sosafe

Cybercrime Trends 2023

The latest threats and security best practices

Contents

Cybercriminals are leading the innovation race

As technology becomes more advanced and continues democratizing cybercrime, it's more important than ever to be prepared to prevent potential attacks. Artificial intelligence and all its innovative applications, cyberattacks exploiting the world's increasing fragmentation, digital supply chain attacks with large-scale reach, ransomware-as-a-service, or multi-channel phishing: Cybercriminals are always innovating and expanding their repertoire of tactics. When your technical precautions fail, remaining vigilant and having a strong security culture makes all the difference in protecting your organization.

Staying ahead of the evolving threat landscape is key to strengthening resilience to security risks. Here are the eight latest trends in cybercrime for 2023 and helpful tips for companies to stay secure.

01

The rise of artificial intelligence: A driver for cybercriminals' innovation

Artificial intelligence (AI) is gradually permeating into our everyday lives, and cybercriminals didn't hesitate to take advantage of this societal advance: They quickly realized that it can be used for social engineering attacks as a prime opportunity to maximize their profits.

Deepfake technologies, and voice cloning specifically, were one of the first AI methods hackers employed in their vishing (voice phishing) attacks to successfully dupe employees into believing they were speaking with members of their own organizations. Back in 2019, criminals used artificial-intelligence-based software to impersonate an executive of a German company and demanded a fraudulent transfer of €220,000 from his subordinate, the CEO of a UK-based subsidiary of that company.[1] These AI-powered calls can also be used in combination with other tactics. For example, criminals have been reported to call their victims to give them a heads-up about an email they are about to receive so that when the email – that is actually a phishing email – arrives, the victim is not suspicious. This dangerously increases the criminals' success rates since the emails are less likely to be identified as harmful. If that weren't impactful enough, the release of VALL-E this year, a transformer-based text-to-speech model by Microsoft that can generate speech in any voice after only hearing a three-second sample of that voice, is likely to further worsen the current voice cloning threat landscape.[2]

Voice manipulation is, however, only one side of the coin: The alteration of video material has been weaponized by cybercriminals, too. A fake surrender by Ukrainian President Zelenskyy made the rounds in early 2022, illustrating the potential impact this type of AI attack might have – especially if further improved.[3] Similarly, alleged deepfake attacks caused a stir in Germany when the mayor of Berlin joined a video conference with Kyiv's Mayor Vitali Klitschko to discuss the Ukraine War. He spoke for 15 minutes until it was discovered that this was not Vitali Klitschko himself but a "cheapfake" in which manipulated audio was dubbed over existing video. This incident made clear the ruthless extent of video manipulation that imposters attempt – and how easy it still is for them to disguise their plans.[4]

As the quality of deepfakes continues to improve, cybercriminals are likely to conduct more believable and successful social engineering attacks this year. In fact, legal and security experts worry that deepfakes will be misused to erode trust in surveillance videos, body cameras, and other evidence, as well as for cyberbullying, blackmailing, stock manipulation, and the worsening of political instability.[5]

But deepfakes and other AI-based methods, such as automated password-guessing and CAPTCHA-breaking, were just the beginning of a new era. AI is boosting the sophistication and scale of cyberattacks by the minute, and many organizations have just begun to prepare against them. One stark example is the use of generative AI to craft malicious emails that can bypass spam filters. A study conducted in 2021 by a research team at the Government Technology Agency of Singapore discovered that generative AI can create convincing spear phishing emails that are clicked on more often than those created by humans.[6] The tool they used for the study was none other than the predecessor of ChatGPT, which is now publicly available.

In fact, the launch of ChatGPT at the end of last year made cyber security professionals face new challenges, and many researchers are concerned that this type of generative AI solution will democratize cybercrime.[7] With this publicly available and free tool, anyone can generate malicious code and convincing phishing emails with little technical expertise. And ChatGPT has even been reported to craft sophisticated "polymorphic" malware that can shapeshift its way around traditional security mechanisms.[8]

Ransomware attacks are also likely to become more destructive with AI-powered targeting as they will help hackers find new vulnerabilities and victims. And since the ability of AI to mimic human behavior is evolving by the minute, it might soon surpass certain biometric systems or even imitate human activity so that stolen accounts aren't flagged by behavioral security systems.[9]

While security experts also use artificial intelligence for defensive purposes, such as testing code and threat intelligence, there's no way to deny that it has significantly complicated and exacerbated the threat landscape. Only the future will tell who will leverage this technology more effectively: security teams or cybercriminals.

PRACTICAL TIPS

Just like with any new type of cyberattack, the best protection is prevention. Security teams should continue adopting new technical and organizational solutions to keep up with the criminals' pace of innovation. For example, using AI-powered tools for threat intelligence or AI-based breach risk assessments is one way of technically mitigating the risk of attacks.

At the same time, continuously teaching employees about new attack scenarios, raising their awareness, and equipping them with smart support tools to detect attacks will help companies stay ahead of the game.

And the same goes for security teams: Regular training helps them to continuously minimize risks and be able to respond quickly should an issue arise, despite all the measures taken.

[1] The Wall Street Journal (2019). Fraudsters used AI to mimic CEO's voice in unusual cybercrime case.
[2] Metaverse Post (2023). VALL-E: Microsoft's new zero-shot text-to-speech model can duplicate everyone's voice in three seconds.
[3] NPR (2022). Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn.
[4] DW (2022). Vitali Klitschko fake tricks Berlin mayor.
[5] The New York Times (2023). As deepfakes flourish, countries struggle with response.
[6] Wired (2021). AI wrote better phishing emails than humans in a recent test.
[7] VentureBeat (2022). How ChatGPT can turn anyone into a ransomware and malware threat actor.
[8] Gizmodo (2023). ChatGPT is pretty good at writing malware, it turns out.
[9] Techmonitor (2022). How AI will extend the scale and sophistication of cybercrime.

02

Evergreen phishing: Attackers’ weapon of choice

Manipulating their victim's emotions to steal confidential information will continue to be one of the favorite tactics for cybercriminals in 2023. In the last few years, attackers have become experts at influencing human behavior, such as by creating a sense of trust, authority, scarcity, or urgency, making victims click on harmful content and/or disclose sensitive information.

These social engineering tactics like business email compromises and romance scams already generate billions for them, but it doesn't stop attackers from improving their schemes. One of the newest real-life examples is pig butchering scams, where scammers cold-contact people via text messages or social media, dating, and communication platforms. They start with a simple salutation, and if their recipient responds, scammers make the victim believe they found a potential friend. Then, they boast about the considerable amount of money they earned through cryptocurrency investments and convince the victim to become involved. They set up malicious web platforms or impersonate platforms from legitimate institutions – and even let victims make video calls with their new "friend" or allow them to withdraw a small amount of money from the platform for reassurance. In 2022, a 52-year-old San Francisco man was reported to have lost $1 million to a pig butchering scam after being contacted by fraudsters pretending to be a former colleague.[10] This 271,000-word conversation revealed the extent to which cybercriminals use sophisticated social engineering tactics for their malicious goals. In 2023, cybercriminals are expected to exploit people's economic and environmental concerns much further, creating a wide variety of new techniques and schemes.

In our professional lives, these attacks could come in the form of a false profile on LinkedIn, a Zoom meeting invite sent by a hacker impersonating one of your colleagues, a spoofed email containing hidden malware, or a WhatsApp message from an "internal IT manager" asking to grant access to internal networks. Any of these has the potential to put organizations at risk, and they are real-world examples from the cyberthreat landscape in which we live and work today. Marketing automation company Mailchimp has recently been reported to have fallen victim to a social engineering-related data breach – the second attack of the kind that the company suffered in less than a year. The malicious actor launched social engineering attacks on Mailchimp employees and stole their credentials, accessing select Mailchimp accounts after gaining entry to one of the tools used by the company's customer-facing teams.[11] In another dazzling case, the attackers even set up a Zoom call with the victim and then sent a malicious URL in the chat during the call.[12]

As seen in the previous trend, ChatGPT and other generative AI solutions that imitate human behavior have the potential to be one of the most powerful phishing and social engineering tools of the century. For example, writing phishing emails without typos or unique characteristics in style and format that today serve us to differentiate these attacks from legitimate emails will become significantly easier. Cybercriminals will even be able to add variations by using different sets of prompts, such as "make the email look urgent" or "email with a high likelihood of recipients clicking on the link".[13]

With 82 percent of data breaches involving the human element[14], it becomes crucial to stay up to date on the latest developments – and on cybercriminals' innovations – to be prepared for the incalculable amount of social engineering attacks that will land in our inboxes, communication tools, and social platforms in 2023.

PRACTICAL TIPS

In addition to the necessary security precautions like firewalls and ETDR tools, a strong security culture plays an essential role for companies to avoid becoming a victim of a phishing attack.

They should communicate to employees the relevance of information security, how different cyberattacks work, and the importance of notifying their company's information security team about suspicious activities on their devices while motivating them to comply with respective regulations.

The good news is that there are effective ways to do this – from awareness training and learning platforms to attack simulations.

[10] Forbes (2022). How one man lost $1 million to A crypto 'super scam' called pig butchering.
[11] TechCrunch (2023). Mailchimp says it was hacked — again.
[12] ZDNet (2023). Phishing attacks are getting scarily sophisticated. Here's what to watch out for.
[13] DarkReading (2023). ChatGPT artificial intelligence: an upcoming cybersecurity threat?
[14] Verizon (2022). 2022 Data Breach Investigations Report.

03

Geopolitcal crises: Exploiting the increasing global fragmentation

Cybercriminals are unscrupulous in their emotional manipulation tactics, and they particularly like using topics that affect society as hooks for their phishing attacks. One of their favorite methods: Provoking fear and uncertainty to pressure their victims into clicking on malicious content or disclosing sensitive information. The coronavirus pandemic was one of the most striking examples: Just a few weeks after the Omicron variant spread globally, a massive attack in the UK was launched with text messages and emails about the availability of COVID tests, even featuring National Health Service (NHS) branding, that were designed to lure people into giving out personal information.[15]

This shows cybercriminals spare no opportunity for attack – even when it comes to geopolitical crises. Russia's war on Ukraine resulted in a sharp increase in coordinated cyberattacks as part of the offensive, impacting organizations in both these countries and worldwide. For example, a Russian-based hacking group targeted several US-based non-governmental organizations (NGOs), the military of multiple Eastern European countries, and a NATO Centre of Excellence to steal confidential access credentials for espionage or the spread of malware.[16]

But these are not the only major events our society has had to tackle in recent years. After decades of increasing globalization, now the world seems to be experiencing a new megatrend: deglobalization. Although some signs appeared in 2008, this trend has recently accelerated because of the strategic competition between the United States and China, which is apparent in bilateral trade, investment flows, and in technology.[17] While the US-China relationship continues to worsen due to events like the coronavirus pandemic and the Taiwan crisis[18], we are already seeing the effects of increased volatility in supply chains, inflation, demographic changes, and even a food and energy crisis.

In light of these global events, geopolitics and cyber security have become inextricably linked. For example, several official websites in Taiwan were taken down by a series of DDoS attacks last year. The timing added concerns over China's involvement and opposition because the attacks occurred at a similar time to the visit of senior US Lawmaker Nancy Pelosi.[19] These attacks affect not only public entities but also private organizations worldwide. During the second half of 2021, China was widely condemned for launching a series of cyberattacks aiming to capture trade secrets, business information, and vaccine studies.[20] Targeted countries included the US, UK, and other global allies, who attributed the Microsoft Exchange hack to threat actors affiliated with the Chinese government.[21]

With DDoS and other types of cyberattacks being progressively used as part of geopolitical protests and scams, there's no doubt that cybercriminals will adapt their attack geographies and industries based on the highest current vulnerabilities. There is no turnaround: Tech and IT have become political, and both public and private organizations in countries experiencing heightened geopolitical tensions will need to implement cohesive security strategies to significantly reduce their cyber risk.

[15] The Independent (2021). Scam warning over fake omicron testing text messages.
[16] ZDNet (2022). Google: Multiple hacking groups are using the war in Ukraine as a lure in phishing attempts.
[17] Bruegel (2020). Deglobalisation in the context of United States-China decoupling.
[18] Reuters (2022). U.S.-China relationship bleeds by a thousand cuts.
[19] NBC News (2022). Taiwanese websites hit with DDoS attacks as Pelosi begins visit.
[20] InfoSecurity Magazine (2022). How geopolitical tension creates opportunities for cyber-criminals.
[21] Fortune (2021). U.S. and global allies blame China for Microsoft Exchange hack attack.

PRACTICAL TIPS

Geopolitical conflicts are mostly outside what we, as companies or individuals, can influence. But we can work on how to prepare for and respond to these new cyberspace challenges.

While regulatory requirements are tightened, companies should invest in ramping up their security measures, reviewing current setups, and patching vulnerabilities.

As the attacks are diversifying and increasing in number due to geopolitical tensions, cyberresilience heavily depends on how well--prepared organizations are for different threats. That also includes preparation on the supply chain level.

Organizations should identify their critical processes, which resources they need to run these processes, and set up business continuity plans for the case when a supplier fails.

Keeping up with the race between attackers and security professionals and continuously adjusting incident response and recovery plans to the new circumstances can make a decisive difference.

After all, cyber security has become political – and this should be reason enough for companies to finally move the topic to the C-level and give it the attention and resources it deserves.

INTERVIEW

“Cyber security is a journey and a process of constant adaptation as attack vectors keep changing.”

Ulrich Irnich
CIO and Modernization Garage Director
Vodafone Germany

Ulrich Irnich has been with Vodafone as CIO since 2020, responsible for the customer-centric IT orientation. Additionally, he directs the global Modernization Garage to drive BSS modernization across VF. Before that, as CIO at Unitymedia, he managed the agile transformation of IT and business. He transformed the company from a project-oriented to a product-centric organization. With extensive telecommunications experience, he brings deep insights into business and digital transformation.

Every company is hit with a cyberattack sooner or later, but there isn’t very much discussion about this. Do you think that conversations about this issue should be more commonplace?

Yes. But there’s not enough openness there yet. Companies might feel like drawing attention to it is an admission of guilt, weakness, or embarrassment. Hacktivists and ethical hackers are working very hard to make sure that everyone can learn from experience. We tried to talk about successful cyberattacks during our recent Vodafone Elevation Tour, but the reception to this was pretty muted. Companies that had been affected only became less hesitant once speakers started openly discussing attacks on stage.

The attacks we’re currently seeing against the backdrop of geopolitical crises and wars are just the tip of the iceberg. What’s your take on this?

Security incidents have become more common as a result of the war in Ukraine, that’s true. But what many don’t realize is that this was dangerous ground even before the war began. That is particularly true for the huge number of ransomware attacks. The number of unreported cases is probably very high. These large scale attacks are becoming more common because cybercriminals’ business models are becoming more appealing.

Are attack tactics changing as cybercrime becomes more professionalized?

The tactics are becoming more professional, too. We used to be able to identify phishing emails at first glance, but now there are more sophisticated tactics, as well as more channels and data, that can be used for attacks. For instance, all manner of platforms can be attacked if just one account is compromised. Nevertheless, the majority of attacks follow a standard pattern: They start with smaller, broad-scale "bombs" that determine who's worth targeting. It's a sort of return-on-investment analysis before the actual attack.

What do you think are the greatest risks to companies at the moment?

In addition to the ransomware attacks I already mentioned, the greatest dangers are social engineering, brute-force attacks, advanced persistent threats, and attacks that are launched from the inside.

Vodafone was targeted by a major ransomware attack in 2013. Have extortion methods changed since then, both for you as a corporation and for your business partners?

First of all, since 2013 we have invested hugely in our cyber defense to increase our maturity level, both in preventive measures and in our ability to respond appropriately. This does not mean we can no longer become a victim, but we have reduced the risk significantly. The danger lies in that cybercriminals today can achieve a much higher return on investment with customer data than they could have just a few years ago, because the data are sold on the black market for immense sums. Ransomware continues to be the main threat, especially for businesses. But the extortion methods are different ones today. In the past, malware was distributed more randomly.

Today, criminals specifically look for financially strong companies and infiltrate “door openers“. After that, they spy on the network, accounts and passwords and, in the course of this, apply further ransomware before extorting the ransom. Vodafone is one of the companies classified as critical infrastructure. So, above all, we have to provide special protection for the system-relevant infrastructure and, of course, for our customer data.

What do you think is the best way to deal with a ransomware attack: to pay or not to pay?

It depends. There could be a situation whereby one doesn’t have a choice. Linus Neumann, hacker and IT security consultant at Security Research Labs, once said, “No backup, no pity.” A proper incident response and recovery plan is crucial. My immediate instinct is to not pay, and to make sure that data can be reproduced if something serious happens, because prevention, detection, forensics, and reproduction are some of the most important steps in the entire process. I’d advise executive managers to know the processes that are critical to their business. The faster they can be up and running after an attack, the lower the risk – and the more uncertainty there is, the longer it will take to regain the data. After a few weeks, that could pose an existential threat to many companies.

Do you feel like the current threat situation at the C-level has resulted in more awareness of information security?

We conduct regular cyber incident management simulations with our executives. The last one was on ransomware, with everything that this type of crisis situation demands: communication with business partners, negotiations, media inquiries. Once you’ve simulated a crisis situation, the executives have this moment of stress that provides them with a new perspective on the risk.

Continuity is crucial, because if everything is working uninterrupted for a long time, and awareness is low due to a lack of incidents, this is precisely the moment when criminals strike. They’re waiting for moments like that to open up.

The question isn’t if your company will be hacked, but when, and how prepared you are for it. You have to know from the start which risks come with an attack, including liability risks for the management level. And it’s especially important to make clear that cyber security is not the task of the security team alone to protect the company. It’s a joint effort.

Which metrics do you use to highlight the relevance of information security at the management level?

The risks and consequences of attacks, and the company’s risk profile, are very clearly understood. We run through our top risks every year and evaluate them together. Business people always understand risks because they translate into monetary damages. The main questions here are, how great is the potential for damage, and how likely is it that something serious can happen? Cyberthreat is the greatest technical risk for the global economy right now.

Security needs investments, but there's no visible benefit if the measures are successful. Have budgets expanded in light of the fact that cybercrime is, by far, the greatest risk?

Cyber security isn't up for discussion – we've grown to such an extent, and achieved a certain level of maturity, that makes it paramount. It's an obligation for us as a critical infrastructure provider.

And for your business partners?

This topic hits much closer to home for companies that have been attacked in the past. If you look at mid-sized enterprises in particular, there's still a lot of progress to be made when it comes to awareness.

People used to always be seen as a vulnerability. It's not terribly motivating from a psychological perspective. What have you learned about establishing a security culture?

It's better to turn that around, rhetorically. People aren't the greatest vulnerability, but rather the best asset that we have when it comes to cyber security. And, above all else, it's important to share and discuss knowledge so that people can learn together.

What is it like at Vodafone? How is the human factor seen?

For us at Vodafone, it's important that we make people alert and resilient. Someone who's mentally well prepared can better protect themselves from the negative – and we're trying to draw more attention to the positive. That's not limited to the world of cyber security.

We have different lines of defense, and every employee is a part of that. One of these is mandatory training. We measure our level of maturity with a Cyber Security Baseline, with different checkpoints throughout the company that we evaluate and grade on a scale. This is work, and sometimes it's hard work. People sometimes complain about always having to do something, but these complaints pale in comparison to the consequences of a potential attack, and most people understand why they need to be vigilant and, as such, part of our defense system.

> “We have different lines of defense, and every employee is part of that.”

How do you maintain awareness among employees in the long term?

We have reached a high maturity level in our security culture. That can lead to negligence in day-to-day business, because employees might feel too safe. That is why we are continuously sensitizing our employees for the risks, for example, with regular awareness trainings. We are often asked: Can't we relax a bit here and there? But infiltration and social engineering are some of the primary danger zones, and awareness of that in the long term is key.

What trends do you see down the road?

We're living in a wonderful age when different lines are intersecting and amplifying: endless bandwidths, designed processing power for very little money, exploding data. The possibilities are staggering.

Take the Metaverse, for example. Can you know that you're talking to someone genuine if they have an avatar? The key word "deepfake" comes to mind. Digital identities will become a hot topic.

Then there's the matter of blockchains. We still have a ways to go as far as technology is concerned, since the processes are still too computationally demanding. There will also be new business models in the Metaverse. Artificial Intelligence will become more mainstream. Payment methods will change – NFTs, crypto – and this will have a major impact on conventional banks.

You could say that the merging of the digital and analog worlds will become more prevalent, and the number of targets will increase as attackers' business models multiply.

We already warned about deepfake tactics like voice cloning back in 2018. How do you rate the potential risk of artificial intelligence?

Obviously, this will give rise to new dangers. If you use technology to systematize knowledge, you can also weaponize it. There are many benefits to technology, but it certainly has a dark side.

The fact that we're not seeing many AI-generated phishing emails in the wild despite new tools like ChatGPT has more to do with the fact that the gates are already easy to open without this technology. But since everyone is working on increasing their own security, it's definitely going to happen sooner or later. Cyber security is a journey and a process of constant adaptation – and that includes adapting to new technology.

What are some concrete ways that employees can be supported in this regard?

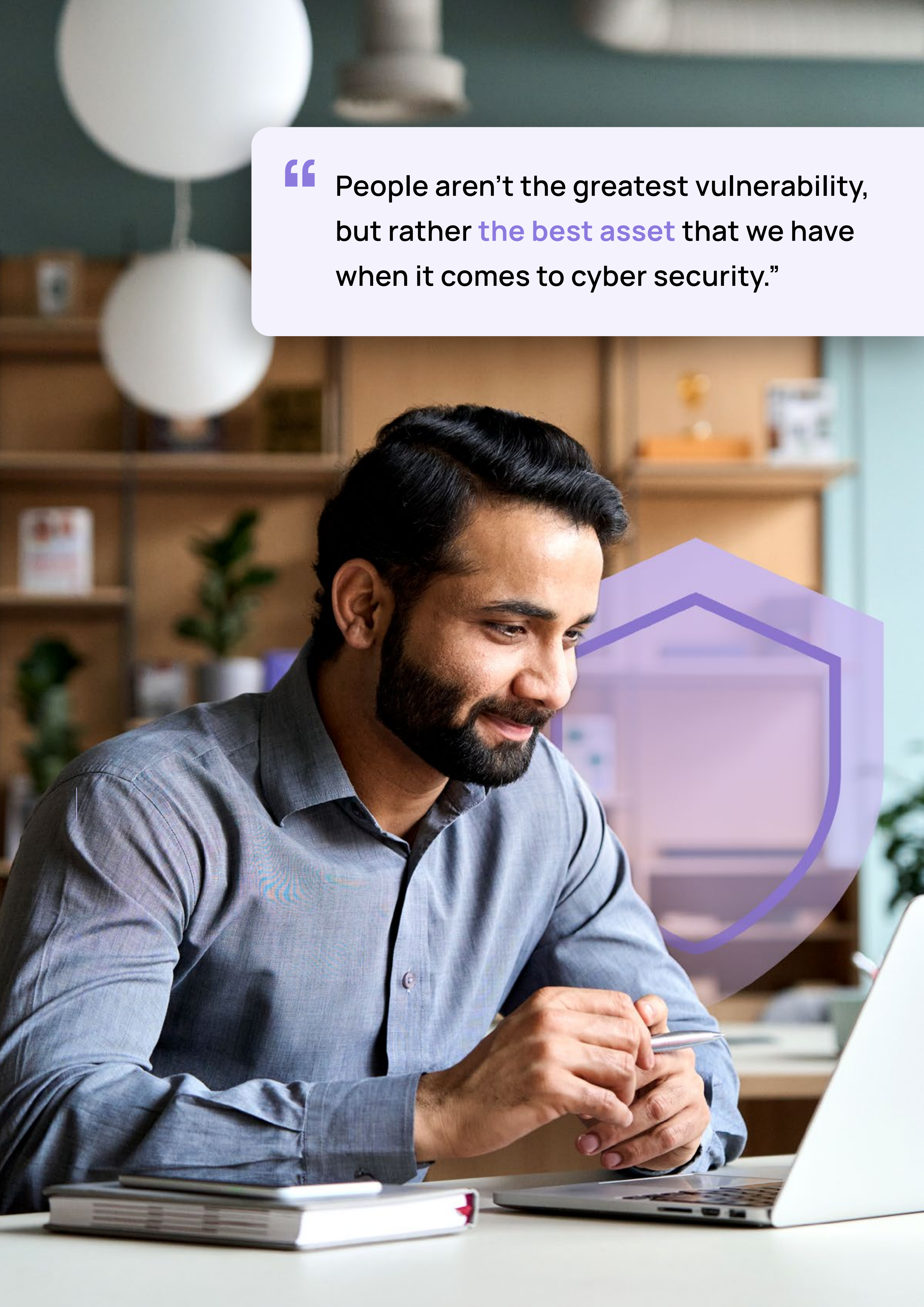
We have, for example, integrated a button into our email software that lets users report suspicious emails right away with one click. And, of course, we've also taken technical precautions so that the worst-case scenario will have the least possible impact. At the same time, we celebrate success and issue Spirit Awards to individuals who have made our organization more secure. We believe in promoting strengths, because punishment is only a short-term solution. Now it comes down to inclusion, making sure that people want to and can actively participate.

In closing: How do you think the next 12 months will look?

Let's start with the positives: many new opportunities in the digital world for solving global issues. New approaches to combating climate change, for example.

On the negative side, I think that attacks will become more common and cause more damage. We have to stay vigilant, adapt to this reality, and actively prepare people for what's to come.

> “People aren’t the greatest vulnerability, but rather the best asset that we have when it comes to cyber security.”

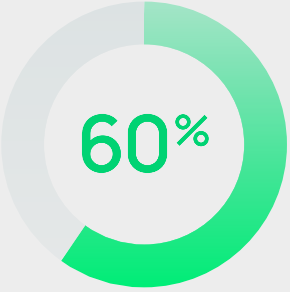


04 Burnout in security and beyond: Cybercriminals never had it easier

An unmotivated workforce is undoubtedly less engaged and committed to their company's goals, significantly negatively impacting overall organizational productivity. However, there is currently an even larger concern that might make companies more vulnerable to cyberattacks: burnout in employees, especially in IT and cyber security professionals.

The current cyberthreat landscape is worsening at a time when cyber security employees are clearly most afflicted with burnout. For the last couple of years, the COVID-19 pandemic, the global geopolitical situation, and remote work have put more pressure on IT and security professionals. For example, hybrid work affords hackers the opportunity to exploit security gaps caused by unsafe connections from home, using personal devices for work, and the increased use of collaboration tools like Microsoft Teams and Slack. To mitigate these risks, security employees are taking on an excessive workload, with around 12 percent working from 51 to 70 hours per week, according to the Chartered Institute of Information Security (CIISEC).[22]

Overworking and burnout are indeed causing many security professionals to leave their jobs. A study from the Information Systems Audit and Control Association (ISACA) found that 60 percent of companies had difficulties retaining qualified cyber security professionals in 2022, with stress at work being one of the top five reasons to hand in resignations.[23] This situation is aggravated by the 3.5-million worker shortage that the cyber security industry is currently experiencing.[24] The result: Cyber security teams are understaffed and unable to cope with the global increase in cyberthreats.



of companies had difficulties retaining qualified cybersecurity professionals in 2022

In this threat landscape, allocating enough resources and budget to security teams is of utmost importance. CIISEC's report also showed that in 2021 only 64 percent of companies raised their security budget, compared to 17 percent that didn't and 9 percent that decreased it. Out of the percentage of companies that raised it, only 9 percent allocated a high-enough budget to outstrip the escalating threat levels. Compared to previous years, statistics show a slight upward trend in companies not raising their budgets enough and a slight drop in businesses that do, meaning businesses now face a more complicated cyber security landscape without sufficient resources.

Stress, lack of motivation, and insufficient budgets draw the perfect picture for cybercriminals, who take advantage of fatigued cyber security experts who are more likely to overlook small details and struggle to find solutions to problems.[25] Besides, overworked professionals easily miss the signs of an attack or even make mistakes that create vulnerabilities for hackers, such as failing to update software.[26] Knowing the vulnerabilities that arise with stressed security teams, cybercriminals are apt to look at their composition and specifically target companies with teams that seem more vulnerable from the outside.

PRACTICAL TIPS

Addressing burnout in security employees should be highly important for businesses because it could prevent threat actors from leveraging it for unethical purposes.

Exhaustion and low morale can be overcome, but it requires a combination of measures, such as allocating the correct budget for cyber security, developing career plans to boost employee retention, and preventing teams from being understaffed and working long hours.

Many security teams also report they must carry the extra weight of being widely perceived to disturb or slow down work processes by restricting software downloading rights for employees on work devices, for example.

It should be top management's concern and objective to communicate the positive impact the security team's efforts have and raise the importance of continuous employee awareness training.

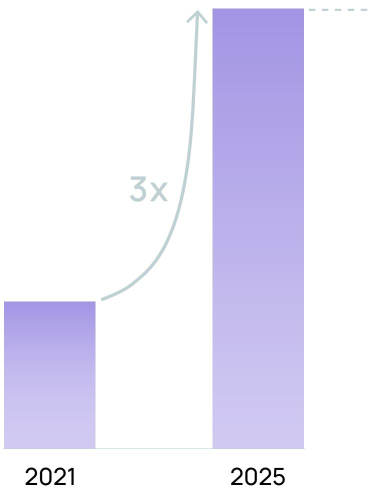
Now is the time to invest in education and the training of tomorrow's cyber security professionals – the very people who will help us stay safe in an increasingly complex threat landscape.

[22] Chartered Institute of Information Security (2022). The security profession 2021/2022.
[23] ISACA (2022). State of cybersecurity 2022: cyber workforce challenges.
[24] Chartered Institute of Information Security (2022). The security profession 2021/2022.
[25] Security Magazine (2023). One of the biggest threats of a cybersecurity team? Employee burnout.
[26] Bleeping Computer (2023). IT burnout may be putting your organization at risk.

05

Digital supply chain attacks: We are all interconnected

The alarming rise of supply chain attacks in 2022 was just a warning of what is yet to come in 2023, as this trend is set to escalate even more. This will affect traditional supply chains, especially digital ones. In fact, Gartner predicts that by 2025, 45 percent of organizations worldwide will have experienced attacks on their digital supply chains, a three-fold increase from 2021.[27]



45%

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

The events of the past two years have been a stark reminder of how much our security depends on the security of others. Cybercriminals continue improving their chances of success by exploiting their victims' partner and supplier networks – or even open-source technology. By taking advantage of any weak points in the supply chain, they infiltrate systems or infect a company network with malware.

One striking case happened in September 2022 when the multinational Vodafone experienced a data breach due to a cyberattack on one of its partners, FourB S.p.A. This incident exposed sensitive data and contact details of thousands of customers).[28] The Vodafone breach is not an isolated case, and the first data breaches of 2023 that can be traced back to partner vulnerabilities are already happening: Nissan North America announced in January that one of its software development vendors suffered a data breach that exposed full names and dates of birth of thousands of Nissan customers.[29]

Since these attacks target entire supply chains and not only individual companies, they impact large corporations like Vodafone and Nissan and local businesses with fewer resources that struggle mightily to recover from the attacks. Recently, the British mail delivery company Royal Mail had to temporarily interrupt their international export services due to a ransomware attack, causing delays of several days in international shipments for many customers. This led to significant financial losses for small business owners.[30]

Open-source software has also proven to be one of the main targets of hackers. Platforms like Codecov have already suffered the consequences. A vulnerability in Codecov's Docker Image creation process gave hackers access to Codecov's customer data.[31] The Log4j vulnerability discovered in December 2021 is another example of the complexity and long-term impact these incidents can have. It is estimated that Log4j was used in around 36,000 programs, meaning the effects of the Log4j incident will be present until all the applications are updated.[32]

These developments – coupled with understaffing in many security teams – are turning the threat landscape into a breeding ground for cybercriminals. The fact that many companies use outsourced solutions for tasks that their security teams don't have the capacity to deal with only widens the attack surface. In the end, using (security) software always comes with a risk, as the August 2022 security breach of LastPass and its customers showed.[33] It is on companies to ramp up their security strategies so that they can cater to the interconnected software landscape we operate in today.

PRACTICAL TIPS

Before entering into a relationship with a service provider or supplier, companies must become familiar with their level of security and compliance to minimize risks.

For example, they should check whether their partners have the appropriate (software) certifications or meet regulatory obligations like GDPR and additional standards like ISO/IEC-27001. Third-party assessments and audits of the company, its customers, and investigating recent breaches can help better understand the suppliers' eligibility.

In the next step, companies are well advised to mitigate the supplier risk to a minimum by agreeing on supplier rights and incident response and notification plans. They can also monitor remote access, restrict it, and strengthen it with additional layers like multifactor authentication.

Regular reviews are key: Checking in on supplier performance and tracking changes in the relationship helps limit risks. In the end, the security of your partners and suppliers is also part of your security.

[27] Gartner (2022). Gartner identifies top security and risk management trends for 2022.
[28] Bleeping Computer (2022). Vodafone Italy discloses data breach after reseller hacked.
[29] Cybernews (2023). Nissan data breach exposed clients' full names and dates of birth.
[30] BBC News (2023). How cyber-attack on Royal Mail has left firms in limbo.
[31] Bleeping Computer (2021). Popular Codecov code coverage tool hacked to steal dev credentials.
[32] Forrester (2021). Log4j, open source maintenance, and why SBOMs are critical now.
[33] The Hacker News (2022). LastPass admits to severe data breach, encrypted password vaults stolen.

06

Ransomware-as-a-Service: Online extortion at the push of a button

Since its advent in the late 1980s, ransomware has been one of the most common cyberattack types – feared by companies and individuals alike. In recent years, however, it has undergone considerable professionalization: In a drastic increase of ransomware-as-a-service (RaaS), cybercriminals are now diversifying their business models.

Today, ransomware attackers don't need considerable IT knowledge or hacking skills – just a simple browse on the dark web and a crypto payment will do the job. With operations that resemble those of normal software-as-a-service providers, including subscription models and dedicated customer services (as the Conti leaks have impressively shown[34]), RaaS operators offer anyone the chance to run large-scale attacks. This has multiplied the potential number of cybercriminals astronomically.

The consequences are as threatening as they are impressive: From 2021 to 2022, there was a 13 percent increase in ransomware – an increase higher than in the five preceding years combined.[35] 2022 saw 71 percent of organizations fall victim to a ransomware attack.[36] With recent IBM research suggesting that a successful ransomware attack costs companies an average of $4.54 million – the ransom not included – the destructive effects on the economy become apparent.[37]

Organizations worldwide have already been targeted with RaaS-based attacks. One prominent example is the attack on pipeline operator Colonial Pipeline initiated by the ransomware group DarkSide in 2021.[38] The attack led to a temporary halt of all pipeline operations and a gas shortage along the US East Coast. Later, it became clear how this attack happened: a compromised password and lacking multi-factor authentication allowed the attackers to access internal systems.[39]

$4.54 million

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

REvil also relied on a RaaS model for many of its attacks. For example, its supply chain attack on software provider Kaseya negatively affected thousands of companies in 2021. Insurance company CNA Financial and Brazilian meat producer JBS are among other well-known REvil victims and made the news with some of the biggest ransom demands ever paid, amounting to $40 million and $11 million, respectively. Although authorities shut down REvil in early 2022, it is believed to have already resurfaced under different names.[40]

The new star in the RaaS domain is probably LockBit. In the summer of 2022, automotive parts supplier Continental fell victim to the group's attacks. On top of placing a ransom note, LockBit stole an estimated amount of 40TB of data and, after Continental refused to pay the amount, placed the data for sale on the dark net for about $50 million.[41] This double extortion can be seen more frequently in RaaS attacks and urges many companies to pay the ransom due to a lack of alternatives. At the same time, LockBit made themselves heard when its members announced a bug bounty program to "make ransomware great again," effectively outsourcing the search for vulnerabilities and multiplying their chances of success with the help of their cyber community.[42]

With harmful attacks being just a few clicks away, multiple extortion techniques booming, and an increased interconnectedness of supply chains, ransomware is an extremely profitable playground for cybercriminals worldwide. Companies are well advised to step up their security because what we have seen recently seems to be just the beginning of a ransomware epidemic.

PRACTICAL TIPS

Preventing ransomware attacks is a massive undertaking, the consensus being that every company will sooner or later become a victim. Therefore, security measures should not only focus on prevention but also on containing potential consequences.

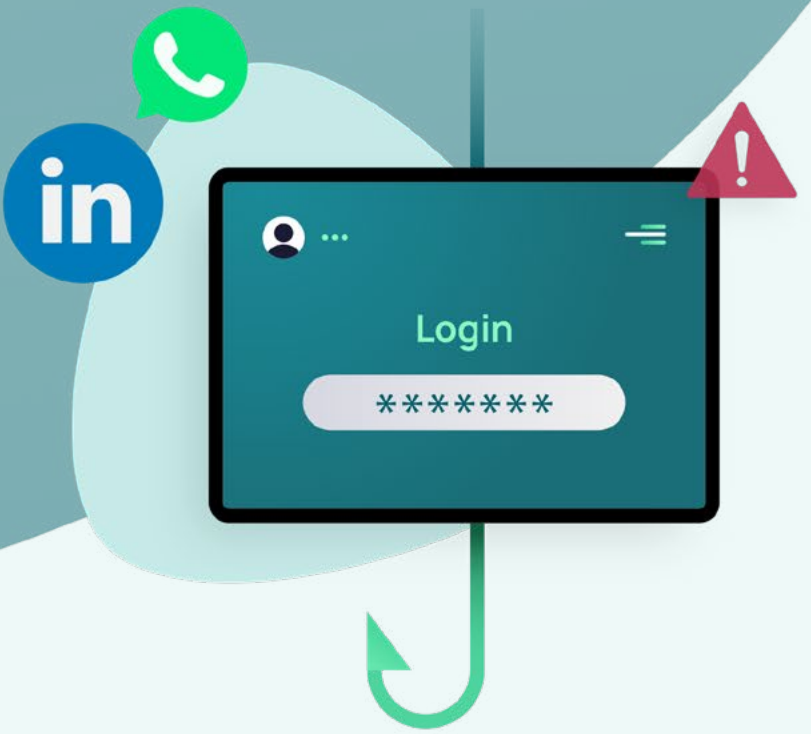
First and foremost, companies need to keep their software updated, continuously patch vulnerabilities, and have reliable endpoint protection and threat detection tools set up.

Restricting employees' administrative privileges on devices, reviewing and pushing through effective password policies, and putting into place strong access management on a server level can also be beneficial measures. They can contain the consequences of potential attacks since they prevent attackers from spreading ransomware throughout entire systems.

At the same time, since many of the attacks start with a form of social engineering, awareness training can effectively minimize the risk of ransomware incidents.

The prime way to avoid having to succumb to a ransomware demand is backing up data and having an incident response plan in place that acts quickly should it come to an attack.

[34] TechCrunch (2022). Conti ransomware gang's internal chats leaked online after declaring support for Russian invasion.
[35] Verizon (2022). 2022 Data Breach Investigations Report.
[36] Statista (2022). Percentage of organizations victimized by ransomware attacks worldwide from 2018 to 2022.
[37] IBM (2022). Cost of a data breach 2022. A million-dollar race to detect and respond.
[38] ZDNet (2021). Colonial Pipeline ransomware attack: Everything you need to know.
[39] Reuters (2021). One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators.
[40] TechCrunch (2022). Russia's FSB 'shuts down' notorious REvil ransomware gang.
[41] Tech Monitor (2022). FBI joins investigation into Continental ransomware attack.
[42] Bleeping Computer (2022). LockBit 3.0 introduces the first ransomware bug bounty program.



07

Multi-channel phishing: Email security is not enough anymore

Gone are the days when email was the only channel hackers used to steal credentials and private information, and cause company data breaches. As phishing becomes more diverse and sophisticated, attackers choose new platforms – or even use multiple ones in the same attack – to steal sensitive data from individuals and companies.

Social media is becoming an increasingly important channel for cybercriminals: The recent attack wave on TikTok pushing malware with the "invisible body" challenge only confirms it. The challenge encouraged people to record themselves naked and use a filter to blur the image. Hackers saw the opportunity to appeal to human curiosity and promoted software that was supposed to unblur the videos. They directed users to a Discord server where they distributed links with malware called WASP Stealer. By doing this, they could steal sensitive information, such as passwords and credit card details from thousands of users.[43]

Cybercriminals also apply tactics used in apps like Telegram and Discord on more professional platforms, such as LinkedIn, Slack, and Microsoft Teams. Remote work has increasingly blurred the lines between private and professional use of devices, allowing intruders to use those channels to access sensitive company credentials and information. One example is the security breach Uber suffered after one of its employees was tricked into accepting an MFA notification. In a WhatsApp message, the hackers pretended to be colleagues from the IT department and asked him to grant them access to internal networks.[44]

LinkedIn has also been used by threat actors to deceive employees – and especially those on the lookout for a new job – by tricking them into clicking on phishing emails or offering fake job offers in exchange for upfront payments or bank details.[45] At the same time, this social platform can be a source of information for spear phishing attacks where the attackers learn about a company's new hires and impersonate their superiors to ask them to click on links and enter login credentials on fake websites to steal their credentials.[46]

Not only LinkedIn but many other professional tools are being exploited by hackers. The video game company Rockstar also suffered an attack that led to a massive leak of footage from the early stages of development of the video game Grand Theft Auto 6 (GTA6). The attackers broke into the company's Slack channel and gained access to a substantial amount of footage and other information, such as the source code of GTA5 and GTA6. They then published 90 videos with around 50 minutes of footage and threatened the Rockstar developers with publishing the source code if they didn't receive a large sum of money.[47]

Phishing can now hide almost anywhere, even in seemingly harmless browser notifications. When used for unethical purposes, they can act as an entry point to our devices and be used as a tool to obtain credentials and sensitive information. One example is browser notifications that warn users of an alleged virus infection on their computer and ask them to click on it to delete the virus. By creating a compelling sense of urgency and fear, hackers make the victim download malware or log in using their credentials.[48]

[43] Bleeping Computer (2022). TikTok 'Invisible Body' challenge exploited to push malware.
[44] The Verge (2022). Uber's hack shows the stubborn power of social engineering.
[45] We Live Security (2022). Common Linkedin scams: beware of phishing attacks and fake job offers.
[46] CSO (2022). How cybercriminals use public online and offline data to target employees.
[47] The Guardian (2022). Grand Theft Auto 6 leak: who hacked Rockstar and what was stolen?
[48] ReviewGeek (2022). That computer virus you can't remove might be a browser notification.

As hackers are now exploiting new channels, such as social media and messaging apps, to barge into our devices, cyberattacks become increasingly harder to avoid and detect. This is the reality we now live in: It won't take much time between the creation of a new channel and its exploitation by cybercriminals.

PRACTICAL TIPS

With humans being in the crosshairs of social engineering attacks, it only seems logical to build security awareness and underline the relevance of being vigilant across channels.

Employees should be vital to a company's ISMS to strengthen the overall security culture. As asset owners for their mobile devices or software they have requested, they are responsible for meeting security requirements.

On top of that, contextual threat detection tools on the different channels might help employees more readily find and report potential attacks.

Since many of these phishing attacks rely on exploiting zero-day vulnerabilities, strengthening the human factor by supporting employees is the most promising way for companies to protect themselves.

08

Multi-factor authentication fails: Not as safe as we thought

Organizations have long relied on multi-factor authentication (MFA) as an effective measure to protect themselves from cyber security incidents. Unfortunately, although MFA has proven to be a significant obstacle for hackers, its ability to keep organizations safe may have been overestimated.

Multi-factor authentication can be implemented in several ways, one of the most popular being pop-up phone notifications asking for authorization from the user. However, cybercriminals have found a way to sabotage this authentication by applying a social engineering tactic called MFA fatigue or MFA push spam, which consists of flooding victims with repeated pop-up notifications until they eventually accept them by mistake or out of exhaustion. As mentioned in the previous trend, hackers then usually contact the victim through another channel pretending to be IT support and encouraging them to accept the prompt. This method was recently used in the massive data breaches of Uber, Microsoft, and Cisco.[49]

Another common way of bypassing MFA is the attacker-in-the-middle (AiTM) technique, which looks like a regular phishing attack but is slightly more sophisticated. It usually starts with a phishing email that leads the user to a fake log-in page that looks exactly like the original. This attack uses a proxy that sits in the middle of the fake and original page, allowing attackers to save the session cookie generated after entering the log-in details and MFA passcode. Afterward, hackers use those cookies in their own browsers to automatically log into the victim's account without going through authentication again. This attack was recently used in combination with spear phishing techniques to compromise Microsoft 365 accounts of C-level employees and divert large money transactions to the hackers' bank accounts.[50]

Threat actors have also tried to leverage MFA as an attack vector in big data breaches, such as the supply chain attack on SolarWinds. The attempt was discovered when someone tried to register a second phone for authorization.[51] However, phone-based MFA attacks are not always easy to detect. In 2021, hackers used a method called SIM-swapping to empty their victims' crypto wallets by tricking telecom providers into assigning the user's phone number to a new SIM card. This allowed scammers to receive multi-factor authentication SMS on a new SIM card, granting them access to their victims' crypto accounts.[52]

Malicious software can also be used against MFA in man-in-the-endpoint attacks. In this attack, malware is installed on the user's device, allowing hackers to start rogue sessions in the background – only visible to them – once the user completes MFA. The attackers can use the rogue session for malicious purposes, such as rerouting paychecks to the hacker's bank account.[53] Another method threat actors use is rebuilding password generators in authentication systems that rely on one-time passcodes. This technique requires a high level of technical skill and consists of reverse engineering the algorithm and seed number of the generator to take control of it. Once done, the hacker can send passcodes to the user and thus circumvent MFA.[54]

No matter the tactic, MFA has become an attack vector in large-scale data breaches. Despite being a strong additional security layer, the way it is implemented and the number of complementary security measures in place will determine the security level it provides.

PRACTICAL TIPS

To benefit from MFA's promise of strongly increasing a company's information security, reviewing both internal organizational processes and employee awareness is crucial.

On a technical level, switching to number matching for MFA and/or limiting the number or time people can accept authentication requests already mitigates risks. Companies should also delete orphaned accounts and review access rights frequently, relying on least privilege access for their systems.

Some people even recommend switching to phishing-resistant MFA practices, such as using physical tokens or avoiding MFA completely by using SSO for as many accounts as possible.

On an organizational level, companies can benefit from employee awareness training. Users who know how to act in case something seems off and can avert attacks when they occur are a company's biggest asset when avoiding MFA bypassing and MFA fatigue, more specifically.

[49] Bleeping Computer (2022). MFA fatigue: hackers' new favorite tactic in high-profile breaches.
[50] Bleeping Computer (2022). Hackers use AiTM attack to monitor Microsoft 365 accounts for BEC scams.
[51] Gartner (2021). How to respond to a supply chain attack.
[52] Tech.co (2021). Hackers are hijacking phone numbers to empty crypto accounts.
[53] Beyond Identity (2020). How your MFA can be hacked (with examples).
[54] Beyond Identity (2020). How your MFA can be hacked (with examples).

Scale your security culture with ease

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

TEACH —

Engaging Micro-Learning

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

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

TRANSFER —

Smart Attack Simulations

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

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

ACT —

Strategic Risk Monitoring

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

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

sosafe

SoSafe GmbH
Lichtstrasse 25a
50825 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.