloning, refers to when attackers use AI to imitate the voice of a superior and call employees with the request to disclose sensitive information or make bank transfers. This was how criminals were able to steal 35 million dollars from a bank in Hong Kong in 2020.[23] Some sources believe that it is just a matter of time until AI technology is used for large-scale, political disinformation campaigns.[24]

1.2.5 Hybrid work: new work model as source of cyber risks

The number of organizations relying on mobile or remote work has increased drastically since the beginning of the COVID-19 pandemic. They are not only faced with logistic challenges, but a greater risk of cyberattacks in particular. According to IBM, the costs of data protection violations in the event of attacks is on average 1.07 million US dollars higher when remote work is involved.[25] The risk is increased due to a variety of reasons: Many organizations do not secure company cell phones or laptops with a connection to the company network. Furthermore, collaboration tools like Microsoft Teams and even cell phones increasingly offer new targets. A study conducted in the USA and Canada by security provider 1Password shows that employees themselves have become more vulnerable as well. Exhausted by the pandemic and remote work, they are far less preoccupied with security guidelines, which in turn makes them more prone to make errors. This also applies in particular to company security specialists who are under greater pressure than ever before due to these changes.[26]

The consequential ransomware attack on Colonial Pipeline in April 2021 was attributed to a VPN network that employees used for remote work. An unsecure password fell into cybercriminals' hands, granting them access to the VPN account and numerous internal systems and data.[27] The result: A weeks-long gasoline shortage along the East Coast of the United States. A clear majority of IT and cybersecurity specialists in organizations confirm the risk that hybrid work entails: 9 out of 10 respondents for this report state that the threat landscape has worsened. 75 percent of these say that mobile work has played a role in this. The Human Risk Review 2021 even showed that the success rate of phishing attacks has tripled with decentralized work compared to centralized work. More than two thirds of the respondents would thus like to expand their awareness measures in the coming year (see poll on page 62).

[23] Forbes (2021). Fraudsters Cloned Company Director's Voice In $35 Million Bank Heist, Police Find.

[24] BBC (2020). Deepfakes: A threat to democracy or just a bit of fun?

INFOBOX

Quantity and quality with AI – the next generation of phishing

In a study conducted by a research team at Singapore's Government Technology Agency, it was recently discovered that AI-as-a-service models can create convincing spear phishing emails. The artificially generated emails were clicked on more often than those created by humans.[28]

→ Phishing on a large scale

The study was small in scale at first. However, the results of the research showed that tactics like spear phishing, vishing, and dynamite phishing with AI models and insufficiently monitored, service-based AI are being adapted to defraud large masses of people and organizations. Criminals can thus create and send seemingly legitimate spear phishing emails with ease and without any advanced knowledge, on a grand scale and with high prospects for success.

→ How can one stay protected?

The results from the research team in Singapore also reveal that AI tools that are designed to detect against harmful AI text or bots are still often faulty. They thus recommend taking AI-assisted, human security precautions.

Organizations should train their employees and provide them with tools that help them recognize harmful content in order to prepare for the flood of automatically generated attacks. Context-based and always up-to-date training minimizes the risk of falling victim to such a cyberattack, sometimes drastically (see Behavioral Security Model on page 50).

[25] IBM (2021). How much does a data breach cost?

[26] ZDNet (2021). Everyone is burned out. That's becoming a security nightmare.

[27] Bloomberg (2021). Hackers Breached Colonial Pipeline Using Compromised Password.

[28] Wired (2021). AI Wrote Better Phishing Emails Than Humans in a Recent Test.

1.3 Global threats lead to stricter regulations

1.6 billion euros: This is how much the European Union (EU) invested in cybersecurity until 2027 as part of the “Digital Europe Programme”.[29] With the new version of the NIS Directive “NIS2”, cybersecurity standards are to be made uniform across EU member states. In the field of organized crime, too, EU-wide cyberattacks have long since numbered in the top 10 priority topics.[30] The more professionalized cybercriminality becomes, the more inter-sector and international the attacks will become. This necessitates cooperation between various countries, states, and private enterprises.

New regulations and liability risk for CEOs

Industry-specific regulations are subjecting companies to further obligations in addition to Europe-wide directives such as the General Data Protection Regulation (GDPR). Cybersecurity is thus increasingly becoming a matter for which companies themselves are responsible. The topic is no longer solely relevant to cybersecurity experts and is becoming a more important topic at the executive level. Executives of limited liability companies and boards of directors at corporations now have to protect their companies against attacks. They are becoming increasingly liable if it cannot be verified that sufficient security precautions had been taken before an attack occurred. The situation is particularly serious in the event of physical security incidents (see “Overview of sectors”, page 27).

[29] European Council (2021). Cybersecurity: how the EU tackles cyber threats.

[30] European Council (2021). Fight against organised crime: Council sets out 10 priorities for the next 4 years.

What companies have to do

→ Establish a culture of cybersecurity

In the future, companies will be increasingly legally obligated to actively take precautions against cyberattacks. Technical measures alone do not suffice. All employees must be involved and educated about potential dangers so that they can properly protect themselves.

→ Ensure verification of adherence to compliance

Verification for certifications such as ISO/IEC-27001 is becoming ever more comprehensive and necessary across all industries. Companies should now start ensuring that they are able to present such verification. You are on a good footing if you have suitable solutions and compliance dashboards.

→ Work together with experts

Regular meetings between CISOs, cybersecurity offers, and the executive level provide an overview of the company’s current security plan and the latest guidelines. This simplifies the continued joint security strategy and budget planning.

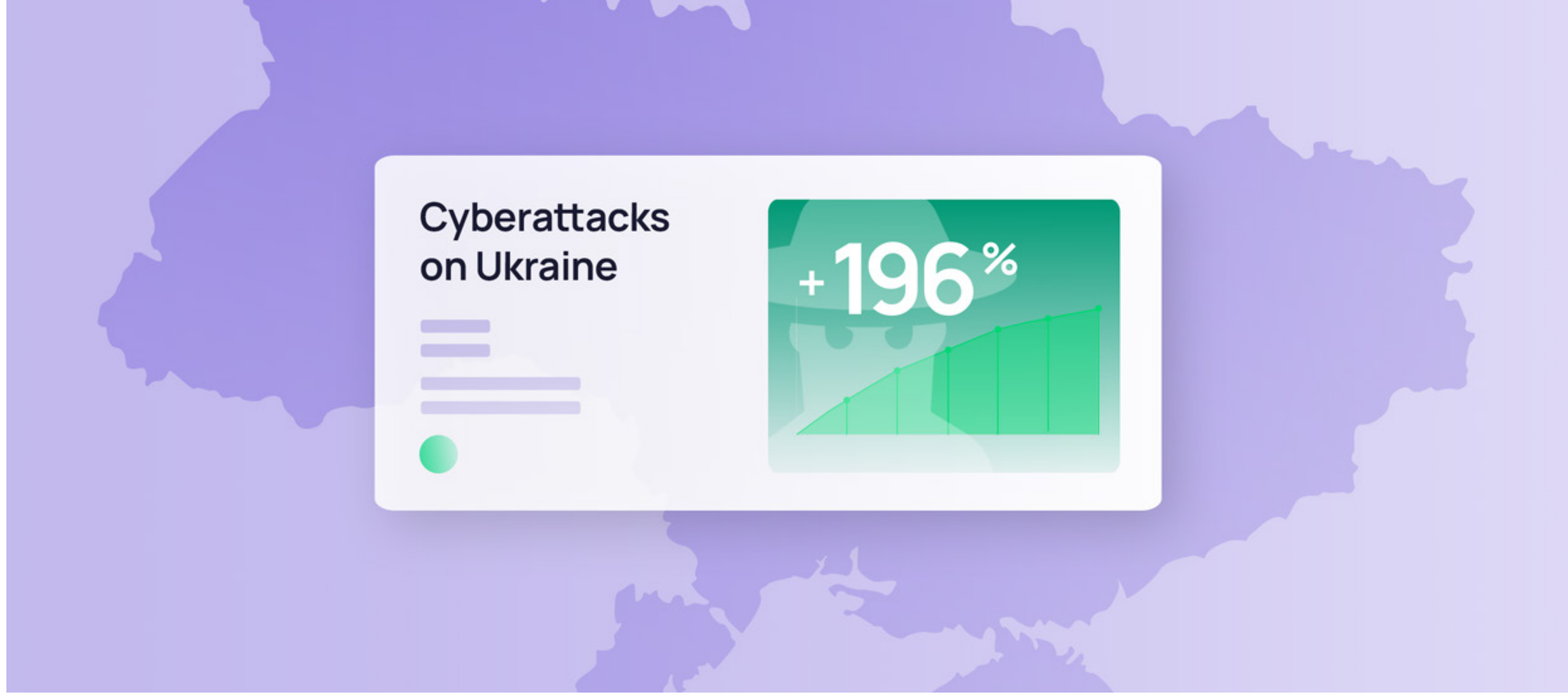
→ Regular reporting to executive management

In order to clearly highlight the relevance of cybersecurity at the executive level as well, you should regularly speak with executives about the current risks and the success of your cybersecurity measures. Make use of reporting to present concrete figures and, in the worst-case scenario, quickly make decisions, such as the swift and efficient implementation of any necessary countermeasures.

1.4 Hybrid war: how Russia's attack on Ukraine is also being waged in cyberspace

Cybercriminals are increasingly taking advantage of current political, social, and societal issues for purposes of social engineering (see page X). Waves of cyberattacks pertaining to current events become particularly extreme when geopolitical conflicts occur. Wars have long not only been fought on the battlefield, but also in cyberspace, as Russia's assault against Ukraine has most recently shown. The scope of this is still difficult to ascertain, and the overall situation is unclear given the wide range of figures, entities, and groups involved.

One thing is certain: Cyberattacks are used to wage hybrid warfare and aim to weaken the opposing side's ability to act. The perpetrators are highly creative in their selection of tactics, and utilize phishing, DDoS attacks, and ransomware, among others. According to Check Point Security, the number of cyberattacks against Ukraine has increased by 196 percent in just the first three days of the war, whereas attacks against Russia increased by only 4 percent. Overall, the number of phishing emails in eastern Slavic languages has increased sevenfold.[31] Google Threats Analysis Group also reports multiple groups, such as FancyBear and Ghostwriter, who are involved in the conflict through espionage, DDoS attacks, and phishing campaigns.[32] Critical infrastructure operations like banks, suppliers, and insurance providers have been under a digital siege since the war began – but other organizations around the world have also been caught in the crosshairs in response to Western sanctions.[33]



Ransomware group Conti, known for its "big game hunting" in which it attacks large corporations, announced it is siding with Russia. Shortly thereafter, internal chats and sensitive data from the "company" itself were leaked. This cyberwar is thus not one-sided, and there have also been reports of counterattacks, such as by the hacker collective Anonymous. Anonymous also appealed to other hacker collectives to attack Russian aggressors and allies.[34]

In addition to the immeasurable destruction and the physical and psychological consequences of the war, organizations are also experiencing "spillover effects". In a digital, interconnected world, cyberattacks on critical infrastructures swiftly spread to supply chains (including software supply chains), thereby putting the Internet security of organizations around the world to the test. SoSafe thus advises organizations to be on high alert in these uncertain times. An already tense cyberthreat landscape is coupled with warnings of ransomware and deceptive social engineering campaigns (including against individuals). State cybersecurity institutes around the world issued security warnings, including the German BSI[35], the Cybersecurity & Infrastructure Security Agency (CISA) in the United States[36], the French Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR)[37], the Dutch Nationaal Cyber Security Centrum[38], and the British National Cyber Security Centre (NCSC)[39]. They recommend keeping a close eye on the situation and implementing security measures. Reinforce your security measures accordingly and ensure that you have taken every necessary step to safeguard your organization (including for liability reasons). These also include business continuity plans so that you can withstand a serious incident. Furthermore, cybersecurity is more than IT. It is closely linked to the physical security of people around the world. Managers from all industries should thus work together on cohesive solutions and create and implement strong security strategies.

[31] Check Point Security (2022). Cyber Attack Trends In The Midst Of Warfare – The numbers behind the first days of the conflict.

[32] Google (2022). An update on the threat landscape.

[33] The Guardian (2022). UK firms warned of Russian cyberwar 'spillover' from Ukraine.

[34] Fortune (2022). Hacker collective Anonymous declares war on Russia.

[35] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2022). Einschätzung der aktuellen Cyber-Sicherheitslage in Deutschland nach dem russischen Angriff auf die Ukraine.

[36] US Cybersecurity & Infrastructure Security Agency (CISA) (2022). Shields up.

[37] Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) (2022). [MàJ] Tensions internationales – Menace cyber.

[38] Nationaal Cyber Security Centrum (2022). Digitale aanvallen Oekraïne: een tijdlijn.

[39] National Cyber Security Centre (NCSC) (2022). NCSC advises organisations to act following Russia's attack on Ukraine.

Achim Berg, Bitkom

> “We require decisive and guiding figures at the management level.”

Achim Berg is President of the digital association Bitkom, with a wealth of experience in management positions in IT corporations like Microsoft. He is also active as a member on the board of directors or advisory board in multiple digital companies, including Flixbus and powercloud.

What role does cybersecurity play in your personal and professional life?

Cybersecurity is a constant in our lives, including my own. It is often subconscious, like routinely using two-factor authentication or encrypted communication, or making automated back-ups. For me personally, but also for the economy and society as a whole, achieving the cybersecurity goals of confidentiality, availability, and integrity play an important role in our personal and professional lives.

Bitkom recently published findings that show that 8 out of 10 Internet users fell victim to cybercrime in the past year. How do you assess the general threat level of the internet?

The threat level in cyberspace is tense. No company, governmental authority, or individual is safe against cyberattacks. The many potential gateways pose a considerable challenge to companies. While most attacks begin with phishing and social engineering, unpatched systems also open up new means of access to cybercriminals. It is ultimately insignificant whether the attackers achieve their goals through phishing, supply chain attacks, 0- or n-day vulnerabilities, misconfigured cloud environments, shadow IT, or insider threats. Criminals find a way. That’s why it’s important to arm yourself for whatever may happen and take a proactive approach to the topic of cybersecurity.

We have seen some spectacular phishing and ransomware incidents this year, with very expensive consequences. Are you seeing this topic become more important at the board level?

Definitely. Cybersecurity cannot be left uncoordinated and in the hands of the many. It requires a centralized area of accountability at the executive level where priorities are defined and budgets are canalized. Only then can a cohesive security culture be promoted and robust security management established. The human factor plays just as important a role as the technical and organizational aspects, of course.

What role do managers play when it comes to cybersecurity?

Managers have the important role of setting an example, as they influence their staff when they prioritize the topic. One of the main problems is that cybersecurity is often seen as a purely technical topic and left to IT departments. This is where the topic is often supposed to be resolved, or so it’s believed. Unfortunately, this is insufficient. In addition to technical measures, robust security management also entails target group-specific training for employees, establishing emergency processes, and regularly assessing the respective security plan. For this we require decisive and guiding figures at the management level.

What do you believe are the most important cybersecurity developments that organizations should keep an eye on in the coming year?

From a normal company’s perspective, it’s important not to focus too hard on what’s happening outside and follow new developments that way. Rather, companies need to look inward. Am I prepared for an emergency? If so, does my emergency management work in practice? Should I not also opt to establish a cybersecurity management system to get ahead of the wave? Are we providing enough personnel and financial resources? These are just a few of the questions that should be openly and honestly discussed within the company. It comes down to this.

The threat level of the human factor further increased last year. Are we optimally prepared for this in Germany and Europe?

Digitization and cybersecurity are two sides of the same coin. Unfortunately, the sluggish rate of digitization in Germany has resulted in a widespread deficiency in digital skills. This has a direct impact on cybersecurity. Nevertheless, in Germany and Europe we have a terrific head start when it comes to IT and cybersecurity. Our research is at the forefront of international rankings, and we have very many strong and highly innovative cybersecurity companies. We have to use that.

What are the three most important aspects for a balanced cybersecurity strategy?

It is imperative that a cohesive security culture be promoted within the company, and that a robust security management system be established. Security is not a one-time solution, but rather a process. This understanding of security has to be embodied in companies and governmental bodies. More specifically, it is a balance of the three pillars: 1. the technology, 2. the organization, and 3. the individual.

02 Overview of sectors: industry-specific cyber risks and regulations

As cybercrime becomes more professionalized, the attackers are specializing in the individual sectors and industries that they target. Cyber-criminals are adapting their tactics to each industry's unique challenges and vulnerabilities. Below we show you what select industries are up against, and what measures can protect them in the future.

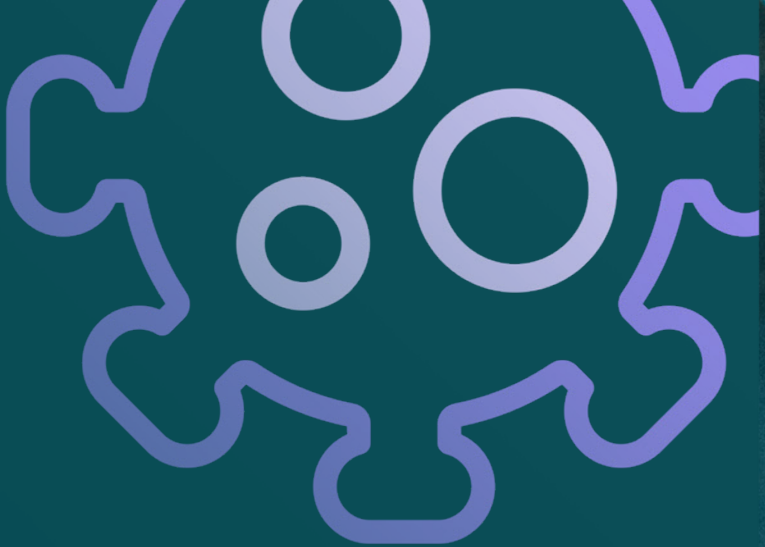
2.1 Retail

Rushed digitization and globally interlinked supply chains

Retail has undergone a precipitous digitization process in the past two years

Lockdown-induced store closures and the rise in online orders shifted many processes into the digital realm. Many local retailers took their first foray into e-commerce and are often still insufficiently prepared for the risks this entails.

Retail companies are already an attractive target for cybercriminals, as they work with sensitive customer information. At the same time, it is difficult to sensitize staff to cyber risks due to the high fluctuation of employees and seasonal peak times. Governmental authorities continue to warn of an increased threat level in particularly busy times such as Black Friday and Christmas.[40] A phishing simulation campaign created by SoSafe for Black Friday also shows that phishing attacks pertaining to current events increase the average click rate by more than 120 percent.



Example case: IKEA struggles with reply chain attack

Shortly before the Christmas 2021 season, Swedish furniture manufacturer IKEA was targeted by cybercriminals who started a reply chain attack with stolen email credentials.[41] They used real IKEA email addresses to send malware like Emotet or Qbot internally and to partners in the supply chain.

This type of phishing is particularly dangerous, as it is quite difficult for employees to recognize the nefarious nature of these emails. Although IKEA was able to respond early on and thus prevent any more serious damage, this case shows how professional attackers have become. Retailers are faced with the risk of costly disruptions to business. For example, the Swedish supermarket Coop had to temporarily close around 500 stores following a cyberattack in the summer of 2021.[42]

[40] National Cyber Security Centre (NCSC) (2021). Guidance for retailers to prevent websites becoming Black Friday cyber traps.

[41] CPO Magazine (2021). IKEA Suffers Ongoing Phishing Attacks From Compromised Internal and Vendor accounts.

[42] BBC (2021). Swedish Coop supermarkets shut due to US ransomware cyber-attack.

2.2 Production

Industry 4.0, costly halts to production, and exclusive, immaterial goods

New attack vectors make production a target for cybercriminals

A few years ago, production companies were relatively safe against cyberattacks. Following the comprehensive digitization for Industry 4.0, and connectivity, however, attackers have new potential targets. Companies in this industry are particularly susceptible to attacks on supply chains and resulting halts to production. Costly suspensions of plant operation caused by malware provide cybercriminals with ideal conditions for extortion.

The automotive industry is responding to the growing risks by stipulating a comprehensive cybersecurity standard: Without Trusted Information Security Assessment Exchange certification (TISAX), manufacturers, suppliers, and service providers from the automotive sector can hardly stay competitive. Sensitization of all parties in the supply chain through extensive awareness measures not only provides reliable protection against cyberattacks, but also upholds TISAX compliance. Verification can most easily be rendered via special compliance dashboards.

Example case: Ransomware disables IT infrastructure at Eberspächer

The ongoing coronavirus pandemic and semiconductor shortage left automotive companies in a difficult position in 2021. Automotive supplier Eberspächer fell victim to a ransomware attack in October 2021.

The family-operated company from Baden-Württemberg employs around 10,000 people across 80 locations in 28 countries and is one of the world's most profitable suppliers for vehicle electronics, among other products. The attack had a massive impact on the company's infrastructure, with the website temporarily unavailable and all IT systems deactivated as a security precaution.[43] In December 2021, automotive manufacturer Volvo announced the theft of confidential research data.[44]

[43] Eberspächer (2021). Nach Hackerangriff auf Eberspächer Group.

[44] Volvo Cars (2021). Notice of cyber security breach by third party.

2.3 Finance

Sensitive data and increasingly strict regulations

Extreme increase in cyberattacks on the financial sector

Credit and financial services institutions have recently introduced faster and smarter online payment processes – and at the same time sent many of their employees to work from home. Online banks such as N26 and other FinTechs also got a boost. It was already evident in the first lockdown phase between February and April 2020 that cybercriminals, too, are making use of this change: The number of cyberattacks on the financial sector increased by 238 percent.[45] Customers' sensitive data and personal banking details can be sold on the black market for horrendous sums. The ransom demands from ransomware attacks are correspondingly high. A data breach in the financial sector costs institutions an average of 5.72 million dollars.[46]

Christine Lagarde, President of the European Central Bank (ECB), goes one step further and sees widespread cyberattacks on the financial system as a systemic risk. Speaking at the annual conference of the European Systemic Risk Board (ESRB), she said: "The cyberattacks on hospitals in Europe during the COVID-19 crisis and the attack on the Colonial Pipeline in the United States have given us a taste of what could happen in the future. Such an attack is probably now a question of when, not if."[47] In view of these developments, the need for awareness and educational training measures for employees is coming to the fore.

Example case: Damage of image at Volkswagen & big game hunting at CNA Financial

In June 2021, numerous customers at German Volksbank and Raiffeisenbank were unable to carry out transactions via online banking and were no longer able to access their accounts digitally. The websites of several cooperative banks were also temporarily unavailable.

The cause: Cybercriminals had sabotaged the data centers of the banks' IT service provider.[48] While the Volks- and Raiffeisenbanks got off relatively lightly in this incident, with a tarnished image, the cyberattack on the US insurer CNA Financial is a classic example of big game hunting by cyber criminals. The attack made headlines mainly because of the ransom. CNA Financial paid the largest known ransom payment to date, $40 million, following a ransomware incident.[49]

[45] Allianz (2021). Financial services: Risk trends.

[46] IBM (2021). Cost of Data Breach.

[47] European Central Bank (2022). Macroprudential policy in Europe – the future depends on what we do today.

[48] Handelsblatt (2021). Sabotageangriff legt Onlinebanking bei mehr als 820 Banken lahm.

[49] Business Insider (2022). One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack.

2.4 Public sector

Increased media interest as a means of pressure

Ransomware as an industry-specific threat

Successful attacks on cities and municipal bodies are increasing. The consequences: Work is interrupted for weeks, sometimes even months.

The IT infrastructure in the public sector is often outdated, making it easy for professional attackers to gain access. In addition, the media interest in these cases is great. After all, many citizens are dependent on the services of local government, such as maintenance payments or vehicle registrations. And if sensitive data falls into the wrong hands, there are consequences for individuals as well. This increases the pressure on the affected organization. In turn, the criminals hope that their ransom demands will be fulfilled all the more.[50]

Example case: First case of German cyber disaster after attack on district

In July 2021, several servers in a district in Germany were infected with ransomware and a large amount of data was encrypted as a result. Many services could no longer be processed.

The Bundeswehr, the German military, provided support. Even months after the attack, the proclaimed emergency was still in effect. The ransom was not paid.[51] But the situation is also getting worse elsewhere: More than 150 American government agencies and non-governmental organizations (NGOs) fell victim to the Nobelium group last year, which also carried out the well-known attack on the US software manufacturer SolarWinds.[52] In spring 2021, a ransomware attack hit Spain's employment agency during an already tense time due to the coronavirus crisis.[53]

[50] Forbes (2021). Municipal Cyberattacks: A New Threat Or Persistent Risk?
[51] Deutsche Welle (2021). Rural German district declares disaster after cyberattack.
[52] Microsoft (2021). Another Nobelium Cyberattack.
[53] Infosecurity Magazine (2021). Ransomware “Paralyzes” Spanish Employment Agency.

2.5 Critical infrastructure
Cyber-physical incidents with dramatic consequences – and increased liability risks

Attacks on operational technology pose significant risks

In July 2021, Gartner analyst Wam Voster made a dramatic statement: Soon there will be deaths as a result of cyber-physical incidents.[54] The prediction relates to increased attacks on operational technology (OT), with which physical processes are monitored and controlled. It is used, particularly, in critical infrastructures – that is, organizations whose aim is to ensure general supply. However, critical infrastructure organizations are sometimes still dependent on outdated software. This is because the systems used, such as large medical devices, are expensive – and are therefore only rarely updated or exchanged for new ones. They are the ideal entry points and targets for cybercriminals.

According to Gartner, such attacks are likely to increase in the future. In addition to the personal losses that cannot be quantified, the analysts assume financial damages of more than 50 billion US dollars by 2023. The liability risks for managers and board members will also continue to increase in this context. 75 percent of the CEOs should have to take responsibility for such fatal incidents already by 2024 (also see Chapter 1.3).[55] It is all the more important to protect oneself proactively and to provide appropriate proof of compliance, which protects against costly consequences should worst come to worst.

Example case: Remote operation with almost fatal consequence

A water treatment plant in Florida recently experienced for itself what such as attack can look like. An unknown person got access to the plant's control system via remote access software and adjusted the sodium hydroxide levels to 100 times their level, up to a level that is hazardous to health. Thanks to the diligence of one employee, the attack was quickly detected, and the values could be reduced again. This saved consumers from the worst-case scenario.[56]

[54] Gartner (2021). Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans.

[55] Gartner (2020). Gartner Predicts 75% of CEOs Will be Personally Liable for Cyber-Physical Security Incidents by 2024.

[56] CNN (2021). Florida water treatment facility hack used a dormant remote access software, sheriff says.

Vivien Bilquez, Zurich Resilience Solutions

> "Humans are the most important factor in cyber resilience."

Vivien Bilquez has been in the IT and cyber security sector for over 15 years and until recently taught IT & Information Security at the Université de Lorraine. He currently holds the position of Principal Cyber Risk Engineer at Zurich Resilience Solutions, helping companies to reduce their cyber security risks continuously.

Considering the recent geopolitical shifts as well as the professionalization of cybercrime over the last years, what do you think will be the biggest cyber risks to look out for in the upcoming months and years?

When looking at the recent cyber events in the news, whether a cyber-attack is perpetrated by a cybercriminal, an insider, a hacktivist or a nation-state hacker, in most instances, ransomware was involved. It's not a secret to mention that the number of ransomware attacks doubled in 2021 (compared to 2020). Those attacks not only involved encrypted data of companies but also data exfiltration and the leakage of that data on the public domain. With damages from cybercrime expected to increase considerably this year, we also expect the number of ransomware attacks to increase and newer forms to become more sophisticated and disruptive. The rise of the ransomware attacks is mostly due to the dramatic shift from a linear attack model to an insidious multi-dimensional Ransomware as a Service (RaaS) model. This subscription-based model enables anybody (called an "affiliate") to use ready-to-use ransomware tools to execute attacks and potentially earn a percentage of each successful ransom payment. In the past, hacking was executed by high-skilled IT developers which is no longer true today. Nowadays, anybody can become a hacker. This is multiplying the number of threat actors and obviously the cyber risks for the upcoming months and years.

What are the main trends and changes you see within the cyber insurance industry?

When onboarding a new customer or processing a renewal, our cyber risk assessments used to be mostly of the technical nature. Over time, with most of our customers outsourcing parts of their IT infrastructure to third party vendors or the cloud, the way we are assessing their cyber maturity posture has changed. We are also focusing more and more on governance and compliance as well as Third Party and Cloud Risk Management. The technical controls remain, and expand and become more specific. For example, with the emergence of connected hardware and software to control industrial equipment (OT or Operational Technology) or connected objects (IOT – Internet of Things) in smart offices, we are no longer only looking to Information Technology (IT) security but also to OT and IOT Security. We were always cautious, and we usually recommend physically segregating IT and OT environments to our customers in order to prevent cross contamination. However, a trend on the market is the convergence of IT and OT as IT teams assume the responsibility for the security of physical devices. This new integrated environment, that we can call Industrial Information Technology, is emerging and increasing the attack surface. Ultimately, we can make a link with the previous question, and ask ourselves if the new trends could bring new risks. I personally fear the evolution of cyberattacks from a theft-to-data to a theft-of-control model. By controlling devices that directly interact with people, this could ultimately harm people in the near future.

How do you see the human factor in cyber security from a risk model perspective?

The human factor is probably the most complex factor to address in cyber security. Currently, I participate in external cyber security and our focus is to investigate how to make human-centered security feasible. The group is composed of Cyber Security experts (CISO) and vertical experts like the NCSC, legal, neuroscience and awareness specialists, and technology partners. It is very interesting to challenge the academic view on the topic with the practical experience CISOs struggle with day-to-day. Humans are the most important factor in cyber resilience. When ransomware hits a company, it is often because somebody clicked on a malicious link in a phishing email, trusted and shared confidential information with an unauthorized person over the phone, or left their computer or mobile device exposed and unattended in a public place. How can we avoid this? Awareness trainings, phishing exercises and reward processes for employees are fundamental. It is a constant process and companies have to be creative with their way of delivering the message. Nevertheless, while company employees are one of the primary vectors of cyber-attacks, I always recommend to start with cyber security awareness training for the C-levels. Companies must understand that they are continuously exposed to cyber risks, and they should include security objectives as a fundamental part of their overall business strategy, across all business functions. This is the approach we've taken at Zurich. On the one hand, C-level's highly privileged accounts are a target of choice for hackers. They grant them access to the most sensitive information of a company. On the other hand, C-levels set an example for the rest of the company. As such, they must drive the security culture and avoid exceptions to bypass security measures. Otherwise, it becomes difficult to expect anyone else to follow the internal cyber security guidelines.

A lot of regulations are currently being tightened and liability in case of a successful attack becomes an issue, also for the C-level. What role does cyber insurance play in this situation? What are the most important action areas for the C-level now?

Cyber insurance helps companies reduce their financial risks while doing business online. It typically provides coverage for financial losses suffered due to a cyber incident and includes security and privacy protection as a standard. Liability claims, especially against C-levels, may be addressed with specific D&O (Directors & Officers) Insurance. To mitigate the cyber risks, I would definitely recommend C-Levels to take part in more cyber security training but also to organize and participate in table-top exercises to simulate different cyber scenarios and to test their cyber resilience.

From the cyber insurance perspective, what are the three things every CISO should have top of mind?

Companies must demonstrate a certain cyber security maturity to be a candidate for a Cyber Insurance. If we consider the elements already discussed above, I would recommend every CISO to:

1) Define, implement and test the ransomware readiness of their company (at the IT but also OT/IOT levels);
2) Ensure a proper Third-Party Risk Management;
3) Drive a security culture and strategy built on a top-down approach.

03 Human security risks through social engineering – an analysis

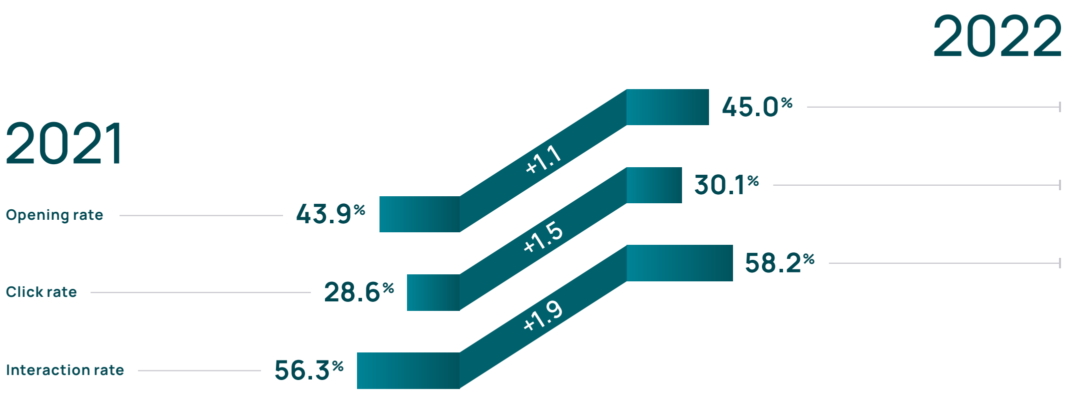
The previous chapters show one thing above all: The threat situation has continued to intensify, and attacks are becoming increasingly focused on people.

But how exactly do cybercriminals attack us? What social engineering tactics work particularly well? And which trends and recommendations for action can be derived from the insights?

In our annual core analysis of phishing and social engineering, we compile psychological and technical data and analyses from various sources and answer these questions.

3.1 Psychological and technical attack vectors in phishing simulations

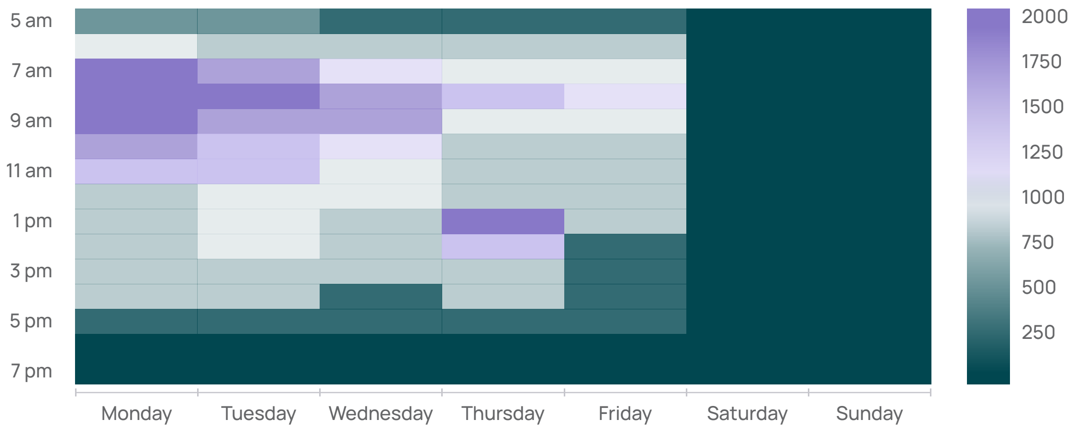
These analyses (pages 42-46) are based on exclusive response data from the SoSafe Awareness Platform. For this purpose, over 4.3 million simulated phishing attacks from 1,500 customer organizations from 2021 were anonymously evaluated, and the probability of success of various attack tactics was analyzed. This results in exclusive insights into psychological, technical, and other vectors that influence human risks in organizations.



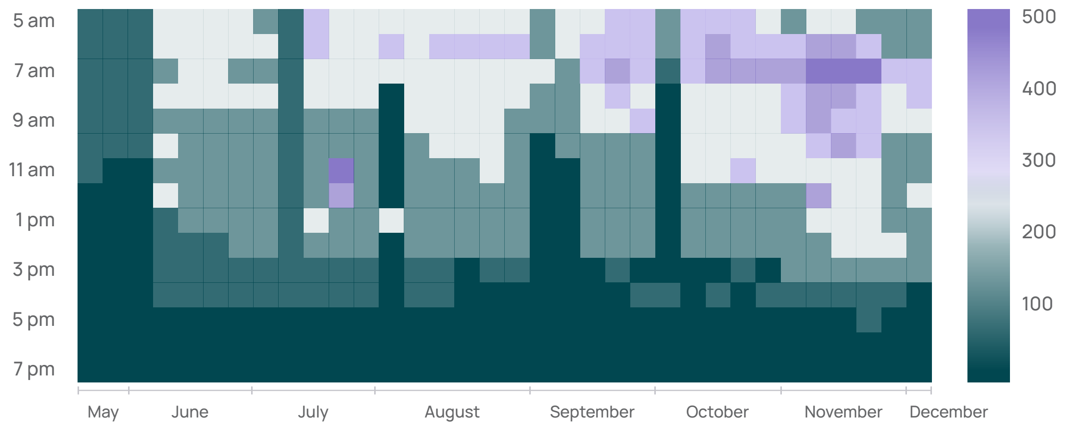
The cyberthreat landscape has intensified – and human risks have not decreased either. The open, click, and interaction rates for phishing emails remain at a high level. Compared to the previous year, they have even increased.

Two out of three users open phishing emails, while almost every third user clicks on links, attachments, or other harmful content. 58 percent of these users, in turn, also interact with the content and, for example, enter personal data in fake login screens.

Reporting rates: The early bird gets phishing emails



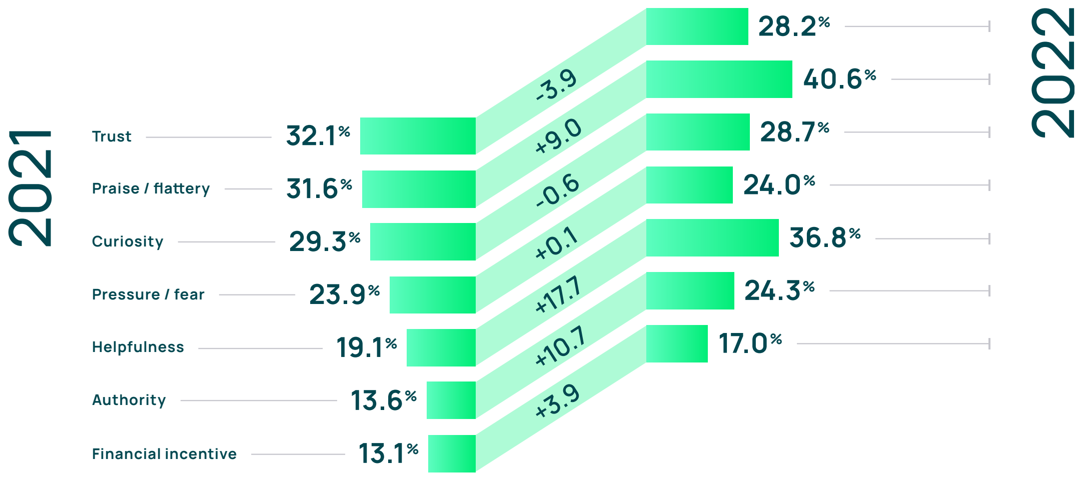
Most phishing attempts are noticed by employees on Monday mornings. On Mondays, users reported the most suspicious emails between 7:00 and 9:00 a.m. Over the course of the week, the number of reported phishing emails remains highest in the morning – so particular caution is required, especially before or during your morning coffee. But that does not mean that you can generally feel safe after the lunch break: The fluctuation on Thursday shows that even inattentive behavior during the day can be dangerous.



Heat map based on real phishing emails reported via the SoSafe phishing report button.

The view of the entire year confirms the findings from the weekly analyses – in general, most phishing emails are recognized by employees before 9:00 a.m. At the end of the year, it is also clear: Cybercriminals like to take advantage of peak sales times in retail. Significantly more phishing attempts are reported during the months of October to December than in the middle of the year. Black Friday, Cyber Monday, and the Christmas holidays, for example, fall during this period.

Positive emotions lead to false conclusions



In phishing emails, cybercriminals use various psychological tactics to trick potential victims into revealing data or opening compromised files. Recipients are most susceptible to emotions with positive connotations: As was the case last year, the most successful tactics include helpfulness, praise/flattery, curiosity, and trust. With praise and supposed willingness to help, cyber criminals tempt more than a third of recipients to click on malicious content.

The high increase in click rates in the areas of helpfulness and authority shows parallels to the new normal in the context of the pandemic and hybrid working models. Due to increased communication via digital channels and the elimination of personal encounters, it is now part of everyday life to be asked for help by colleagues via email collaboration tools. A quick response is usually expected. This may lead to thoughtless action – especially when the request comes from an authority figure. Cybercriminals also know this and use exactly these channels for their attacks.

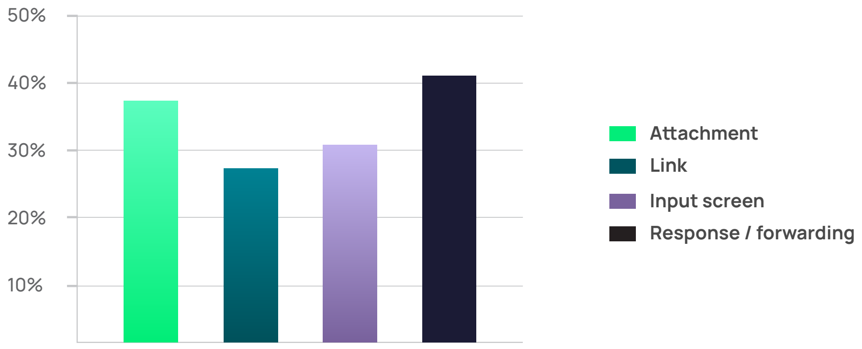
On the positive side, people have become more skeptical when it comes to seemingly trustworthy content, such as fake newsletters from well-known organizations or alleged delivery information from shipping providers. Here are the numbers compared to last year. In general, the fewest recipients are attracted to phishing with financial incentives. It is reasonable to believe that this topic is well known because it has been used for a long time.

The top 10 phishing topics

1	66%	Authority	The following task must be completed: Distribution of documents and task review
2	66%	Helpfulness; curiosity	You have 2 references
3	57%	Authority; pressure/anxiety	Important: CORONAVIRUS update
4	51%	Authority; curiosity	General information: new wage accounting software
5	50%	Pressure/anxiety	Missed meeting
6	49%	Curiosity; trust	Newsletter for September 2021
7	46%	Authority; curiosity	Report form the board
8	46%	Authority	[EXT] Update organization instruction for mobile services
9	42%	Curiosity	Your scanned form
10	41%	Trust; pressure/anxiety	Your Office 365 password expires today

Which subject lines induce recipients to click on a phishing email? This evaluation also shows that the falsification of authority and the exploitation of human helpfulness are especially effective when an element of curiosity is added. However, the reference to new, hybrid working models (1st place and 5th place) and COVID-19 (3rd place) in subject lines breaks with the typical pattern. In this context, the onset of negative emotions such as pressure and fear leads to particularly high opening and click rates. The insecurity of the general public caused by the pandemic apparently still plays into the hands of cybercriminals. A clear sign for those responsible for security: With hybrid working models in particular, employees should be given the opportunity to train their behavior in dealing with cyber risks in order to be able to protect themselves from the dangers.

Suspicious formats or typos: These technical vectors generate the most clicks



Cyber criminals not only try to gain access to sensitive information and data with emotional, psychologically effective content, but also manage to fool their victims by using technical changes and tricks within the phishing messages themselves.

The most dangerous for organizations are phishing emails that impersonate an email conversation. About 40 percent of all employees click on these supposed follow-up emails. Also, attachments do not seem to be perceived as harmful – more than one in three employees click on these.

If cybercriminals manipulate sender addresses, an equally dangerous picture emerges

23,6% **Typo squatting**
An inconspicuous spelling mistake is built into a web address.

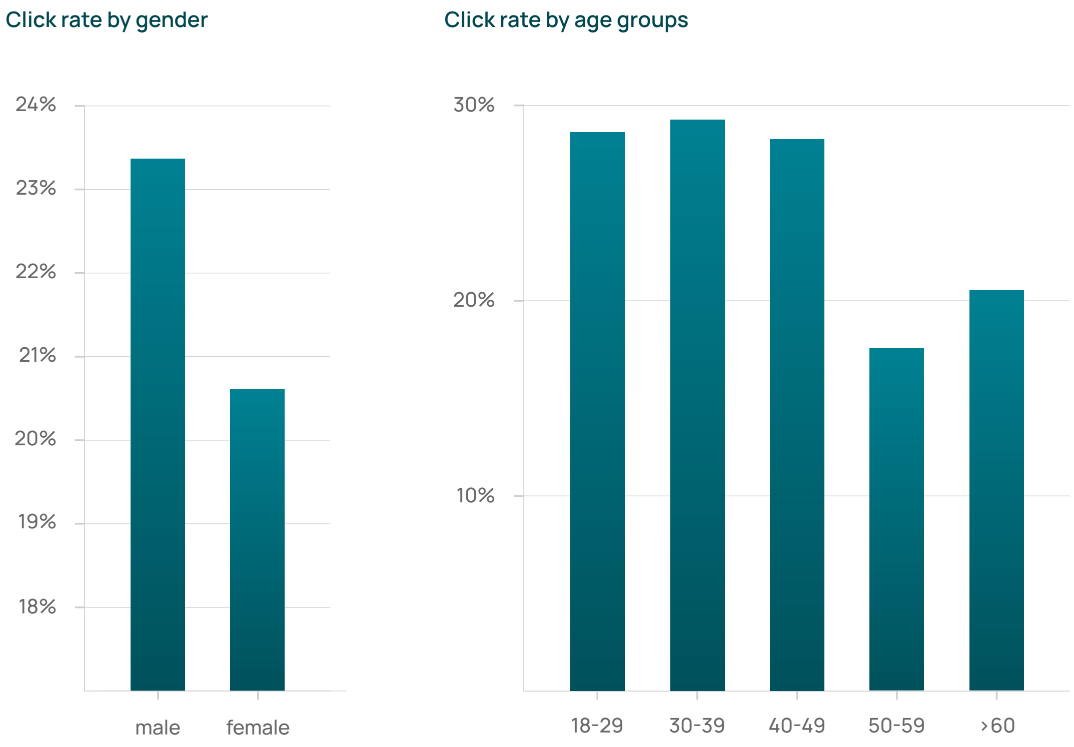
31,2% **Email address spoofing**
The sender in the email header is overlaid.

31,3% **Subdomain squatting**
A fictitious sub-domain is placed in front of an inconspicuous top-level domain.

19,8% **Domain squatting**
The fictitious domain closely resembles the impersonated domain.

3.2 Differences between groups of people

The annual "Phish-test" study on general phishing awareness, conducted by SoSafe and Botfrei, provides demographic insights into the click behavior of users. In 2021, over 1,350 users took part, and within a week received three phishing emails classified as moderate in the simulation, which had to be identified.



With an average click rate of 23 percent across all demographic groups, it shows that citizens should be made even more aware of how to deal with cyber threats.

As in the previous year, despite the only moderate complexity of the phishing mails, it was mainly male participants who interacted with the content – almost every fourth male clicked. In contrast, only every fifth female clicked.

An interesting picture also emerges when looking at age cohorts: The younger participants between the ages of 18 and 49 clicked more frequently, at a rate of 28.6 percent, than those over 50, with an average of only 19 percent. As in previous years, this shows that "digital natives" perhaps are a little more inexperienced in the digital space.

+24%

Particularly exciting: For people who rate their level of knowledge about information security as low, the average click rate is 24 percent higher than for people who rate it as high. This gives reason for hope: If the groups of people are aware of knowledge gaps, they can actively fill them in – and thus protect themselves from cyberattacks.

04 The "Behavioral Security Model"

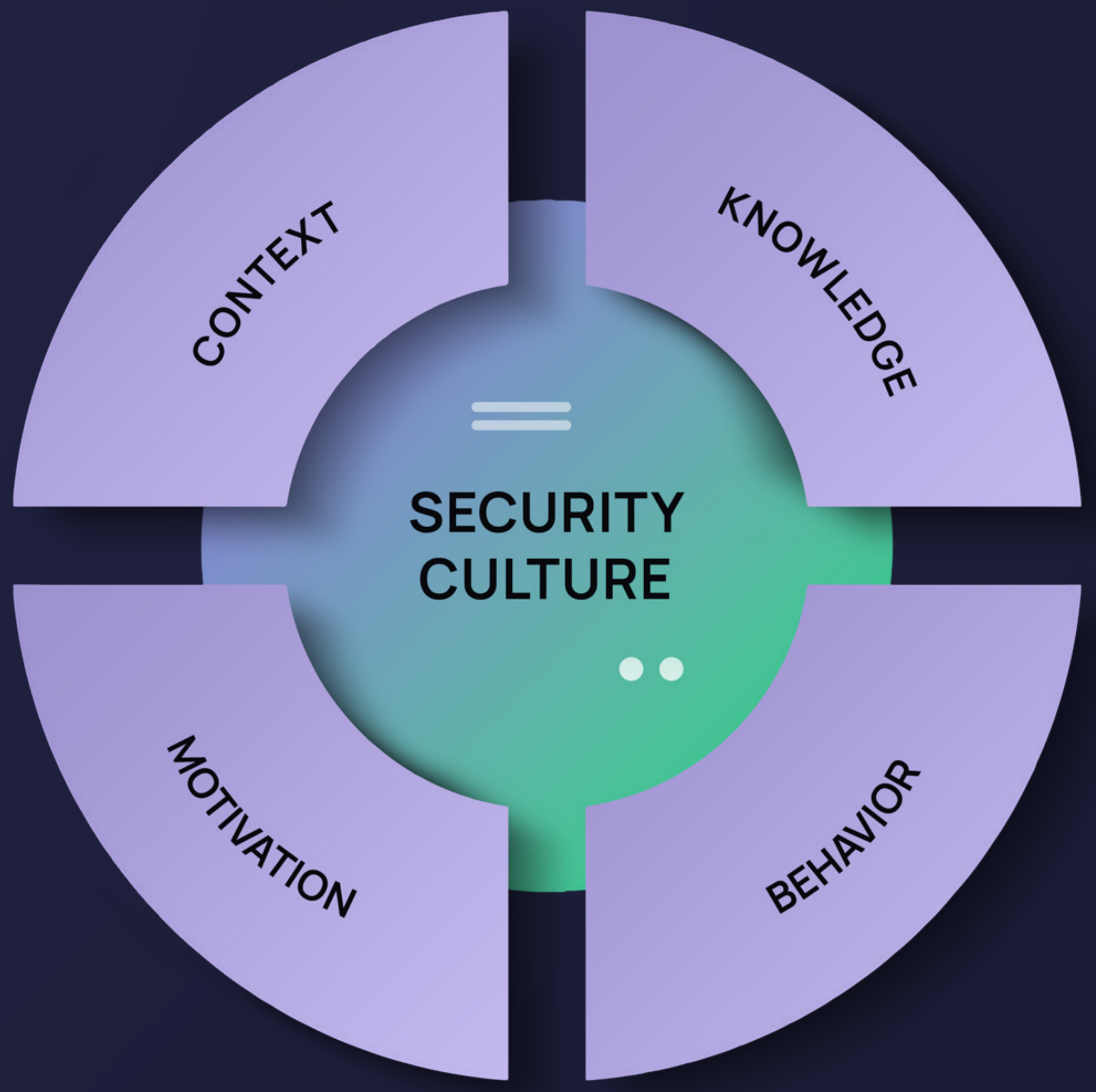
Comprehensive building of a security culture

The fact that the majority of cyberattacks start with the human factor is easy to explain: Attacks happen in any organization – and always in a similar way. It is irrelevant how complex the infrastructure of an organization is. Employees are the universal tools for criminals to access internal systems because they can be emotionally manipulated.

At the same time, humans also play a central role in defending against cyberattacks. Alert employees who spot a phishing email can help prevent serious ransomware incidents. The right behavior at the right time, therefore, can save companies from considerable expenses. Enabling and promoting this, therefore, is the goal of a sustainable security culture. That this also can have a clear ROI from a risk perspective is also shown by the figures on the SoSafe Awareness Platform. Systemic awareness-raising measures can reduce the risk of a successful phishing attack by up to 90 percent.

In the "new normal" of a hybrid working world, employees face enormous challenges. Collaboration tools and new forms of communication are increasingly vying for our attention. An increasingly networked world of work leads to an increased volume of information. More complex attack tactics also bring with them the need for a higher digital skill level. Attempts to meet this challenge with methods of pure knowledge transfer or by confirming policies do not only lead to frustration on all sides, but often even to phenomena such as security fatigue (employees being overwhelmed by too many security issues).

A modern security culture tries to meet people where they are and needs to meet them with comprehensive understanding. The aim is not to impart pure knowledge or to tick a checkbox. Instead, it should support and motivate them to look at their behavior and practice safe routines. The "Behavioral Security Model" presented here has four dimensions, all of which should be considered equally for modern security awareness and used as levels of intervention.

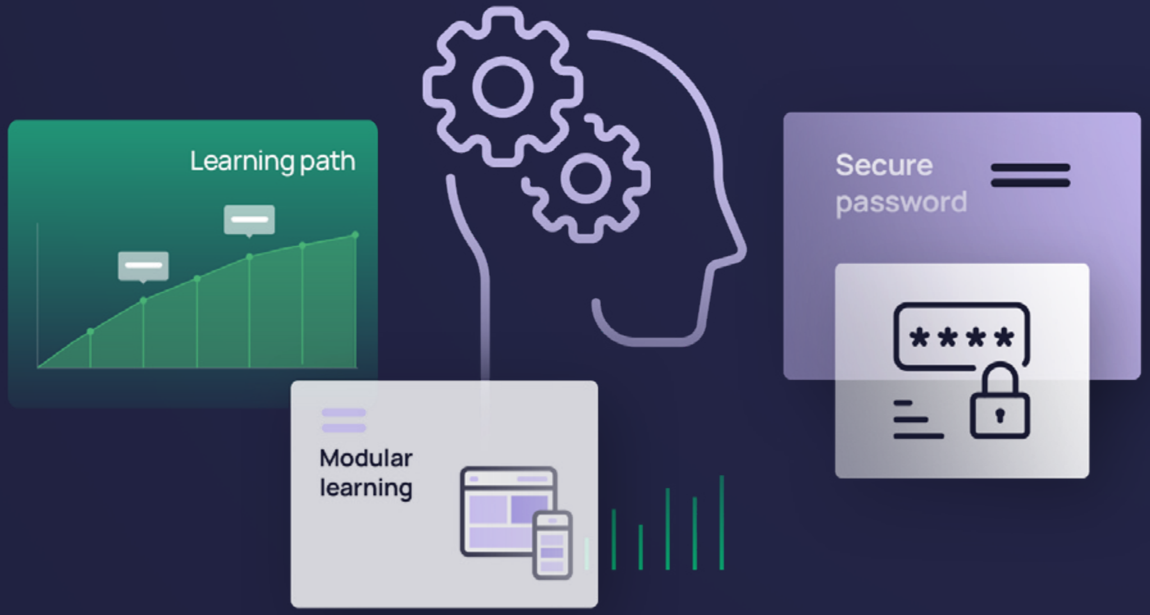


→ Context

Not every person within an organization has the same starting point: The individual role has a significant influence on how cyber risks develop. For example, employees in managerial positions, people with a company cell phone, people with certain access rights and tools, or employees in the finance department are exposed to greater danger because cybercriminals exploit their position for targeted attacks. The industry of a company also has an influence on the risk (also see "Overview of sectors", page 27).

Therefore, organizations should create a context that generally favors safe behavior. For example, if there are no established reporting chains or clear contact persons for possible incidents in the company, the corresponding reporting behavior is made very difficult. On the other hand, if employees can report suspicious emails quickly and easily, for example by using a Phishing Report Button, this makes it much easier to act accordingly. Based on the SoSafe platform data, up to 70 percent of employees can be actively involved in defense after the introduction of the button. With this collective awareness, numerous potentially dangerous situations can be avoided.

At the same time, context is to be understood in another way. The personal context of employees influences the individual learning experience. For example, not all employees need information on how to use a company cell phone safely if they do not use one at all. Therefore, learning experiences should be tailored to the employees: Personalized learning paths, for example, go into more detail about the individual situation of the learners and make what they have learned tangible and relevant.

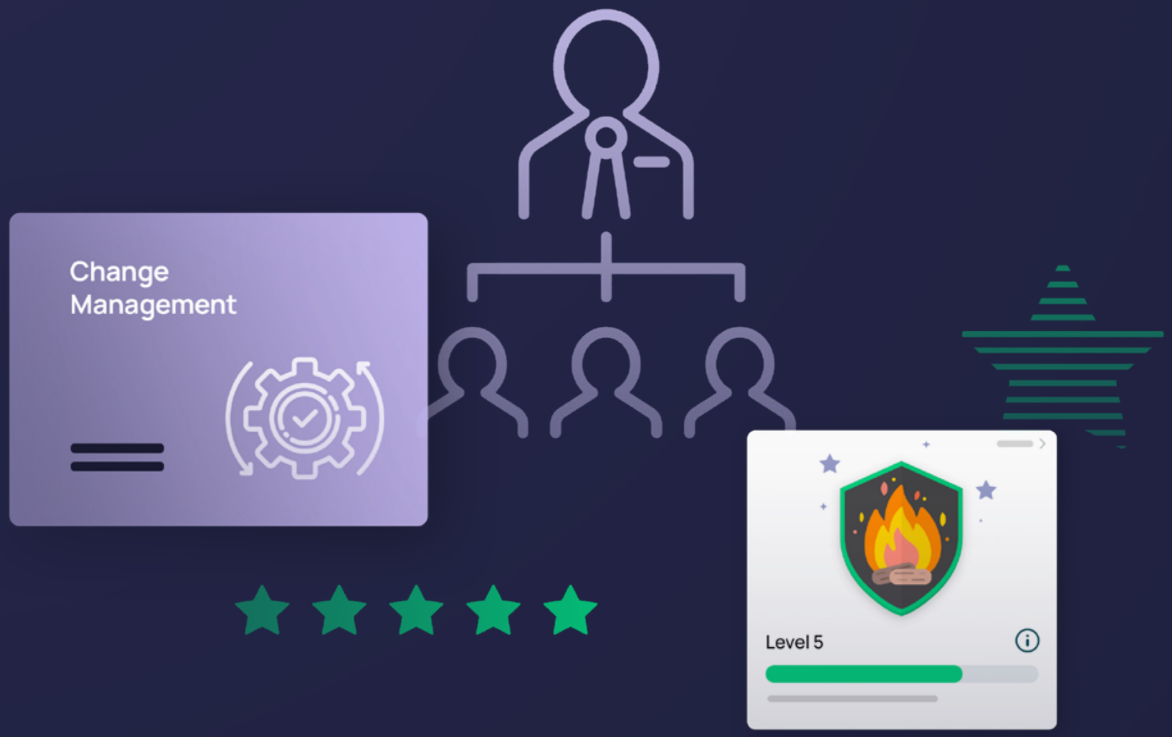


→ Knowledge

In order to show a certain behavior, knowledge about the correct behavior must first be presented. The first step towards a strong security culture, therefore, has traditionally always been to impart knowledge – for example on how to create secure passwords or how to recognize phishing emails. In the past, however, knowledge was often conveyed linearly and in "high doses". Long videos or seminars were followed by a simple knowledge test to demonstrate learning.

However, it has long been known that linear and massed learning only to a limited extent contribute to long-term knowledge. As early as the 1950s, the German psychologist Hermann Ebbinghaus showed that schoolchildren had forgotten most of the subject matter after just a few days. Ebbinghaus also found that stable memory engrams (the "imprints" of knowledge in the brain) form better when knowledge is shared and actively repeated.

In order to impart cybersecurity knowledge, organizations should therefore resort to approaches based on learning psychology instead of pure "frontal sound reinforcement". Highly modular training and constant nudges to learn, or "nudging", flatten the curve of forgetfulness and thus minimize human risks in the long term. Results from the SoSafe Awareness Platform show that nudging continuously increases engagement by 30 percent and even up to 90 percent in the introductory phase. This is how employees memorize knowledge effectively and sustainably.



→ Motivation

Safe behavior is always influenced by certain factors. This can be easily illustrated using the everyday example of road traffic: Although we know that we are not allowed to drive 80 mph in the city center, we also need to understand why, in order to actually comply with the regulations. In a strong security culture, employees not only know about cyber risks and understand how they can proactively counteract them in their individual context. Such a culture is characterized by the fact that it favors the motivation of those involved and emphasizes the relevance of the measures.

Management is responsible for strengthening the motivation and security culture and includes the adaptation of processes under aspects of information security. This makes it a matter of change management. Recent studies show that the commitment of managers plays a decisive role. If managers involve employees at an early stage and communicate directly with them, they are much more willing to change their behavior and even to drive development themselves, with positive effects on minimizing human risks. The use of gamification also has clear effects in this context: With it, the activation rate in security awareness training increases by up to 50 percent.

→ Behavior

Ultimately, the human risk in an organization depends on how well employees put what they have learned into practice and cultivate safe ideas. Context, knowledge, and motivation play a role. What is decisive, however, is to what degree safe behavior becomes "flesh and blood".

In order to train safe behavior, it is important to impart necessary knowledge in a motivating manner – for example with the help of gamification. Behavioral psychology also shows: Continuous, incidental learning in particular strengthens habits. The behavior learned is repeatedly put to the test by means of ongoing attack simulations, for example, and called into the active memory of the employees. Results from the SoSafe Awareness Platform show that phishing click-through rates stay low and report rates stay high over time.

Why investing in behavioral security pays off

By enabling and promoting safe behavior, organizations minimize risks effectively and sustainably – and thereby save costs in the long term. After all, the investment in security awareness should be seen as an investment in the security of the organization and calculated against the potential costs in the event of damage. In the event of a successful cyberattack, a company with a turnover of 10 billion euros, for example, will have to pay 106 million euros. However, through systematic awareness measures, click rates on phishing emails are drastically reduced. If the click rate is reduced by 70 percent, the expected damage is reduced to 32 million euros. As a result, organizations investing in security awareness and building their security culture can expect long-term savings.

Marisa Fagan, Atlassian

> “Every awareness program should be based on behavioral science techniques.”

Marisa Fagan has a background in information security and community building, and has been working in the tech and security industry for more than 10 years. She previously worked at Salesforce and Synopsys, and currently is Head of Trust Culture & Training at Atlassian where she enables employees to make educated security decisions.

Your role is Head of Trust Culture and Training, can you explain the underlying philosophy of highlighting “Culture” and “Training” together?

The mission of our program is to empower our employees to work securely. Inspired by the model for behavior by BJ Fogg, we define empowerment as the alignment of ability, motivation, and prompts. It’s not enough to roll out a training that delivers awareness as a part of ability. You need to influence people’s motivations as well, and you can do that by influencing company culture.

Security awareness and training has experienced a fundamental shift in paradigms over the past five years. What are the key aspects of that change from your perspective?

The security awareness space has matured dramatically in the past 5 years. More companies are investing in full-time security teams. Several start-ups have appeared in the space focusing on providing data visibility to these teams. They now focus on measuring security events and behaviors, attributing them to people, and assigning risk levels to the data. They can take a step back and look at “people risk” from an organizational level and provide executives with a view of that risk as well. This shift in perspective will continue as we begin empowering employees by presenting to them their own data and story. With this concrete knowledge, they can then modify their behavior regarding risk levels accordingly.

What’s the difference between training staff by just “deploying information” and creating a sustainable trust and security culture? What’s the secret ingredient for building a strong security culture?

Every person is different, and you need a variety of techniques to meet people where they are. There’s a type of person that values brevity and another that may need simple training to interact with accessibility tools. So, there’s definitely still a place for the classic staff training courses, but you need many other strategies as well. The more choices you can provide, the more people will buy into what you’re asking of them. The secret ingredient to influencing company culture is a healthy mix to create an “ambience of security” that covers the whole company year-round. In our case, we have a full-time team of 4 to provide this kind of coverage for our company and offer online training, a blog, a newsletter, Slack channels, a Security AwarenessMonth event, a calendar of year-round monthly events, and a Security Champions community.

From your perspective, what role does behavioral science play in the context of awareness and trust culture?

Behavioral science techniques are the fundamental trade tools that every program should be based on. We use the Fogg Behavior Model as an exercise to identify what problems we have when we are not seeing the outcomes, we are looking for in our training efforts. Once we understand whether we want to improve on the ability, the motivation, or the prompt aspect, we choose one of many different techniques rooted in behavioral science to make progress and “move the needle”. For example, we publish a leaderboard by team to show which team has finished the training the fastest. It’s a technique based on social psychology called “social comparison” that makes that useful. Even with no prior motivation, people will more readily take a training when they see their peers have completed one.

You’ve previously spoken about security champion programs and motivating people to engage in security. How do you encourage staff to go out of their way to improve resilience?

I think people in this space forget that they are also a part of the target audience. Are you bought in and do you practice security the way you’re asking others to do? The first step to engaging people in security practices is to ensure that the asks are reasonable. Solve as much of the problem as can be solved using technology and ask people to act as a last resort. Then the most important step is communication. Present all the facts and make your case. If you can draw a straight line between the request and the good reason behind it, you will get people to buy-in if they have the ability to do so. For example, using password managers is a low participation activity. We communicate to people that the reason for using a password manager is because “according to a study from Google in 2019, 65% of people use the same password for multiple accounts” and “85% of breaches last year involved stolen passwords.” It communicates this is a high-risk habit and lets them make the decision. Communication and transparency don’t convince everyone but giving people all the information and trusting them to make the right choices is a big part of our culture.

Is there also a change in metrics you are now focusing on?

We have changed by combining all small signals into one risk metric. We have a metric for organizational employee risk that is comprised of weighted values for several inputs including phishing credentials stolen, phishing reporting, training completion, and password manager adoption. By using multiple inputs, we can paint a more nuanced picture of the risk at the organization level. Our plan is to keep adding more “behaviors” to this weighted list of small signals and to keep refining the measurement of how empowered our employees are to work securely

Do you see new challenges arising from the “new normal” of hybrid first and working from home?

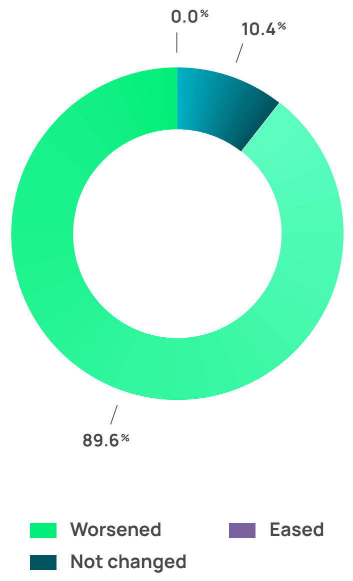
Definitely! We’ve had to streamline our training calendar. People have much less time now. Courses are now limited to 60 minutes whereas before we would have pulled everyone into a room together for a 3-day summit at HQ. We focus more now on setting the tone from the start with new hire trainings both as scheduled presentations on day one and takeaway self-service resources that new hires can refer to later as they settle into their new role.

05 Security officers confirm: Cyber risks are increasing – and cyber resilience is becoming more important

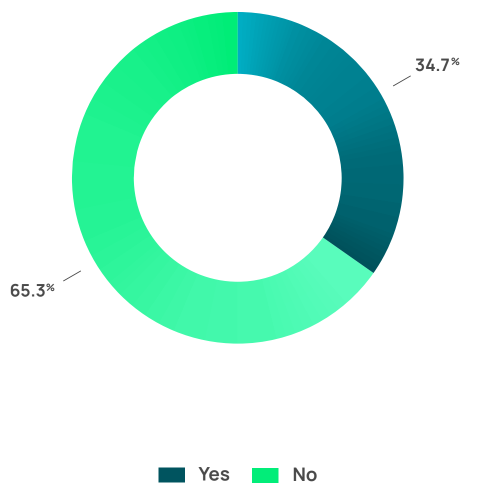
A professional cybercrime industry and increasingly successful social engineering tactics – how do organizations react to the increased challenges? For our Human Risk Review, we ask IT and cyber security officers every year about how they perceive the cyberthreat situation and what plans they have with regard to awareness in their organization. This year, 251 experts shared their experiences with us.

The perception of the cyberthreat landscape in 2021

Recap of 2021: How did you perceive the cyber threat situation?



Our company (or one of our service providers) has itself experienced a cyberattack.

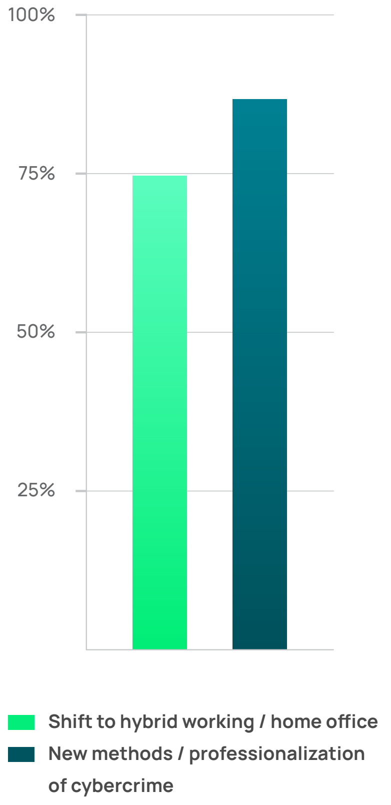


9 out of 10 respondents agree: The cyberthreat landscape has intensified in 2021. More than a third of those surveyed have even experienced a cyberattack within their own organization or via a service provider. The high numbers show that hardly any organization feels safe from cyberattacks. But what drivers do the experts surveyed see for this development?

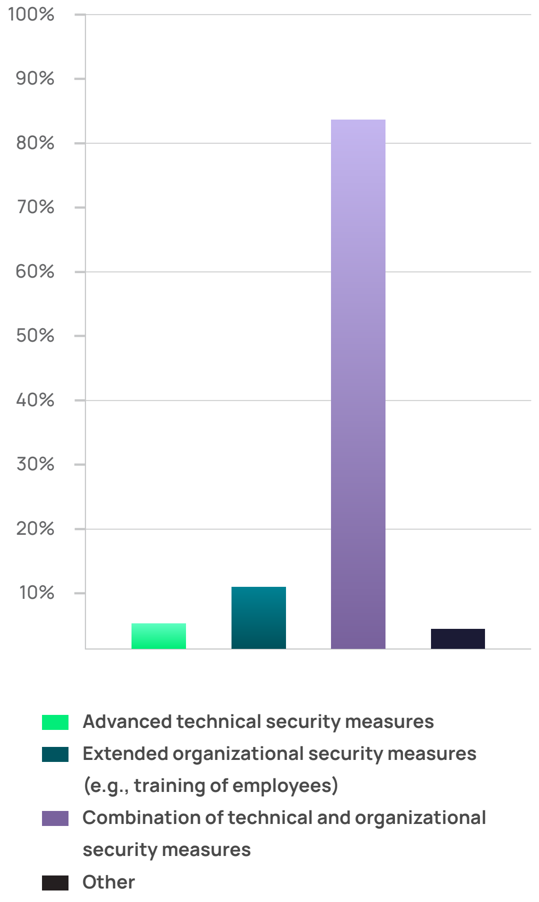
Three quarters of the IT and cyber security officers confirm that the increase in mobile work and home office models offer new points of attack. More than 85 percent see the cause of the heightened threat situation in the professionalization of cybercrime.

Although the respondents agree that working from home offers new areas of attack, they are also confident that various security measures make working from home more secure.

These drivers have contributed to the aggravated cyberthreat situation.



What would make hybrid work / home office safer?



The answers show that the combination of technical and organizational security measures, such as awareness training, is primarily considered to be conducive to a safer working environment when working remotely.

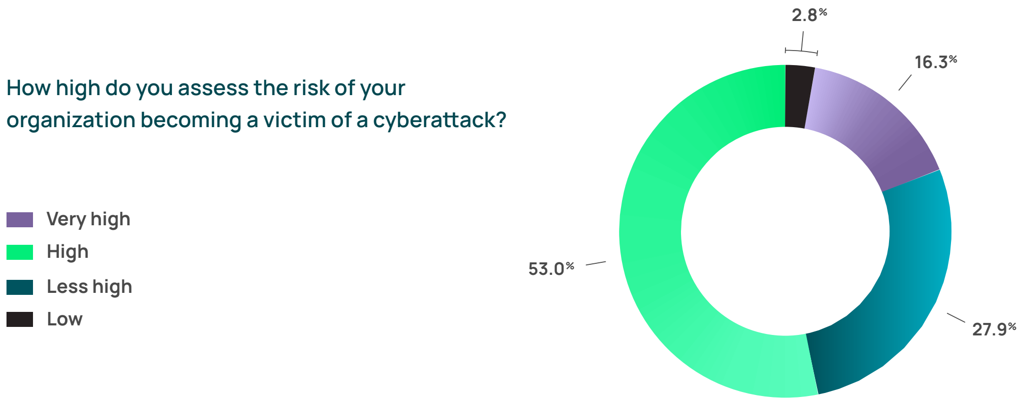
Human risks in your own organization

The assessments of the importance of security awareness in organizations show a clear trend: 9 out of 10 respondents recognize security awareness as an important or even very important topic – and the more important the topic is within an organization, the higher the respondents rate the awareness level of the employees on average. This confirms that the awareness of cyber threats grows from a security culture in which the topic is clearly placed accordingly.

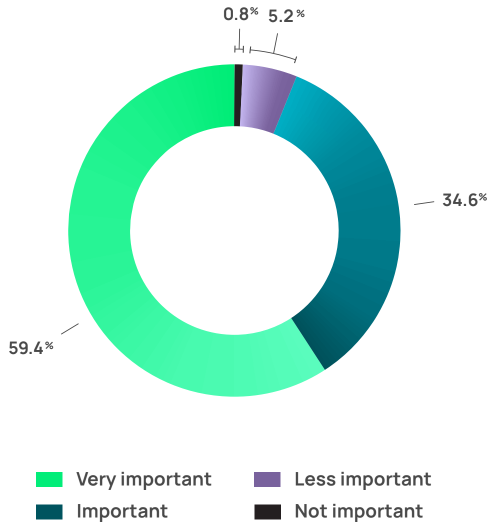
Nevertheless, a clear "security awareness gap" emerges when looking at all the responses on the assessment of human risks: In 40 percent of the organizations that consider the topic important or very important, the awareness level of employees is still rated as low or very low. This shows that there is currently a need for action in many companies.

In fact, more than two-thirds of respondents rate the risk of a cyberattack within their organization as high or very high. Most IT managers therefore seem to be well aware of the connection between human risks and the threat to their own organization.

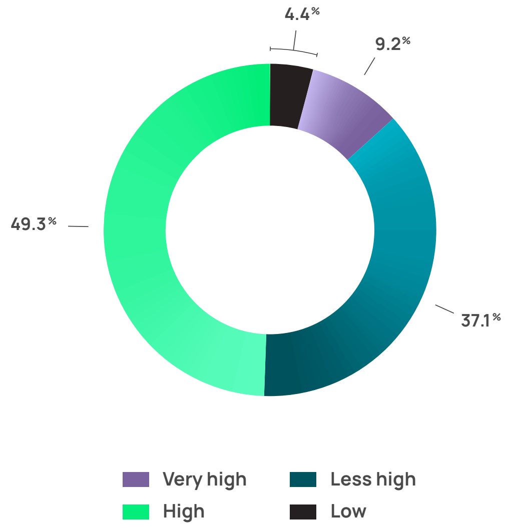
How high do you assess the risk of your organization becoming a victim of a cyberattack?



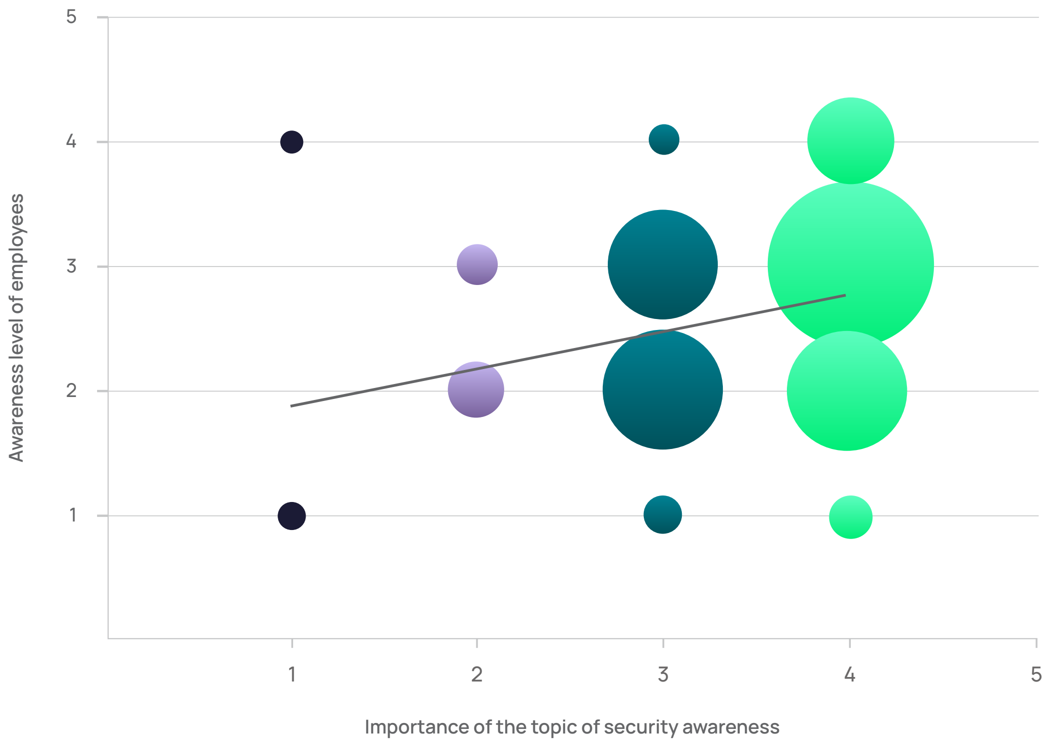
How important is the security awareness topic in your organization?



How high do you rate employee awareness in your organization?



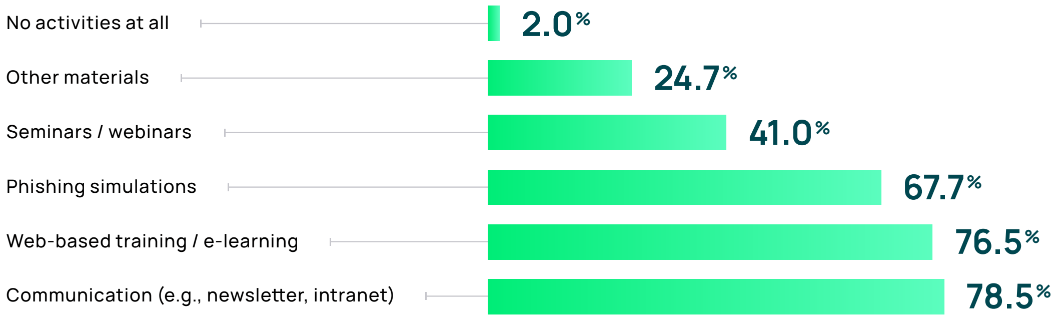
Correlation between the importance of security awareness and the awareness level of employees



Awareness measures in one's own business

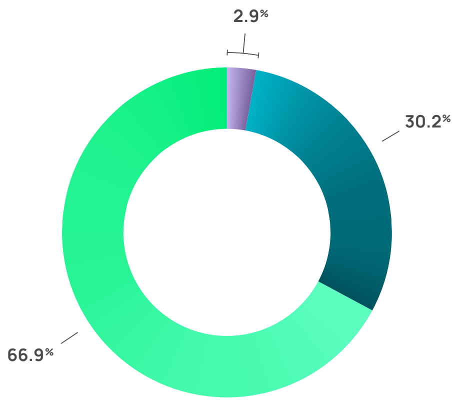
This is also reflected in the use of awareness measures in their own organization. A year-on-year comparison shows that organizations have caught up! While the majority still rely primarily on internal communication measures, the use of web-based training and phishing simulations has increased significantly and is now the standard.

What measures are used to increase awareness among employees in your organization?



In addition, two out of three respondents plan to further expand measures to increase cyber security awareness among employees. Particularly encouraging: Organizations that stated in the survey that the topic of security awareness is currently less important or not important, state more frequently on average that they want to expand measures to protect against cyber risks in 2022. Companies now understand that the human factor plays a crucial role in a comprehensive security strategy.

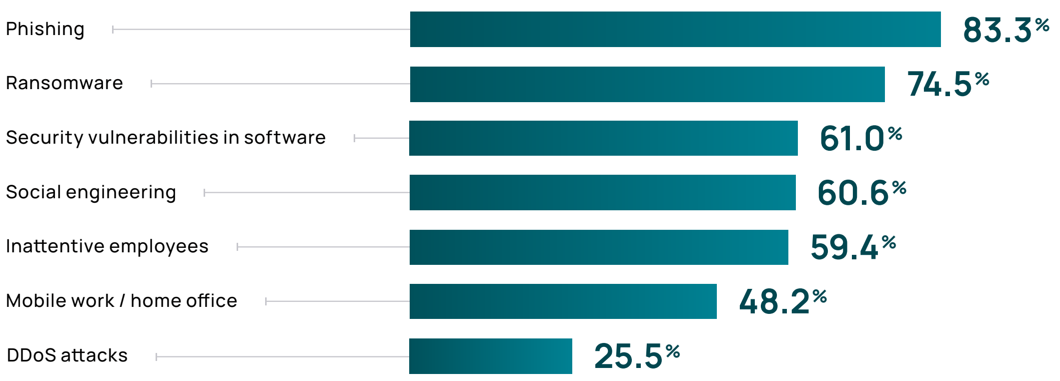
What are your plans in terms of measures to raise employee awareness in 2022?



A colorful bouquet of attack vectors

When it comes to the question of which attack vectors will be used most frequently in the future, respondents commented that the most outstanding are the ones that affect the human factor. Above all, phishing and ransomware are perceived as future risk factors. DDoS attacks seem to be less of a focus for the experts. Nevertheless, new record attacks are always being recorded, for example the largest DDoS attack of all time on Azure in November 2021 according to Microsoft.[57] Software security vulnerabilities are also seen as dangerous - the vector presumably remains anchored in the minds of the respondents, not least due to the large Log4j gap.

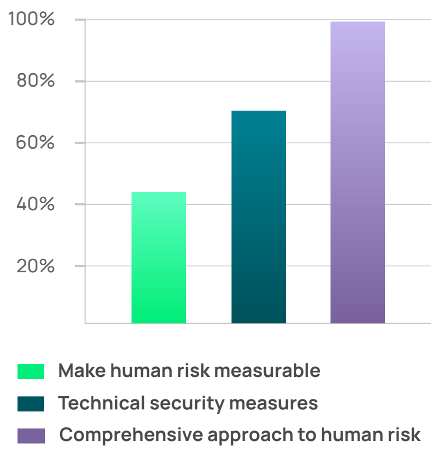
Which attack vectors will be used most in 2022?



Where do we go from here? The outlook for 2022

Almost unanimously, 99.2 percent of all respondents state that security awareness training and strengthening their own security culture will become more important in 2022. Furthermore, in addition to the further expansion of existing technical security measures, the holistic consideration of the human factor (see Chapter 4) is also important to the respondents.

Which cyber security topics will become more important in 2022?



[57] ZDNet (2022). Microsoft: Here's how we stopped the biggest ever DDoS attack.

INFOBOX

→ New expert opinion confirms doubts about GDPR compliance of US software providers

Following the Schrems rulings of recent years, a new expert opinion by US lawyer Stephen Vladeck now also casts doubt on the GDPR-compliant data processing by US as well as their EU subsidiaries. The opinion takes into consideration the current state of US surveillance law and draws conclusions about the ability of US companies to comply with European data protection standards. In fact, it is not enough to process data on EU servers to prevent access by authorities or intelligence agencies from other EU countries.

This new opinion provides clarity to organizations and confirms that they should play it safe when choosing their software providers. To fully protect sensitive employee data – and protect themselves from regulatory fines and employee complaints or lawsuits – organizations should choose vendors that:

- Process data exclusively within the EU, and
- also have their headquarters within the EU.

This applies in particular to security awareness providers. After all, phishing simulations sometimes involve the processing of sensitive data that must be protected at all costs.

Dr. Judith Nink, Director Legal & Risk at SoSafe:
"Even almost two years after Schrems-II, there is no clear and legally secure solution for the use of providers accessing EU citizens' data from outside the EU. In addition to the Damocles sword of fines and the obligation to shut down providers, companies continue to face the challenge of processing their employees' data in a (legally) secure and trustworthy manner. The safe way, therefore, is to choose an EU-based provider processing data within the EU."

06 Outlook & Recommended Actions

New processes, new threats, new channels: Hybrid ways of working call for new awareness approaches

The world has changed, cybercrime is becoming more professional - and information security must now also undergo an evolution. Security awareness measures must adapt to hybrid ways of working and new communication channels. At the same time, it is necessary to respond to the intensified threat situation and anticipate new types of attacks that exploit remote work. This transition does not just involve constantly updating learning content. Modern awareness measures should also make employees responsible for protecting their organization, especially on the various new channels - in addition to classic email communication, for example, also via telephone or collaboration tools, and with the help of approaches based on behavioral science such as gamification and nudging. This is the only way to reach employees in a hybrid working environment and motivate them to actively protect themselves against online threats.

Security Awareness belongs at the board level: Involve your management in the topic of information security

The current cybercrime situation is increasingly being discussed on executive floors. There is no denying the relevance of this topic for the boardroom: Cyberattacks are often consequential for short- and long-term business success. Therefore, actively involving your management in the topic of security awareness is crucial. Regulatory frameworks and standards provide both national and global legal obligations and can help in decision-making. It is also important to support the need for action with success metrics and KPIs on the economic effects of the awareness measures instead of merely referring to security key figures such as click rates. Use tools that continuously measure the ROI of the measures and thus clearly demonstrate the value of long-term security strategies.

Safety is a matter of culture: Establish the right behaviors and views among employees

Your security measures are only as good as the security culture in your organization. If employees are not aware of the relevance of information security and awareness measures, their handling of cyber threats will not improve. Strengthen this awareness through internal and ongoing communication and awareness-raising actions, and put prudent behavior at the center of all digital processes.

Take a holistic view of human risk: Get an overview with tools and comprehensive metrics

Security risks inevitably arise in companies – even due to human behavior. Get an overview of these risks with the right tools so that you can react quickly and take preventive measures in the event of an emergency. According to Gartner, as early as 2025, almost two thirds of all organizations will use cyber risks as a factor in deciding with whom to enter into a business relationship. Minimizing human risks will thus become a decisive factor in the success of companies, and one that is in your own hands. Organizations should approach this challenge holistically: To sustainably reduce risks, it is important to collect metrics at the various levels of the "Behavioral Security Model" and to take appropriate awareness measures that positively influence employees' knowledge, motivation, context, and behavior.

[58] Gartner (2021). The Top 8 Cybersecurity Predictions for 2021-2022.

About SoSafe

SoSafe empowers organizations to scale agile awareness programs that build a security culture. Our dynamic upskilling platform fuses behavioral science, smart algorithms, and a human-centered approach to empower every employee to be part of their organization's human firewall. Beyond building secure habits among employees, you can understand exactly where vulnerabilities lie with contextual data, proactively respond, and measure the ROI of your awareness programs.

Employees receive smart attack simulations and personalized micro-learning experiences within their daily work environment. Curated content delivered with a level of gamification makes the trainings engaging, informative, and effective. Our self-learning systems react to personal risk scores, continuously delivering tailored trainings to each employee. This continuous process drives secure behavior at scale.

The SoSafe difference is how easy it is to deploy, manage, and scale our GDPR-compliant solution, saving you time and resources. Organizations can leverage our simple self-serve model or opt fordone-for-you implementation and service from our team of experts.

TEACH —

Engaging Micro-Learning

A continuous and curated security awareness platform that employees love: Strengthen your resilience to online and offline threats, and fulfill compliance obligations with engaging and impactful learning experiences across channels with ease to build long-lasting, secure habits.

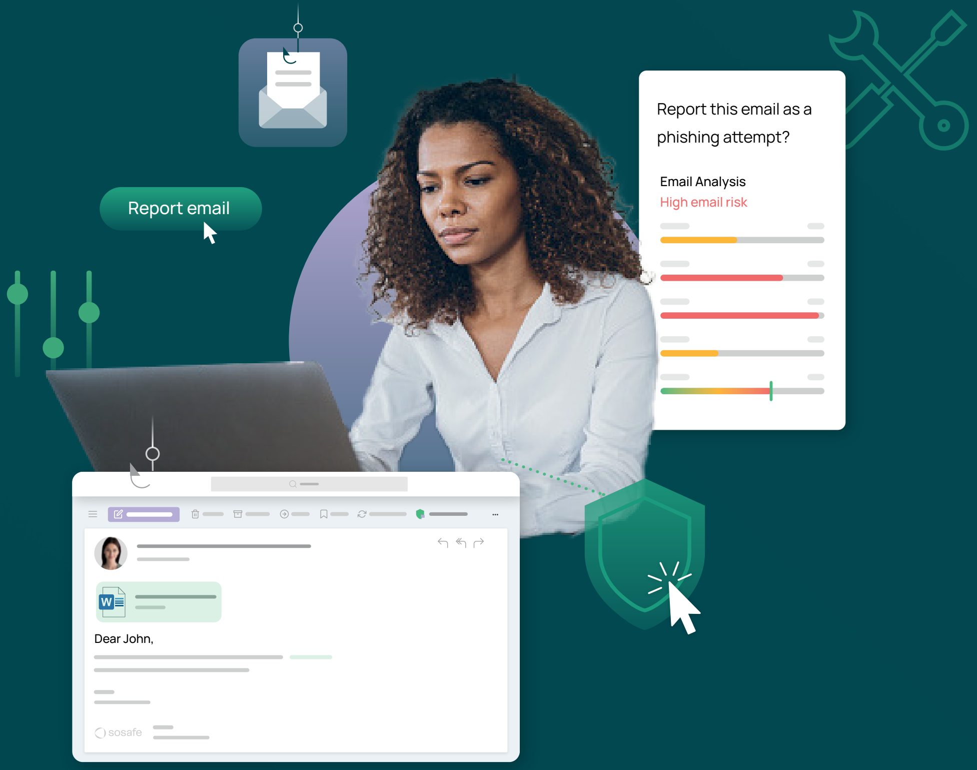
- → Fun, story-driven and effective gamified learning designed to engage
- → Curated and guided content library readily scalable for your growth
- → Customization and branding engines to fit your organization

TRANSFER ——

Smart Attack Simulations

Behavioral science-based Smart Attack Simulations that make secure habits stick: Help employees learn to spot attacks using automated spear phishing simulations – and effectively reduce risk and crucial threat detection time!

- → Personalized and realistic threat simulations
- → Context-based learning walkthroughs delivering fresh learning experiences
- → One-click reporting of simulated and real threats via Phishing Report Button



ACT ——

Strategic Risk Monitoring

Understand exactly where vulnerabilities lie and proactively respond: Use advanced analytics to quantify and manage your organization's risk, track vulnerabilities, and make data-informed decisions!

- → Contextual data with technical and psychological KPIs
- → Actionable insights on key areas of improvement
- → Dashboard to track KPIs, compliance (e.g., ISO/IEC-27001) and platform ROI

sosafe

SoSafe GmbH
Ehrenfeldguertel 76
50823 Cologne, Germany

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

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.