Cybercrime Trends 2025

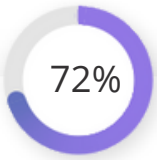
sosafe

itb cyber solutions

Contents

Executive summary

The scale and impact of cybercrime has reached new heights



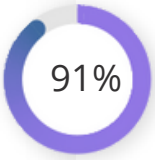
of organizations report rising cyber risk.[1]

$13.82 trillion

in damages from cybercrime projected by 20282...

... nearly a **50%** increase since 2024.

Cybercriminals are weaponizing AI faster than companies can adapt...



of security experts expect a significant rise in AI-driven threats over the next three years.

And even though **96%** of professionals recognize the importance of detecting AI-based attacks, ...

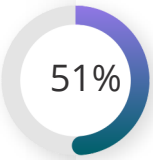
... only **26%** rate their ability to do so as "high".

...but AI isn't just a threat — it can also become a powerful ally

> We should not only use AI to combat its dangers but also leverage it to prepare ourselves for possible scenarios through targeted training.

Frank Schätzing
Science-fiction book author

Attackers are no longer relying on just one entry point — they're using every channel available



of security professionals still report email as a primary target, but...

94% of organizations report a rise in multi-channel attacks leveraging email, messaging apps, social media, and deepfake voice calls.

[1] World Economic Forum (2025). Global Cybersecurity Outlook.

[2] Statista (2024). Cybercrime Expected to Skyrocket in Coming Years.

Protecting your own company is no longer enough — attackers target your entire network

94%

of organizations rely on third-party vendors – each connection expands the potential attack surface.

And your personal life is now also part of their attack surface

83%

of organizations have been targeted through personal devices or accounts.

We need to go beyond just company security training. Train your family and your friends — because attackers are targeting everyone.

Andrea Szeiler
Global CISO at Transcom

In this escalating threat environment, attackers do not hesitate to prey on the most vulnerable

98%

of respondents believe the security gap is widening,

leaving critical industries and small companies unprepared to fight against threats.

According to the World Economic Forum,

over 1/3

of small organizations believe their cyber resilience is inadequate1.

The public sector is also struggling...

38%

of companies report insufficient resilience1.

And the only way to stay ahead of them is by joining forces

Collaboration between the private and public sector is essential. As it's usually said, 'it takes an international network to defeat an international network'.

Philipp Amann
Group CISO, Österreichische Post AG

[1] World Economic Forum (2025). Global Cybersecurity Outlook.

The new era of cybercrime: More threats, less boundaries

Cybercriminals are more ambitious than ever — and they know exactly how to exploit every corner of our digital lives. This year's trends reveal a shift where attackers are relentlessly exploiting not only corporate networks but also personal identities, accounts, and even family members to gain access to organizations. At the same time, they are becoming more strategic and efficient, leveraging AI to enhance attack sophistication, supply chain vulnerabilities to scale their reach, and multichannel deception to bypass traditional defenses. By blending tactics across email, SMS, social media, and collaboration platforms, they are manipulating trust and exploiting every possible entry point. As a result, cyber risk is escalating — with 72% of organizations reporting an increase in threats, according to the World Economic Forum. As the attack surface has never been larger, organizations must prepare for a future where threats are more personalized, scalable, and harder to detect.

Understanding the trends is the first step to staying ahead. This report breaks down what's shaping cybercrime in 2025 and provides practical tips from SoSafe's security leaders to help you prepare for what's next.

Methodology and sources

Cybercrime Trends Survey 2025

For this survey on the cybercrime trends in 2025, we partnered with Censuswide, an international market research consultancy headquartered in London. 500 security professionals from 9 countries (UK, France, Germany, Austria, Switzerland, the Netherlands, Belgium, Luxembourg, and Australia) were surveyed in December 2024.

Survey on The State of Next Generation Social Engineering

This global survey gathered insights from over 100 SoSafe customers across more than 10 countries in 2024 to examine how social engineering tactics are evolving and the growing risks organizations face as attackers refine their techniques.

1 The rise of AI as an exploitable attack surface

Cybercriminals keep exploiting AI to widen their reach...

Artificial intelligence is revolutionizing industries, but it's also creating unprecedented opportunities for cybercriminals. AI is not only being weaponized to orchestrate sophisticated attacks with, for example, realistic deepfakes, but also to produce mass-scale AI-generated phishing campaigns that require fewer resources while delivering more effective results for attackers. According to the World Economic Forum, there was a 223% increase in the trade of deepfake- related tools on dark web forums between Q1 2023 and Q1 2024.1 The effects of this surge are starting to be seen in real life. Recently, the CEO of the world's biggest advertising agency, WPP, suffered a highly sophisticated multi-channel deepfake scam where attackers used voice cloning to impersonate the executive and extract money and personal details from employees.2

However, AI is not only used as a tool to break into organizations: it's also now widening the organizations' attack surface. Many companies are developing internal AI tools to enhance their business operations, from automating processes to analyzing sensitive data. However, many of these tools often lack sufficient cyber security safeguards, turning them into a significant liability. If cybercriminals gain access, they can use these tools to uncover sensitive information, map vulnerabilities, and navigate security systems undetected, exposing the organization to severe risks.

...and level up their game to outpace organizations' defenses

Looking ahead, 91% of respondents of our customer survey expect the threat and intensity of AI-based cyberattacks to increase over the next three years. But it's not just the volume of threats that's increasing; their complexity is escalating as well. Obfuscation techniques, such as AI-generated methods to mask the origins and intent of attacks, is the top concern of AI-driven attacks for cyber security leaders – according to our Cybercrime Trends survey.

While organizations seem to be aware of this escalating risk, with 96% of professionals recognizing the importance of detecting AI-based attacks in our customer survey, only 26% rate their ability to do so as "high." This lack of preparedness highlights a critical vulnerability—but AI itself can be part of the solution. By training employees through smart simulations, correlating security alerts, and automating code corrections, AI has the potential to become truly transformational in cyber security defense.

> We should not only use artificial intelligence to combat its dangers, but also leverage it to prepare ourselves for possible scenarios through targeted training.
>
> 
>
> Frank Schätzing
> Science-fiction book author

1 World Economic Forum (2025). Global Cybersecurity Outlook.
2 New York Post (2024). CEO of WPP, world's biggest advertising agency, falls victim to elaborate deepfake scam.

Practical tips

- Educate and raise awareness: Train staff on AI's capabilities and associated risks, including recognizing AI-driven attacks like deepfakes. Early adopters must prioritize security during the design, implementation, and maintenance of AI technologies to minimize risks.
- Establish AI governance: Create a governance committee and process to manage all AI solutions within your organization. Maintain an inventory of AI tools, assign ownership, assess risks, and outline recovery paths for potential failures. Include mechanisms to monitor emerging risks related to your organization's specific AI decisions and strategy. Use frameworks like ISO42001 as a foundation.
- Avoid AI unification: A single AI with access to all data may simplify user experience but introduces major risks. Segregate training data sets to prevent boundary-crossing, like a warehouse worker accessing network designs or a developer accidentally exposing HR data. Use specialized AIs rather than an all-encompassing system.
- Cover security essentials: Strengthen basics like least privilege access, segregation of duties, regular privilege reviews, MFA, and patching. Ensure a robust, well-rehearsed incident response plan is in place.
- Align AI with regulations: Treat AI outputs and decisions as subject to existing regulations. Ensure AI systems comply with GDPR and other frameworks by maintaining auditable records and clear accountability for AI owners.

What aspect of AI-driven attacks concerns you most, if any?

	All	UK	Australia	France	DACH	BENELUX
The difficulty in attributing attacks	50.8%	55%	52%	52%	54%	41%
The creation of entirely new attack methods	44.8%	45%	43%	56%	38%	42%
Realism of AI-generated content	41.6%	45%	44%	40%	36%	43%
Targeted precision	41.4%	46%	49%	33%	48%	31%
Lack of preparedness and detection tools for AI threats	38.8%	29%	48%	37%	41%	39%
Scale and speed of automated attacks	38%	38%	43%	38%	32%	39%

2 The rise of multichannel attacks

Cybercriminals are combining channels in highly sophisticated 3D phishing attacks...

Cybercriminal tactics and channels have rapidly advanced in recent years. While 51% of security professionals still report email as a primary target, attackers are increasingly diversifying their methods, often combining multiple channels in the same attack.1 Furthermore, advancements in AI enable cybercriminals to execute highly sophisticated and harder-to-detect hyper- targeted attacks. In fact, according to our Cybercrime Trends survey, 94% of organizations report an increase in multichannel attacks over the past year.

Why? Attackers have it easier than ever as new channels are added to the human communication toolkit. They are targeting victims through a combination of email and social media accounts, phones, and messaging apps, which allows them to mimic normal communication patterns to appear more legitimate – for example, sending a document via email and then following up on a messaging app.2 These tactics — including phishing, vishing, smishing, and QR phishing — are evolving into 3D phishing attacks, which seamlessly integrate voice, video, and text-based elements to create highly convincing scams powered by advanced AI.3 The attack on the CEO of WPP mentioned in Trend 1 highlights how cybercriminals combined WhatsApp to build trust, Microsoft Teams for further interaction, and an AI-generated deepfake voice call to extract sensitive information and money.4

...that are more targeted and harder to detect than ever

What makes these attacks so sophisticated is not just the multichannel approach but also the hyper-targeted nature of their execution. Attackers use advanced social engineering tactics like pretexting to exploit personal information shared online, which helps them craft false narratives based on real details to gain trust and credibility. And these attacks are on the rise - according to Verizon, phishing and pretexting account for 73% of breaches in social engineering incidents.

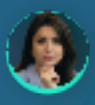
These threats are hard to detect not only by individuals but also by authorities, as they are often carried out on platforms with minimal regulation, such as Telegram. Beyond facilitating attacks, these platforms are also central to the professionalization of cybercrime. A UN report revealed how criminal networks in Southeast Asia are thriving on Telegram's underground markets, trading stolen data, hacking tools, and other illicit services with minimal oversight. This is driving the rise of multichannel attacks, further worsening the already volatile cyber threat landscape.

1 SoSafe (2024). Human Risk Review 2024.
2 Northdoor (2024). Phishing Threat Trends Report.
3 Cyber security insider (2024). New Surge in Risky Business Email Compromise Phishing Attacks.

Practical tips

- Educate staff on attack methods: Employees need to understand how attackers operate. Your awareness program should highlight key techniques and channels to help staff stay vigilant.
- Multichannel awareness training: Move beyond email phishing simulations to include smishing and vishing to prepare your workers for diverse attack vectors.
- Restrict corporate communication to secure tools: Collaboration tools often allow external parties to connect, creating opportunities for attackers to exploit 'trusted' environments. Disable this feature unless absolutely necessary to reduce exposure to potential threats.
- Reinforce core access controls: Ensure that essential protocols like segregation of duties and least privilege are not only in place but also effectively implemented. Regularly review these controls to minimize the risk of unauthorized access.

> For so many years, we said, 'If you're unsure about an email, call and verify.' But now, even if you call or hear the voice, maybe it's not real. It's becoming more and more complicated.



Yasemine Douadi
Cyber security expert & CEO of
RISKINTEL MEDIA and RISK SUMMIT

4 New York Post (2024). CEO of WPP, world's biggest advertising agency, falls victim to elaborate deepfake scam.
5 Verizon (2024). Data Breach Investigations Report.
6 Reuters (2024). Telegram app hosts 'underground markets' for Southeast Asian crime gangs, UN says.

3 Supply chain attacks: Third-party risks that escalate into massive breaches

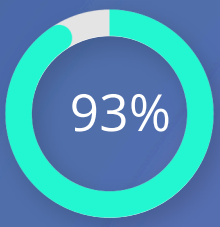
Third-party vendors have become essential to business operations...

No matter how strong your security strategy is, it's only as secure as the vendors you rely on. According to our Cybercrime Trends survey, 93% of companies now rely on third-party services to deliver their main value proposition. And this reliance comes at a price. Every additional provider introduces new dependencies, data exchanges, and access points — each a potential entryway for cybercriminals. They no longer need to breach a company directly; they can infiltrate a less-secure vendor and move laterally to more valuable targets. Alternatively, they can disrupt or compromise a service and impact multiple organisations simultaneously.

Last year showed just how effectively cybercriminals can exploit digital supply chains. In July 2024, attackers exploited a critical vulnerability in Fortinet's FortiOS and FortiProxy, allowing them to bypass security protections and gain unauthorized remote access to affected systems.1 Only one month before, a ransomware attack on CDK Global, a key software provider for over 15,000 car dealerships in North America, forced the company to shut down its systems, leading to widespread operational disruptions and significant financial losses across the automotive companies that it serviced.2

...but every added dependency expands the attack surface

The consequences of supply chain vulnerabilities are even more severe now that companies — especially large ones — depend on highly complex, interconnected ecosystems. It's not just a matter of relying only on third-party vendors anymore — but also on their vendors' suppliers, creating an extended web of exposure known as fourth-party risk.3 This lack of visibility limits organizations' awareness of the risks embedded in their partnerships and the full extent of their attack surface.



of companies now rely on third-party services to deliver their main value proposition.

1 Cybersecurity Dive (2024). Critical CVE in 4 Fortinet products actively exploited.
2 The Cyber Express (2024). CDK Global Cyberattack Ripple Effect: Several Car Dealers Report Disruptions.
3 Dataminr (2024). Third-party Vulnerabilities Put the Public Sector at Risk: What to Consider.

Practical tips

- Build and maintain a third-party inventory: Many organizations lack full visibility into their supplier portfolios. Maintaining an accurate inventory requires more than listing vendors - it may involve scanning web traffic, workstations, and gateways for shadow IT, reviewing invoices and company credit card transactions, and gathering self-declarations from business units during BCP/DR planning. Regular updates to this inventory are essential to uncover hidden dependencies and mitigate risks.
- Classify third parties by risk level: Develop a risk model to assess potential threats from each vendor. Tie scrutiny, contractual obligations, and controls to their risk levels, and ensure the supplier management team implements it.
- Enhance risk assessments: Supplement traditional questionnaires with on-site reviews, penetration tests, and perimeter scans to evaluate technical risks. Don’t overlook human factors like security awareness and culture within the vendor organization.
- Segregate external collaboration zones: Separate collaborative zones from critical systems to minimize the impact of a breach if a supplier is compromised.
- Diversify your supply chain: Avoid over-reliance on a single supplier. Ensure operational flexibility to pivot to alternatives if needed, reducing risks from attacks targeting key partners.

> We need to ensure that purchased software follows secure development processes. I want to see reports, know security criteria, and verify that secure development practices exist.

Lars Kukuk
CISO of the German Federal Employment Agency

4 Personal identities: The quiet doorway to corporate systems

Hackers are turning personal devices into organizational threats...

Personal identities are more at risk than ever. Cybercriminals have always targeted individuals, but their objectives and methods have changed. They are now using personal identities as a backdoor into corporate systems. Alarmingly, 83% of security professionals report that their organizations have already been hit by cyberattacks originating from personal devices or accounts. These attacks bypass traditional corporate defenses, broaden the attack surface, and leave organizations more exposed than ever.

The stakes are even higher as attackers scale their operations. Fueled by AI, cybercriminals are automating "consumerized attacks," enabling them to deploy numerous smaller-scale, highly targeted threats. Our data reveals that 73% of respondents have seen a surge in consumer-focused threats. By preying on individuals at scale, hackers are achieving their financial objectives through smaller, cumulative payouts.

...and no one is spared, not even your loved ones

This issue is escalating as the lines between personal and professional life blur. With hybrid and remote work models, employees increasingly rely on personal devices and accounts, expanding the attack surface far beyond corporate firewalls. Adding fuel to the fire, large-scale data breaches and the oversharing of personal information online have made it easier than ever for cybercriminals to exploit sensitive data like passwords, addresses, and family connections. Threat actors are now targeting employees' relatives, using them as an indirect route to breach organizations. In fact, in a recent case, attackers used SIM swapping to target the child of an executive, leveraging psychological manipulation to extort a ransom.1 This is putting everyone at risk, not only employees and executives but also their families.

The result? A constant wave of large-scale scams and targeted identity attacks, bombarding people and greatly increasing the chance of human error.

> We need to go beyond just company security training. Train your family, your friends - because attacks are targeting everyone.

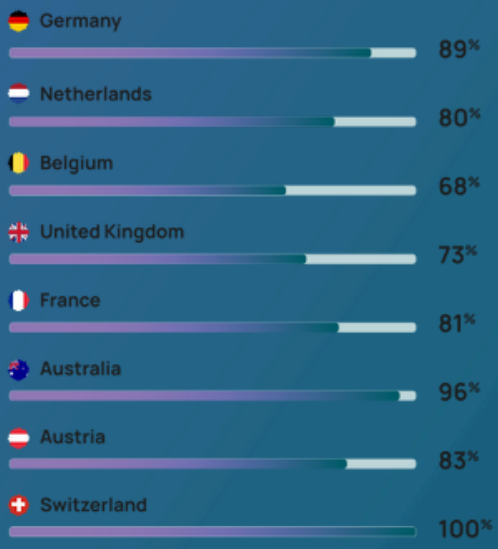
Andrea Szeiler
Global CISO at Transcom

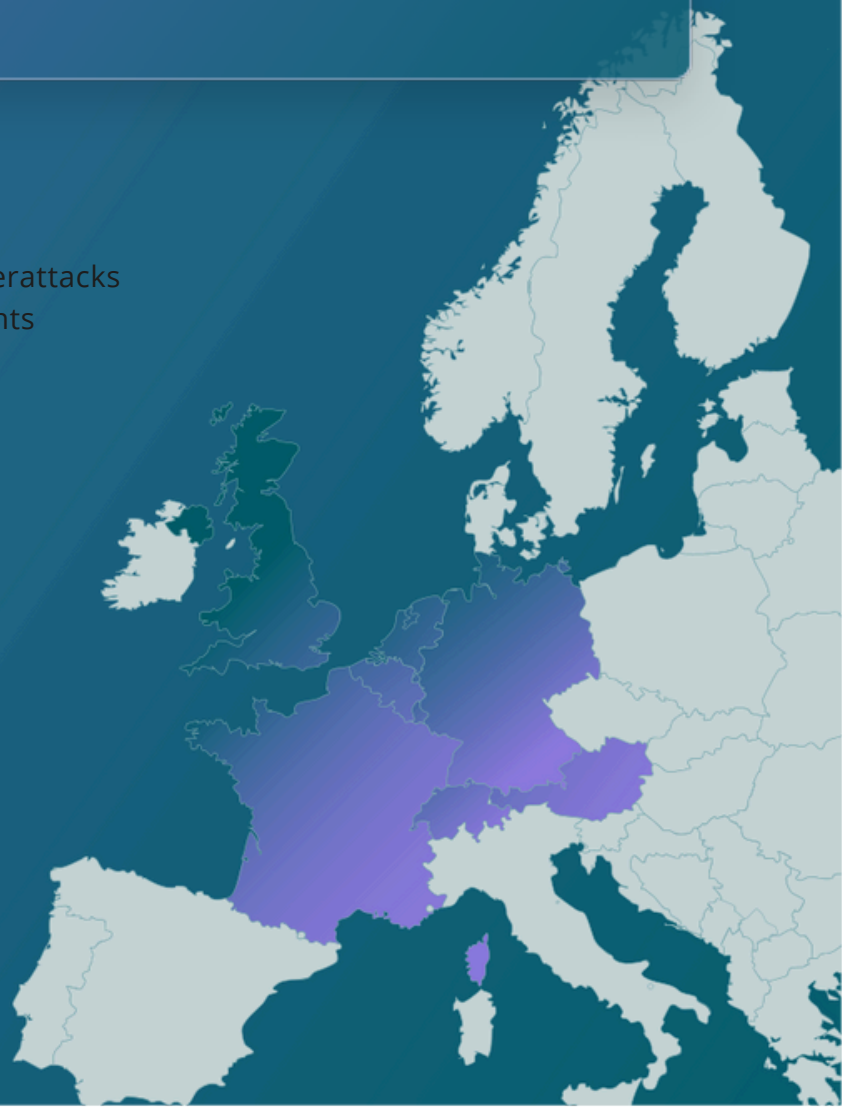
1 The Register (2024). Ransomware crooks now SIM swap executives' kids to pressure their parents.

Practical tips

- Train on both personal and work identities: Focus training on personal and work identities, highlighting attack tactics and consequences to help users understand their value to attackers in both roles.
- Extend training to families: Include families in training to protect their digital lives, as attackers may target relatives to access networks or extort employees.
- Extend technical protection to home devices and non-corporate hardware: Staff often use personal devices for work purposes, so consider partnerships with software vendors to achieve discounts on tools and controls that will enable them to be better protected, without increasing the burden on your security team to manage additional hardware.
- Ensure secure remote connections: Secure remote connections with MFA, VPNs, endpoint validation, and DLP to prevent accidental exposure of sensitive data outside corporate protection.
- Strengthen access controls: Operate under the expectation that breaches will happen and audit systems that safeguard sensitive data or operations. Maintain at least 12 months of logging and monitoring to trace employee activity if needed. Review and clean up password managers, eliminate shared accounts, and reinforce access protocols to minimize vulnerabilities.

Organizations that have experienced cyberattacks on employees' personal devices or accounts



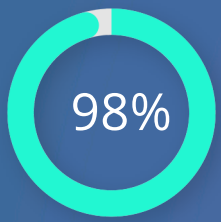


5 Cyber resilience inequality is putting essential services at risk

Critical sectors are fighting an uphill battle against cybercrime...

Security isn't equally accessible to everyone, and the gap in cyber defenses is growing wider. Highly regulated sectors – such as financial services – and large global corporations continue to strengthen their resilience, allocating significant financial and human resources and leveraging advanced technologies. Meanwhile, less regulated and resource-constrained sectors – such as critical infrastructure, healthcare, charities, manufacturing, and retail – struggle to keep up. Data from our internal Cybercrime Trends survey reveals that 98% of respondents believe this gap is widening, leaving these industries dangerously exposed to increasingly sophisticated cyberthreats. This imbalance is more than a technical issue – it's a systemic vulnerability that puts public welfare and economic stability at risk.

> The cyber security of critical infrastructure supply chains and the public sector must improve. There is a growing disparity between the resilience of our infrastructure and the threat we face.
>
> National Cyber Security Centre of the United Kingdom



of security professionals believe the gap in cyber defenses is widening.

...and hackers are exploiting the cracks in their defenses

Cyber resilience inequality stems from systemic challenges, with financial services benefiting from strict regulations and large corporations leveraging extensive resources for stronger defenses. In contrast, smaller organizations and sectors like critical infrastructure, healthcare, and manufacturing lack sufficient oversight and resources, leaving them more vulnerable to cyber threats.

Budget constraints, reliance on outdated systems, and limited leadership commitment further widen the gap. According to the World Economic Forum, over a third of small organizations (35%) believe their cyber resilience is inadequate – a sevenfold increase since 2022.1 The number is even higher when it comes to the public sector, with 38% of companies reporting insufficient resilience, compared to just 10% of private organizations.

The global shortage of cyber security professionals adds to the problem, allowing well-funded sectors to attract top talent while under-resourced organizations struggle to secure the expertise needed to counter modern threats. As highlighted before, public sector organizations continue to suffer the most, with 49% reporting a lack of the talent needed to meet their cyber security goals — a 33% increase from 2024.1 These vulnerabilities make less mature sectors increasingly attractive targets for cybercriminals and state-sponsored hackers and underscores the escalating risks to essential services and public safety. Bridging this gap has never been more urgent.

Practical tips

- Adopt recognized frameworks to stay ahead of threats: Adopt recognized frameworks like ISO 27001 and NIST CSF as your strategic foundation, regardless of regulatory requirements.
- Collaborate with regulators: Work proactively with your industry's regulators to develop practical guidelines that can benefit the wider industry and promote collective security.
- Hold other departments accountable: Security teams shouldn't bear the burden of inefficiencies in other functions. Ensure OS patching, code hardening, and legacy system deprecation are owned by the appropriate teams, with clear accountability for addressing the risks they create.
- Learn from mature industries: Network with organizations in highly regulated sectors to understand how they design resilient controls and adapt lower-cost alternatives that fit your industry's needs.
- Build diverse talent pipelines: Partner with universities and technical schools in underrepresented areas to create internships and apprenticeships that attract diverse cyber security talent.
- Make strategies accessible to all teams: CISOs in less regulated industries and smaller companies should ensure cyber security strategies are clear and actionable, enabling less technical teams – such as blue-collar workers – to actively contribute to defense efforts.

1 World Economic Forum (2025). Global Cybersecurity Outlook.

6 The boom of cybercrime

Cybercriminals are exploiting global connectivity to fuel their operations...

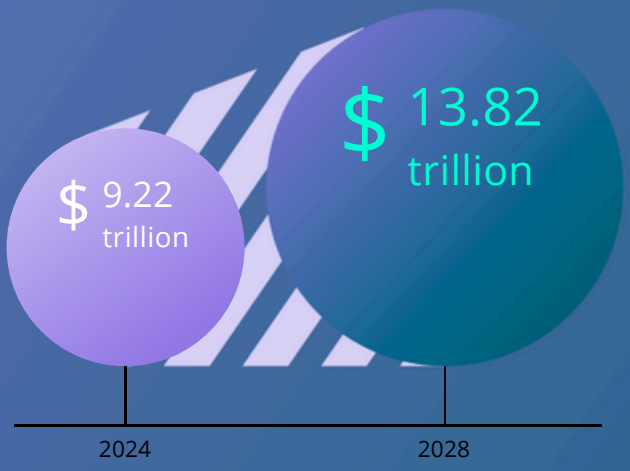
Cybercrime has transformed into a highly organized, global industry, thriving on society's growing reliance on technology. The rapid rise of remote work, the explosion of connected devices, and the adoption of new technologies such as AI, IoT, and cloud environments have massively expanded the attack surface, giving cybercriminals more ways than ever to infiltrate systems. Every sector and individual are now part of an interconnected digital web, where a single attack can send shockwaves across businesses, industries, and entire communities. The financial stakes are enormous – global cybercrime costs are projected to hit $10 trillion this year.1

However, what drives this booming market is not just its scale, but the methods cybercriminals use to make it so profitable. They have mastered precision, coordination, and adaptability, often targeting high-value individuals and organizations in jurisdictions with weak cybercrime enforcement to reduce their risk of prosecution and maximize their profit. To execute these crimes on a global scale, they leverage global online platforms like Telegram – with its vast and minimally moderated channels – to coordinate cross – border attacks. The professionalization of cybercrime, through services like ransomware-as-a- service (RaaS), has also greatly increased the profitability of the cybercrime market by lowering the barrier to entry. This model extends to a broader cybercrime-as-a-service ecosystem that offers malware kits, phishing templates, and Distributed Denial of Service (DDoS) attack tools to aspiring or inexperienced cybercriminals.2

...and global collaboration is key to containing these threats

The cost of cybercrime is already projected to climb from $9.22 trillion in 2024 to $13.82 trillion by 2028, and without immediate action, it will only continue to spiral.1 Combating this growing threat requires more than individual initiatives — it demands collective effort. Collaboration between organizations, industries, and governments is essential to share threat intelligence, establish unified defense strategies, and close enforcement gaps that cybercriminals exploit.

Projected cost of cybercrime



1 Statista (2024). Cybercrime Expected to Skyrocket in Coming Years.
2 Europol (2024). Cyber-attacks: the apex of crime-as-a-service.

> Collaboration between the private and public sector is essential. As it's usually said, 'it takes an international network to defeat an international network'.

Philipp Amann
Group CISO,
Österreichische Post AG

Practical tips

- Recognize and prioritize your expanding attack surface: Understand which elements are under your control – and which aren't. Focus on technical, people, and third-party risks by applying the right scrutiny, due diligence, and resources based on your specific threat levels.
- Simplify for agility and lower cost: Each new layer, process, or system increases operational complexity and makes responding to threats more cumbersome. Consolidate vendors and systems where possible, and work with business units to ensure they maintain the same focus on streamlining.
- Strengthen operational resilience: Partner with business process owners to ensure they can continue critical tasks even in the face of a cyberattack – including offline methods like pen-and-paper workflows. This ensures your organization can always deliver a minimum viable service or product.
- Hold other departments accountable: Security shouldn't carry the weight of poor quality control across the organization. Escalate concerns so that OS patching, code hardening, and legacy system deprecation are owned by the right teams, holding them accountable for addressing the risks they create.

Cybercrime Trend Resilience Matrix

How ready is your organization to face today's cyber threats?

This Cybercrime Trend Resilience Matrix provides a clear benchmark to help you understand your organization's level of preparedness against key cybercrime trends. It outlines the critical steps you need to move from a reactive security posture to a fully resilient one.

	Level 1 - Reactive	Level 2 - Proactive	Level 3 - Resilient
AI as an attack surface	Basic 'don't use' or 'take care' policy regarding AI use. Internal AI tools lack security controls. AI-driven threats (deepfakes, phishing) are not monitored.	AI governance committee in place; associated risks are documented and acknowledged. AI risk managed through limiting AI data access; some prompt controls exist to remove obvious malicious intent. AI-driven threats are monitored occasionally.	AI security is fully integrated into the development and maintenance lifecycle. Strict data access controls; output monitoring and continuous AI threat surveillance. AI-specific employee training and risk assessments.
Multichannel attacks	Security focuses mainly on email. SMS, voice, and social media attacks are addressed only through policy and education. No response plan for multichannel threats.	Some monitoring of SMS, collaboration tools, and social media. Detection exists, but responses vary across channels. Employees receive limited multichannel phishing training.	A unified defense strategy covering all attack channels. Proacvtive monitoring across email, SMS, and social platforms. Regular personalized employee simulation on multichannel threats.
Supply chain and third-party risk	Lack of certainty of 100% 3rd party coverage Vendor security limited to compliance checklists. No tracking of fourth-party risks. No structured response to vendor breaches.	Vendors are assessed, but third-party risks remain unclear. Security requirements for suppliers, but enforcement and oversight are weak. Incident response includes vendor breaches but lacks formal processes.	Regular third-party risk assessments, with testing and audit commensurate with the associated risk/ dependency. Security requirements embedded in vendor contracts, including 'cascade-down' requirements where essential. Fourth-party risks considered, assessed and managed. Clear contingency plans for supply chain attacks. Suppliers involved in business continuity rehearsal scenarios.

	Level 1 - Reactive	Level 2 - Proactive	Level 3 - Resilient
Threats to personal identities	A Basic training on social engineering tactics. A No security measures for employee personal accounts. A Non-work identity-based threats are not a priority.	A Workplace awareness training, but no structured protections for personal identities. A Employees are encouraged, but not required, to secure personal accounts. A Focus applied to protecting non-work identities of executives and Board members only.	A Specific program of awareness extends to personal identity and device protection. A Strong protections for executive and employee identities. A Regular monitoring for compromised credentials.
Cyber resilience inequality	A Minimal cyber security investment. A Compliance is perceived as an annoying goal. A Security decisions are reactive.	A Security measures exist, but funding and leadership support are limited. A Regularly compliant with necessary standards. A ISO27k used as a target operating model; or implemented for limited scope. A Cyber security strategy exists but is short term. A Incident response plans are untested or informal. A	A Security is a strategic priority with dedicated resources. A Certified to ISO27k for the majority of important systems. A Engage with industry regulators to craft and evolve regulatory requirements. A Leadership actively supports cyber security initiatives. A Resilience strategies are tailored to business needs.
The boom of cybercrime	A Threats are handled reactively. A Threat and cybercrime trend intel comes from mainstream press. A No long-term adaptation strategy.	A Cybercrime trends are tracked, but responses focus on immediate threats. A Some intelligence gathering and sharing, but limited adaptation to emerging tactics. A Employees are informed of trends but not regularly trained.	A Personalized threat intelligence services actively inform security strategy. A Continuous adaptation to emerging cybercrime tactics, techniques and procedures (TTP). A Awareness of criminal TTP is part of company culture.

Want to assess your organization's readiness?

Use our assessment to get a personalized evaluation of your organization's security posture.

Test your readiness

The “cyber maze” keeps shifting — but there’s a way out

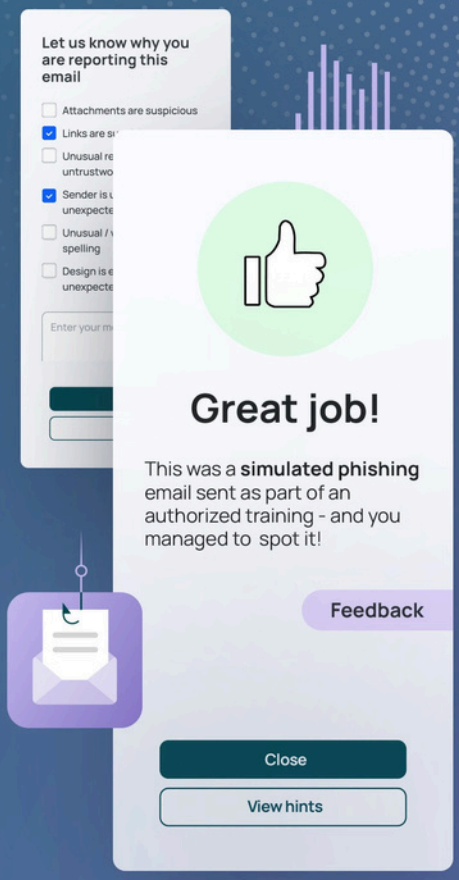
The report has shown how threats have become a labyrinth of ever-shifting tactics – just like our cover, where attackers move quickly, exploiting AI, supply chains, and personal identities to breach organizations from every angle. The attack surface keeps expanding, and with it, the challenges of staying secure. But while the threats are growing in scale and sophistication, we are not lost.

The path forward lies in collaboration and innovation. Organizations must come together, sharing intelligence and strengthening defenses across industries. AI, though a tool for attackers, also holds immense potential to enhance security — detecting threats faster, automating defenses, and improving response times. But technology alone is not enough. Having a strong security culture in place ensures that every individual, from employees to executives, becomes an active defender against cyber threats.

Our mission is to help you get there — sharing best practices from security experts and developing solutions that empower your organization to become cyber resilient. In an era shaped by AI-driven attacks, growing digital interconnectivity, and an increasingly complex threat landscape, we are here to remind you that there is a way out.

The cyber threat landscape is challenging – staying secure doesn't have to be

In a world where AI-powered attacks, multichannel deception, and supply chain vulnerabilities are evolving fast, a smart approach to human risk management is essential to recognize, disrupt, and prevent threats before they escalate.



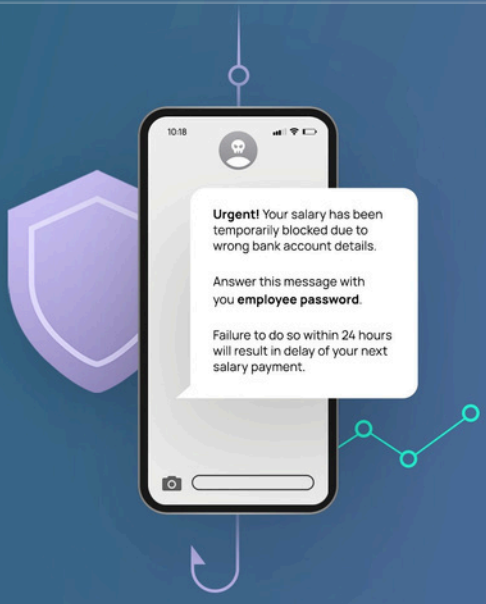
1 Turn AI into an ally and give your security team time to focus on what matters

Sofie AI Security Copilot: Our conversational AI chatbot provides real-time security guidance, instant interventions, and micro-learning on new threats.

AI-powered simulations: Automate the creation and deployment of realistic phishing simulations across email, SMS, and voice channels.

Simulation Studio with AI: Use AI to generate adaptive phishing templates, reducing manual effort and keeping simulations relevant to current threats.

Behavior-based simulations: Adjust phishing email frequency and difficulty to match individual risk levels with our AI-powered simulations.



2 Tackle phishing on every front without extra workload

Vishing protection: Train employees to identify and respond to phone-based phishing attempts that exploit trust and urgency.

Smishing defense: Simulate SMS-based phishing attacks to prepare employees for fraudulent messages and mobile-based malware threats.

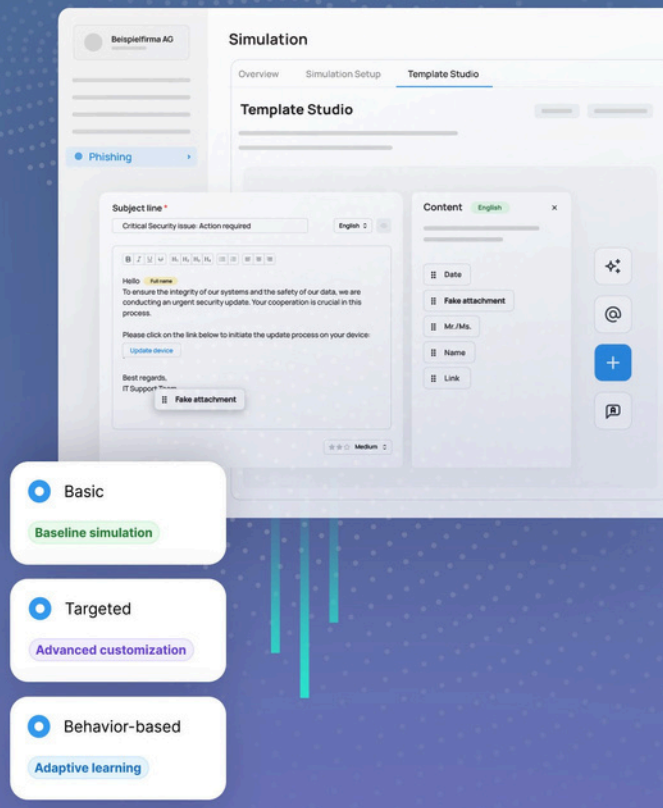
3 Create security awareness at work, home, and everywhere in between

Personalized micro-learning: Our micro-learning solution delivers targeted training based on user behavior, risk profile, and learning needs.

Targeted simulations: Customize phishing emails to address the specific risks of each of your employees, no matter their role.

Training beyond the workplace: We train employees on personal and professional security scenarios that help employees recognize threats beyond the workplace.

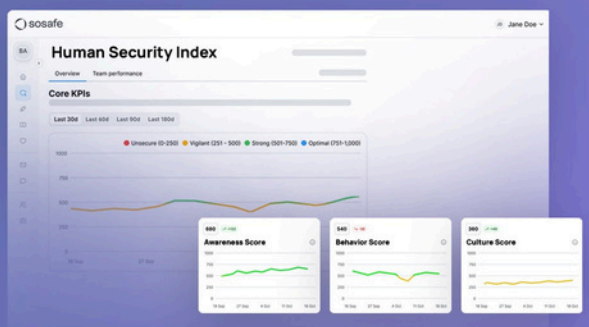
Awareness training for family and friends: Extend cyber security awareness training beyond employees by providing basic learning opportunities to their family and friends.



4 Stop guessing – use data-driven insights to make smarter security decisions

The Human Risk OS: Our Human Risk Operating System transforms security awareness into proactive risk management. It continuously analyzes behavioral patterns, monitors risk signals across multiple sources, and delivers automated, targeted interventions to address emerging threats before they escalate.

Phishing Report Button: Enables employees to report suspicious emails, providing security teams with real-time insights to detect threats and respond faster.



5 Stay secure no matter where you are in your security journey

Audit and compliance readiness: For organizations establishing their security foundation, we help you meet global and industry-specific standards with assessments, compliance frameworks, and awareness programs to meet industry standards and strengthen baseline defenses.

Personalized security and behavioral change: As organizations advance in their security journey, we personalize security training and interventions to embed a culture of security awareness and behavior change in your organization.

Proactive risk management: For advanced security programs, we enable data-driven, proactive risk management by leveraging behavioral analytics, human risk insights, and adaptive security measures to stay ahead of evolving threats.

Contact

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

ITB Ltd - solutions@it-b.co.uk
www.it-b.co.uk
01865 595510