Investing in cybersecurity for a secure and resilient digital future

Summa report in the tech-enabled
resilience series

Investing to solve
global challenges

SUMMA EQUITY

About this report

Thank you for reading Summa's report on investing in cybersecurity for a secure and resilient digital future. This report examines the growing threat of cyberattacks, their economic and societal costs, and the specific capabilities and innovations needed to defend against them. It also connects systemic challenges and market dynamics with opportunities for high-impact investment. We hope that this report serves as an informative resource, and encourages further discussion and collaboration among stakeholders.

Thanks to

The Center for European Policy Studies (CEPS)

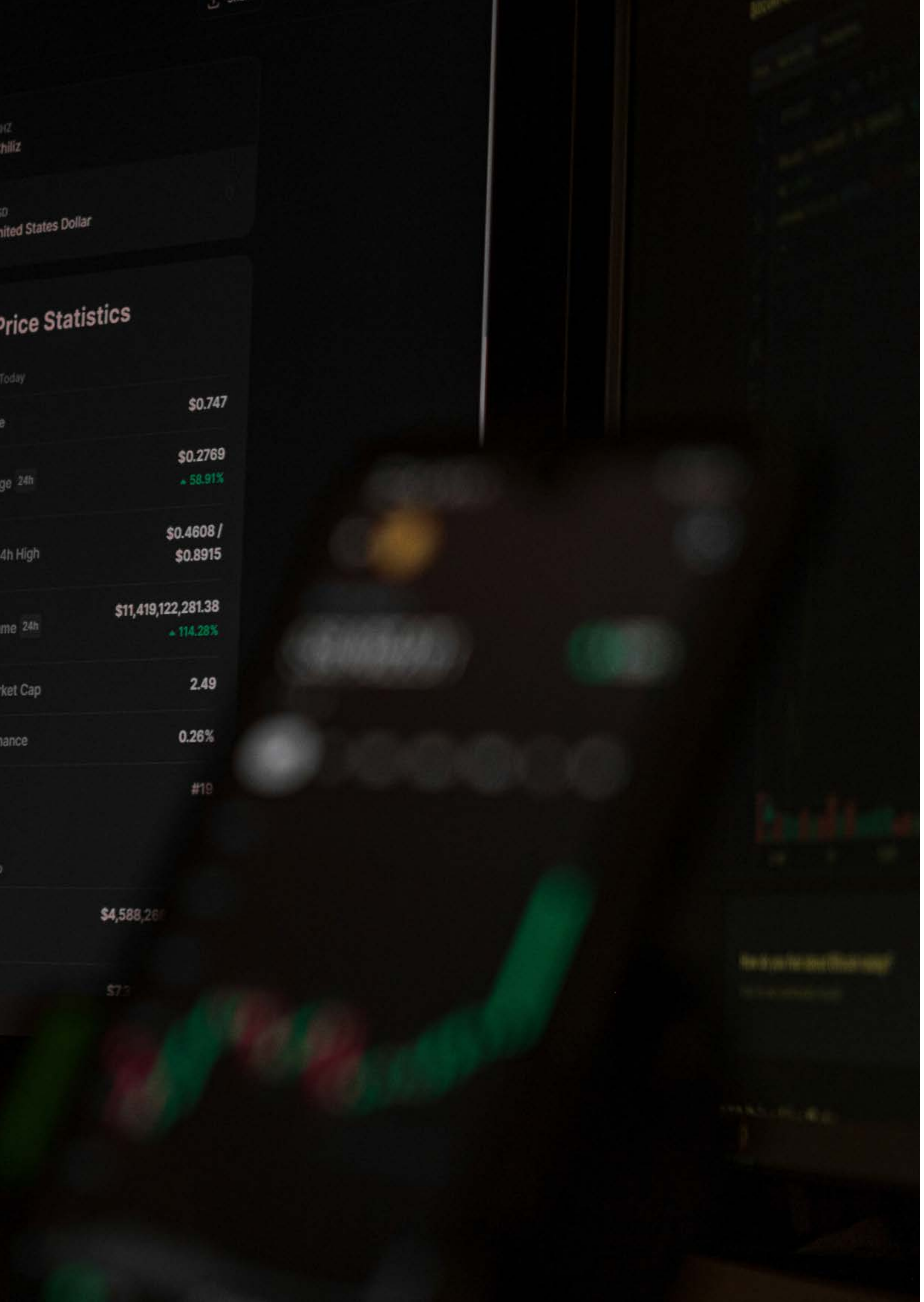
Images

Shutterstock, Unsplash, Fast LTA

Disclaimer

The content draws on and references the latest insights in cybersecurity. This includes Summa internal analysis and work completed by the Center for European Policy Studies (CEPS), specifically the "cybersecurity @CEPS" initiative.

Table of contents



Executive summary

Digitalization has revolutionized economies and societies, but its rapid expansion now exposes critical systems to escalating cyber threats that jeopardize trust, security, and global progress.

Digitalization has transformed how we work, trade, socialize, and govern, driving innovation, productivity, and inclusion in the process. The ICT sector now contributes over USD 6.1 trillion to global GDP and is growing twice as fast as the global economy.[1] This progress comes with a rising cost. As cyberattacks multiply, losses per incident soar, and total annual damage equals about 3% of GDP in advanced economies.[2]

What began as isolated attacks has evolved into highly sophisticated and coordinated operations that threaten the essential systems societies depend on.[3] Malicious actors ranging from organized crime groups to state-backed hackers have turned digitization into a double-edged sword. The systems that also power smart grids, automated factories, precision agriculture, and digital governance now leave societies exposed to theft, manipulation, and disruption.

At Summa, we believe the future of cyberspace can and must be safer and more resilient. Shared norms, credible deterrence, and strong cybersecurity practices can prevent malicious activities. Our goal is a digital environment where people and organizations can operate with confidence, knowing that information, products and services provided in and through cyberspace remain reliable and secure at all times.[4]

Achieving this requires overcoming significant challenges. Globally, defenders are falling behind. Most firms, particularly SMEs, lack core defenses, and several critical sectors have a high societal importance that far exceeds the maturity of their cybersecurity.[5] Overcoming this gap requires solutions that strengthen protection and address inefficiencies that are holding cybersecurity back.

That is why we have identified priority areas where investment can deliver strong returns along with measurable societal impact. These include identity and data security, security operations and services, and back-up & recovery. Summa investments in Logpoint delivers European-native threat detection and response, while FAST LTA provides secure data storage for critical sectors such as healthcare and government.

Cybersecurity is a shared responsibility and a unique opportunity. We hope this report inspires action, collaboration, and investment in building a safer digital future.

Christian Melby
Partner & CIO
Summa Equity

Jacob Frandsen
Partner
Summa Equity

Emelie Norling
Impact Director
Summa Equity

[1] (World Bank, 2024) [2] (Summa & CEPS Analysis) [3] (IMF, 2024a; Office for National Statistics (UK), 2020) [4] (Michael Chertoff, Latha Reddy, Marina Kaljurand, 2019) [5] (ENISA, 2024a)

A resilient digital future – Why cybersecurity can't wait

Digitalization has driven economic growth, innovation, and societal progress. Now it needs to become safe and resilient.

From the creation of APRANET in 1969 to the cyberspace we know today, digitization has created new jobs and industries, reshaped existing ones, increased access to essential services, and enabled more inclusive participation in economic and civic life.[6] Today, cyberspace is not just a technological domain, it is a foundational layer of modern society, underpinning how we relate to each other, govern, trade, and exercise fundamental rights.

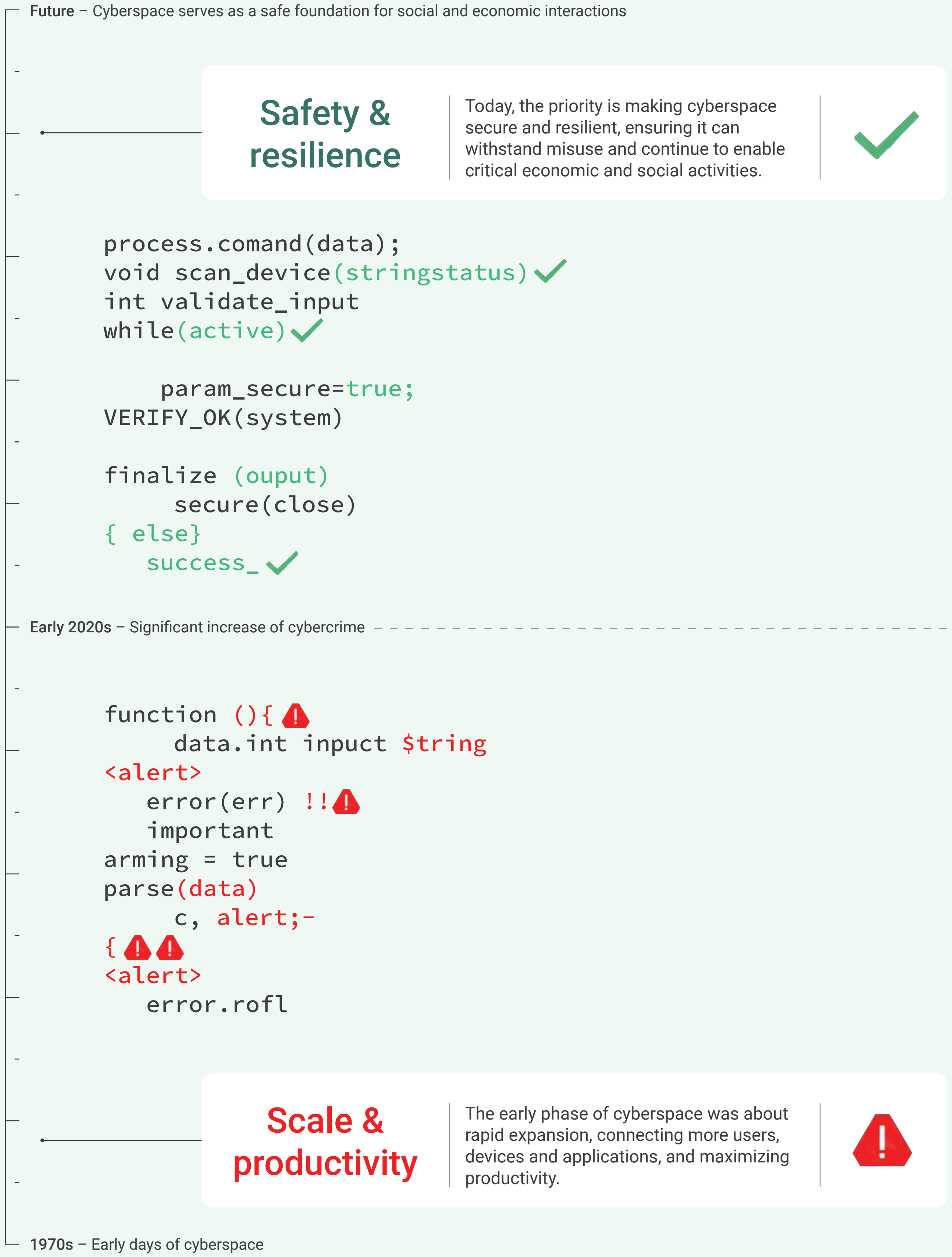
However, vulnerabilities that come with an open and shared digital infrastructure are now exploited at a scale that requires a renewed focus digital security. What began in the early 2000s as sporadic attacks by hackers has grown into a global cybercrime economy, driven by organized groups and increasingly supported by state actors. The frequency and severity of their attacks have grown sharply. Median losses from reported attacks have risen more than fifteenfold, and annual damage from cybercrime in advanced economies is estimated to equal 3% of GDP in advanced economies.[7] Most incidents still go unreported, masking the full scale of the impact.

This makes cybersecurity a societal priority and a central investment focus for Summa. The resilience of digital infrastructure is closely tied to the ability to progress on the most pressing global priorities: next-generation electricity grids for the energy transition, precision agriculture for sustainable food systems, smart factories for resource-efficient manufacturing, and connected healthcare for better patient outcomes. These transitions will link our physical and virtual worlds more closely than ever. Without adequate protection, the risk of attacks spreading from digital systems into the physical world will grow, increasing the chances of severe consequences.

Preventing those requires more than incremental improvements. Collective action is needed to establish shared norms, enforce credible rules, and strengthen defensive capabilities that can inhibit, deter, and preempt malicious activity. At Summa, we see this as both a responsibility and an investment opportunity. By advancing cybersecurity practices and scaling high-impact solutions, we aim to strengthen society's collective security while delivering attractive returns ensuring that digitalization remains a net-force for social progress.

[6] (European Commission. Joint Research Centre et al., 2020; UNESCO, 2019; United Nations, 2022) [7] Summa & CEPS analysis, 2025

Figure 01
The path to a resilient digital future: Early-phase initiatives and the priorities of today and in the future.



Future – Cyberspace serves as a safe foundation for social and economic interactions

Safety & resilience — Today, the priority is making cyberspace secure and resilient, ensuring it can withstand misuse and continue to enable critical economic and social activities. ✓

```
process.comand(data);
void scan_device(stringstatus)✓
int validate_input
while(active)✓

    param_secure=true;
VERIFY_OK(system)

finalize (ouput)
     secure(close)
{ else}
   success_✓
```

Early 2020s – Significant increase of cybercrime

```
function (){⚠
     data.int inpuct $tring
<alert>
   error(err) !!⚠
   important
arming = true
parse(data)
     c, alert;-
{⚠⚠
<alert>
   error.rofl
```

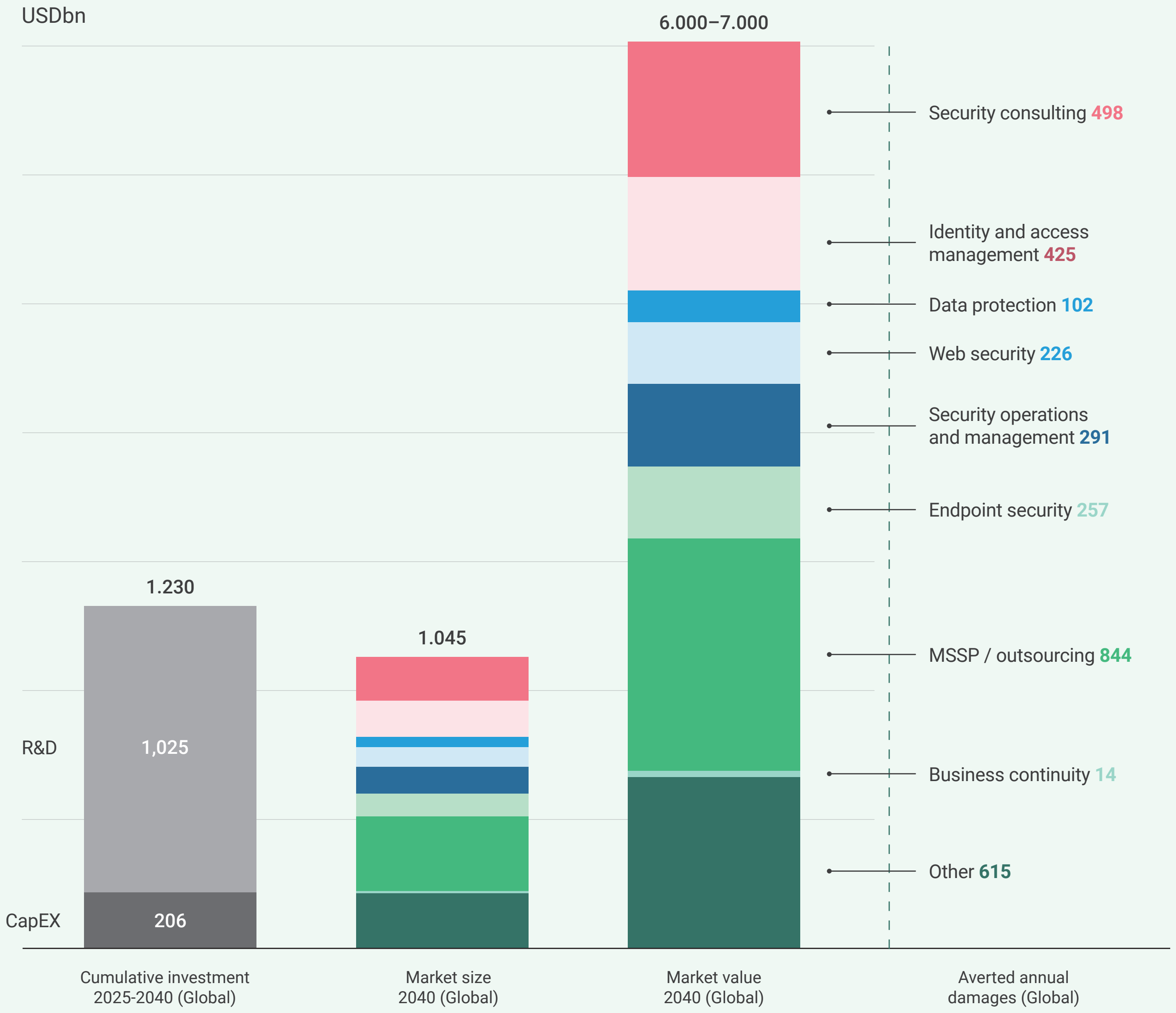
Scale & productivity — The early phase of cyberspace was about rapid expansion, connecting more users, devices and applications, and maximizing productivity. ⚠

1970s – Early days of cyberspace

Figure 02
Cumulative investment needs, market size and value of the global cybersecurity market and averted damages from cyberattacks.[8]

USD
>3.300bn
Averted annual damages from cyberattacks by 2040[9]

213%
Implied average return on security investments[9]



Note: Approximate return on security investment (ROSI) based off Forrester Total Economic Impact Reports (TEI) for multiple cybersecurity enabling solutions

[8] (MarketsandMarkets, 2025; McKinsey Global Institute, 2024; McKinsey & Summa Equity Analysis, 2022; PSMarketresearch, 2025) [9] Summa Equity Analysis,

Cybersecurity – The investment opportunity

We estimate that markets enabling a safer and more resilient digital future could grow more than fourfold to a market size of about 1 trillion by 2040 (c. 11% CAGR from 2025), reflecting the scale of investment organizations must make to strengthen their defenses.

In turn, the solutions and services delivered by these markets could avert more than USD 3.3 trillion in annual damages by 2040, protecting employees, shareholders, and end-users from harm.[10] These solutions will make workplaces safer, returns more predictable, and ensure the confidentiality, integrity and availability of information, products, and services provided in and through cyberspace.

Several forces are driving this growth. Expected losses from cyberattacks continue to rise. Regulators in Europe and elsewhere are tightening requirements and expanding liability. Litigation is increasing, reporting and transparency are improving, and end-user preferences are shifting toward greater security.[10] In return, global surveys show that most organizations expect their cybersecurity budgets to grow.[11]

Meeting this demand will require both innovation and significant capacity expansion across the cybersecurity industry. We estimate that reaching a market value of USD 6–7 trillion by 2040 will require approximately USD 1230 billion in cumulative R&D and capital expenditure over the next 15 years.

Summa contributes by backing cybersecurity solutions that address key capability gaps as well as systemic challenges that hold the industry back from realizing its full potential. These include scarcity of talent, fragmented point solutions, rapid obsolescence, weak quality signals, and perceived trade-offs against other desirable outcomes such as privacy and data sovereignty.

Our investment focus is clear. We target providers of identity & data security solutions (Identity and Access Management, data security, endpoint protection), security operation tools & security services (SIEM, SOAR, UEBA, XDR, MSSPs, security consulting) as well as back-up and recovery solutions.

We look for solutions that are certified best-in-class, automated or delivered as-a-service, consolidating and compliant. By scaling these capabilities, we aim to generate attractive financial returns while advancing societal resilience and ensuring digitalization remains a net positive force.

[10] (Summa Equity & CEPS Analysis) [11] (PWC, 2024)

Understanding cyberspace and the rise of cybercrime

Cyberspace: A foundational layer of modern life

Cyberspace is the digital environment where data moves across computer networks. It's build on a complex system of technologies that enable the storage, processing and exchange of data between humans, machines and automated systems.[12]

From ARPANET in the 1970s, cyberspace has grown exponentially in terms of users, connected devices and volume of data exchanged. In 2023, 92% of individuals in OECD countries used the internet, with global users expected to exceed 7.5 billion by 2030.[13]

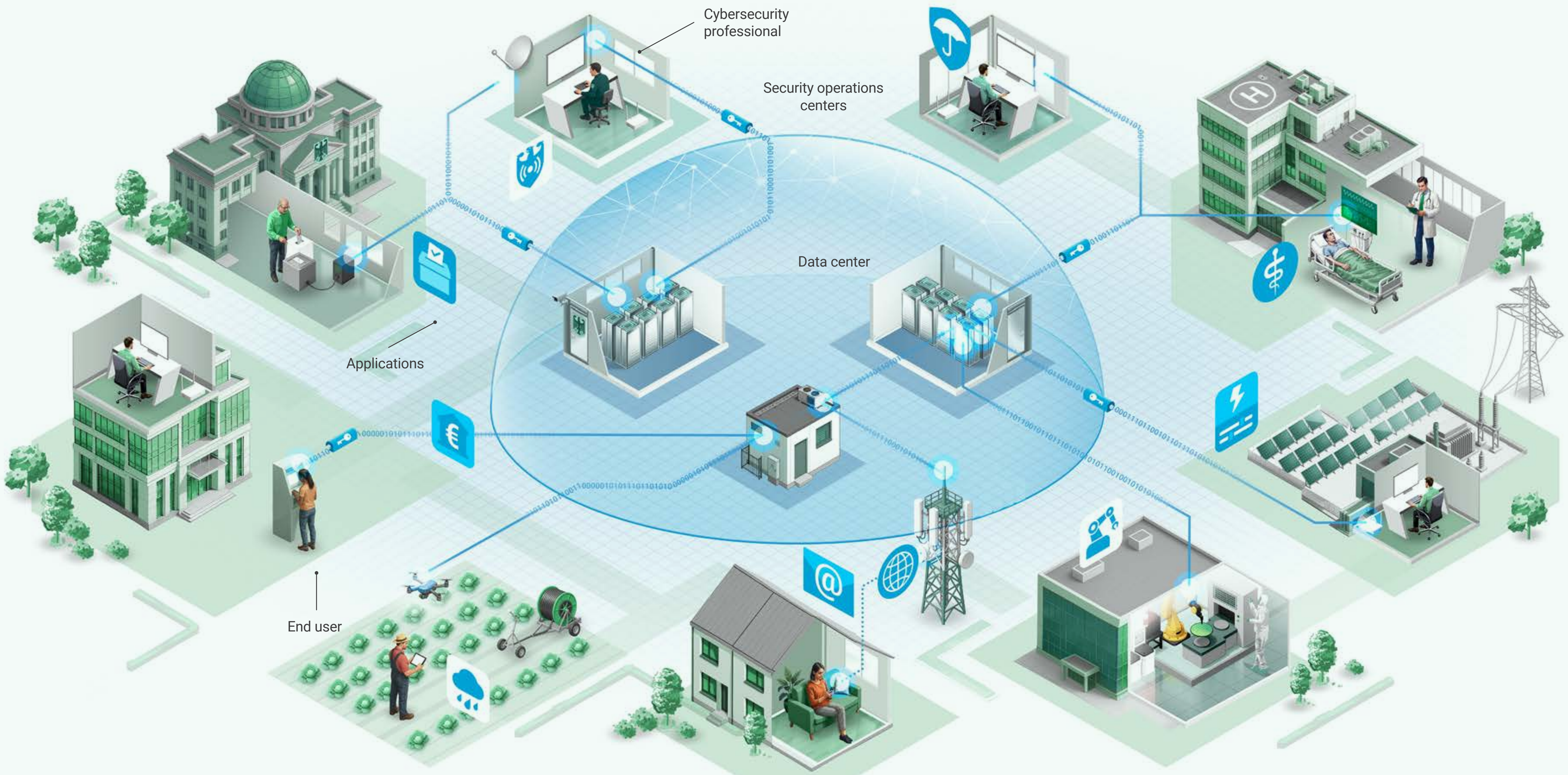
That same year, 29.3 billion devices were connected to networks, equal to about 3.6 per person. The total number is growing by around 10% each year.[14] Together, these devices exchange 7.3 zettabytes of data annually, with machine-to-machine communications already making up about half of all traffic.[14]

5.500m

internet users in 2022

12. (Biener et al., 2015; Oxford University Press, 2023) 13. (OECD, 2024) 14. (Cisco, 2024)

Figure 03
Cyberspace emerges from users interacting with applications running on computing systems connected via network infrastructure.



This aggregation of users, applications, devices, and infrastructure has created a vast network of social and economic relationships with great potential to enable human rights, empower individuals and communities and support sustainable development.[15]

Today, the global information and communications technology (ICT) sector contributes USD 6.1 trillion, about 6% of global GDP. Digital technologies are embedded across industries, from manufacturing and finance to healthcare and agriculture.[16] In the United States, the digital economy already accounts for more than 10% of GDP and 8 million jobs.[17] Research consistently finds that investments in ICT raise productivity and employment, narrow income gaps, and increase social mobility.[18]

Beyond its economic impact, an open, accessible and responsibly governed digital environment has transformed access to knowledge and essential services. It has enabled more inclusive public participation and supported fundamental human rights such as freedom of expression, association, and privacy.[19]

Crucially, it is also central to major transitions societies must deliver. These include smart grids and cross-border electricity networks to balance renewable power, digital platforms to drive circular resource use, precision agriculture to improve yields and reduce waste, connected healthcare to improve efficiency, and digital government to broaden inclusion.

While connecting users, devices, applications and machines through open and decentralized networks generated many benefits for society, it has also created new opportunities for misuse of our shared infrastructure. As dependence on digital information, products and services grows across essential economic, social and civic activities, addressing these vulnerabilities is becoming an urgent social priority.

Today, the global information and communications technology (ICT) sector contributes USD 6.1 trillion, about

6%

of global GDP

[15] (UNESCO, 2019) [16] (World Bank, 2024) [17] (BEA, 2022) [18] (Eynon et al., 2018; Houngbonon & Liang, 2017; OECD, 2012; Ryng et al., 2022; United Nations, 2022)
[19] (European Commission. Joint Research Centre et al., 2020; UNESCO, 2019; United Nations, 2022).

Cyberattacks: The dark side of connectivity

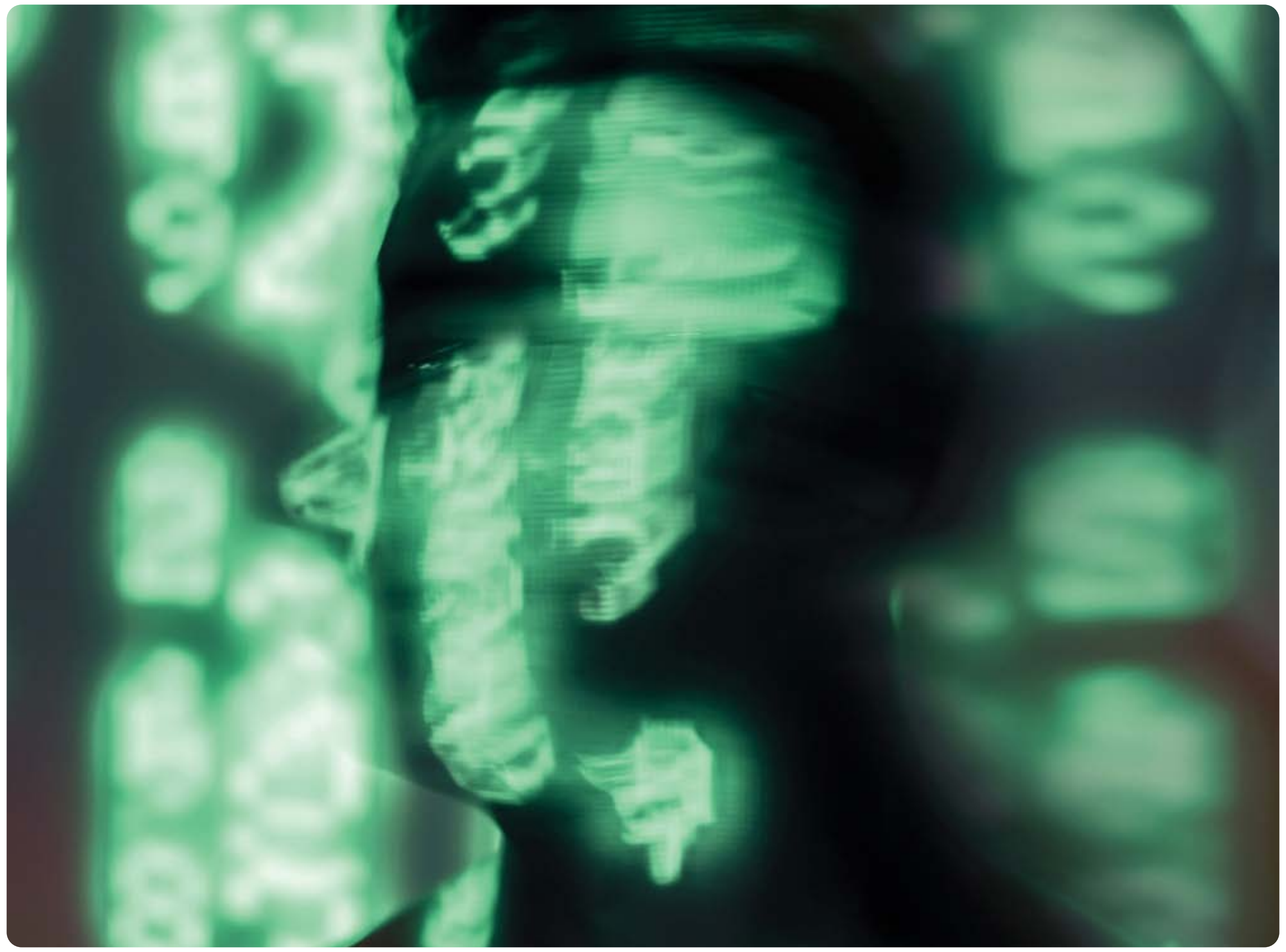
As more systems, services, and products rely on connectivity, the risk exposure grows. The rise of remote work, Internet-of-Things (IoT), cyber-physical convergence and increasingly complex supply chains generate more opportunities for exploitation by malicious actors than ever.[20]

Cyberattacks are cyber-dependent crimes. Unlike cyber-enabled crimes, where traditional offenses such as fraud, harassment, or disinformation are amplified through digital tools, cyberattacks are both executed through and directed against digital technologies.[21]

While cyber-enabled crimes pose serious societal challenges and demand tailored responses, this report concentrates on cyberattacks. These attacks directly undermine the confidentiality, integrity, and availability of digital assets, products and services. By striking at the core infrastructure of the digital economy, they create the potential for cascading disruption across industries and societies, making them the most pressing of digital threats.

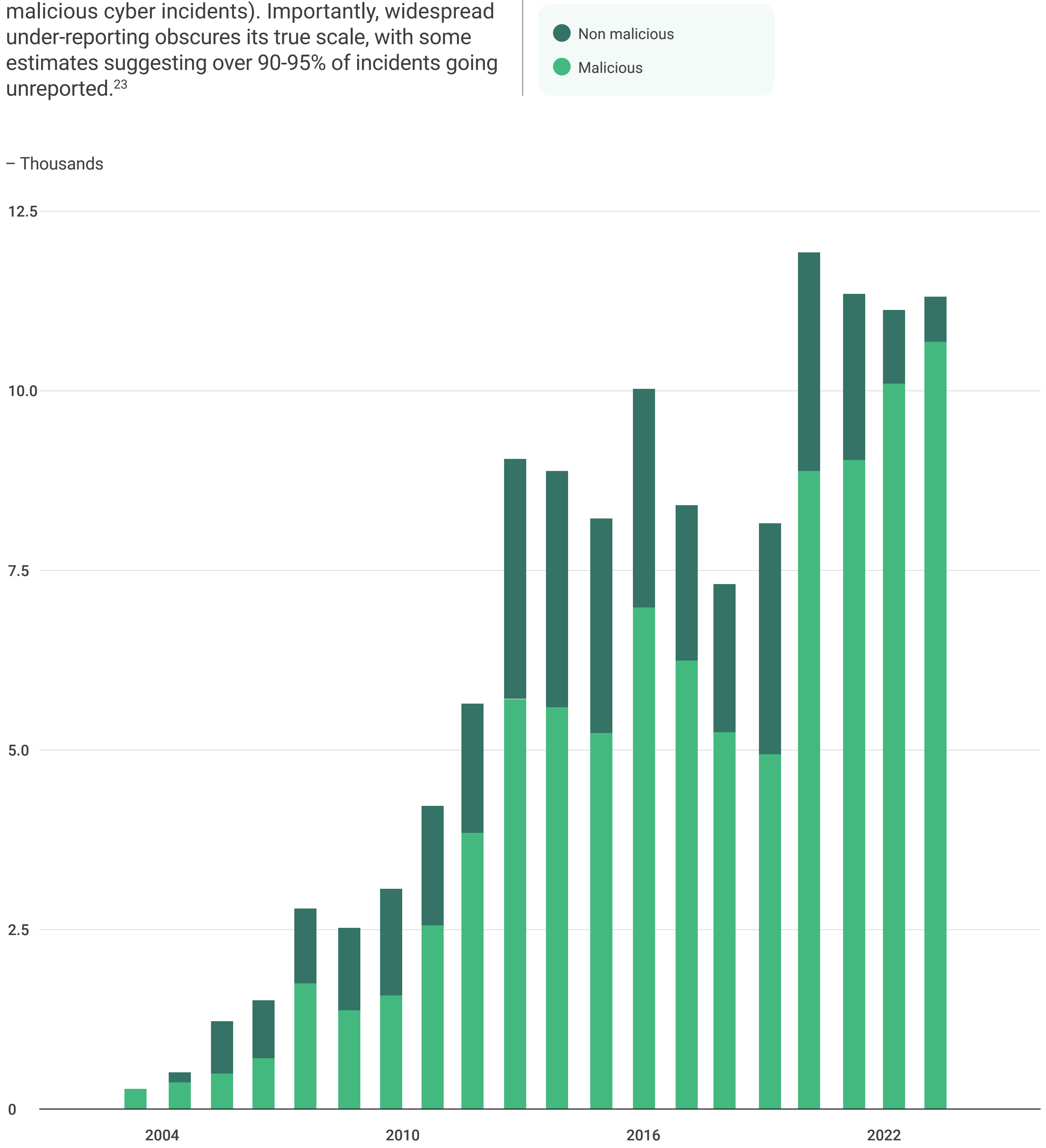
90-95%

of incidents go unreported



Reported cyberattacks have increased sharply since the early 2000s, growing at an estimated global CAGR of 10% since 2004[22] and peaking during the initial phases of the Covid-19 pandemic (see Figure 4, malicious cyber incidents). Importantly, widespread under-reporting obscures its true scale, with some estimates suggesting over 90-95% of incidents going unreported.[23]

Figure 04
Number of cyber incidents recorded in Advisen Cyber Loss Database over time, noting a significant increase in malicious incidents (IMF, 2024).



Escalating financial impact of cyber incidents (2008–2024)[24]

Increase in 50th percentile losses	Increase in 90th percentile losses
15.5x	4.75x

[20] Summa & CEPS analysis, 2025 [21] (CPS, 2018; NIST, 2020)

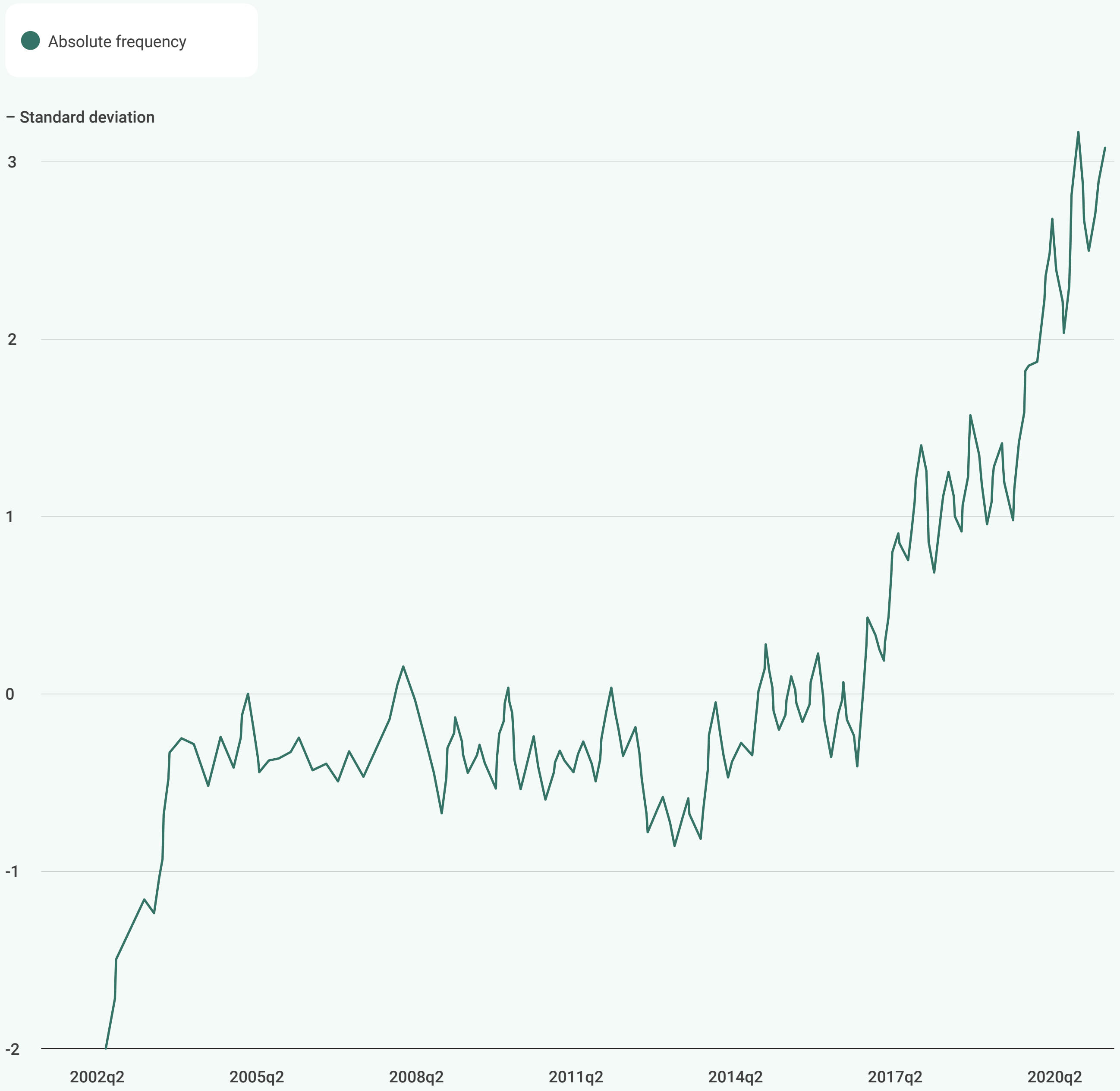
[22] (IMF, 2024a) [23] (Office for National Statistics (UK), 2020; Verleysen, 2016) [24] (Cyentia Institute, 2025)

The severity of cyberattacks has also increased. Median losses per incident are now more than 15 times higher than before, while extreme losses at the 90th percentile are about five times higher. Losses have now reached levels that can create funding pressures for organizations and, in severe cases, threaten their ability to remain financially viable.[25] These figures only reflect part of the picture. They do not yet capture the wider effects on employees, shareholders and end-users, which means the real impact of cyberattacks is still underestimated.

The magnitude of this threat is reflected in rising public concern. Cyber-risk has moved from a niche issue to a boardroom priority. Mentions of cyber-risk in public earning calls have increased sharply since 2017 (see Figure 5).

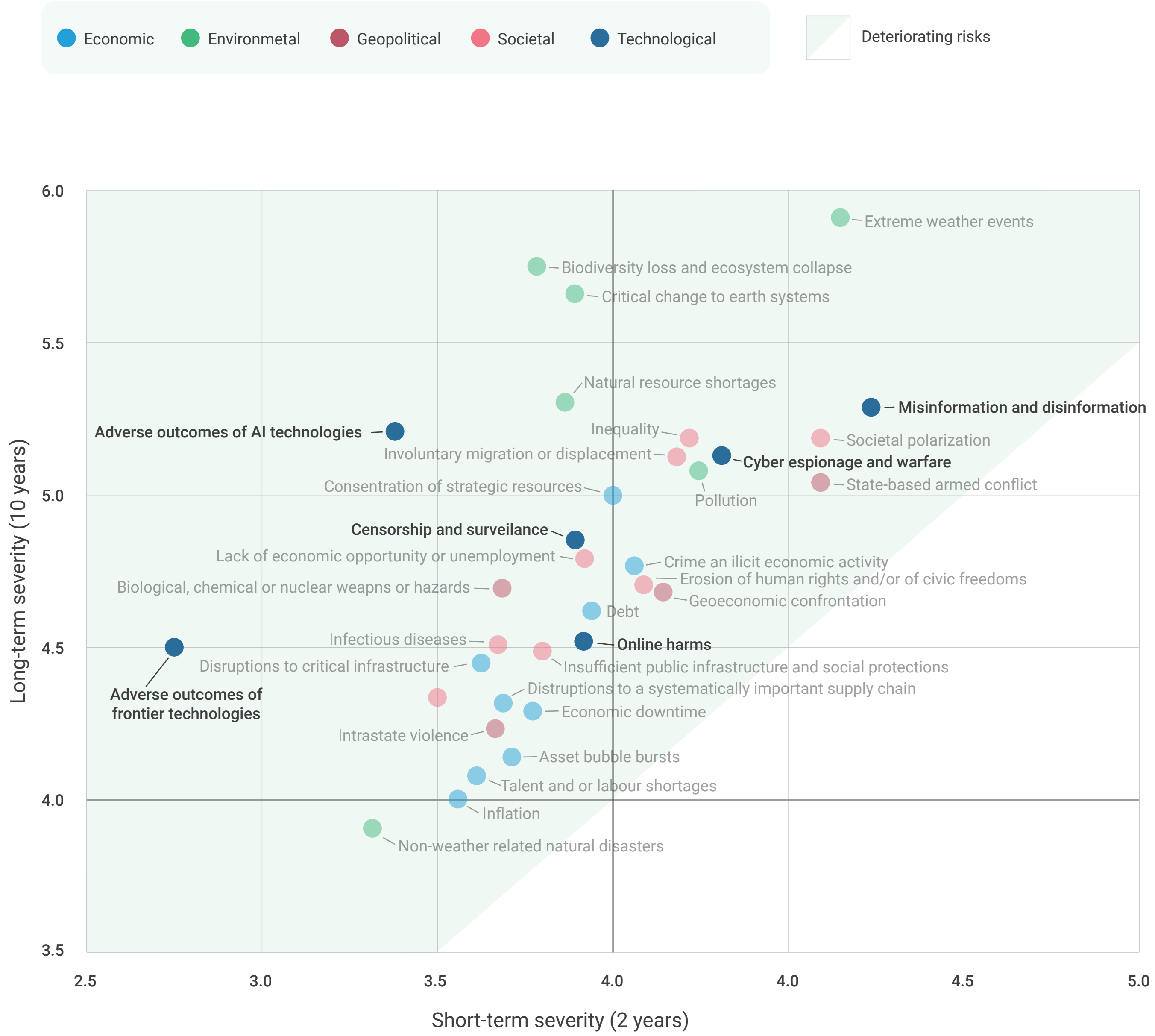
By broad expert and business consensus, cyber espionage and warfare now rank among the top eight global risks, with the highest perceived severity in both short term (2 years) and long term (10 years).[26] The European Union Agency for Cybersecurity[27] also rates the threat to essential and important entities as substantial, realistic and serious.[28]

Figure 05
Concern among shareholders about cyberattacks reflected in increasing frequency of cyber-risk being mentioned in earning calls (Q2 2002-Q2 2022)[29]



[25] (IMF, 2024b) [26] (World Economic Forum, 2025) [27] (ENISA) [28] (ENISA, 2024a) [29] (Jamilov et al., 2021).

Figure 06
Relative severity of cyber risks short and mid-term, assessed on a 1-7 Likert scale (1 = Low severity, 7 = 7 High severity)[30]

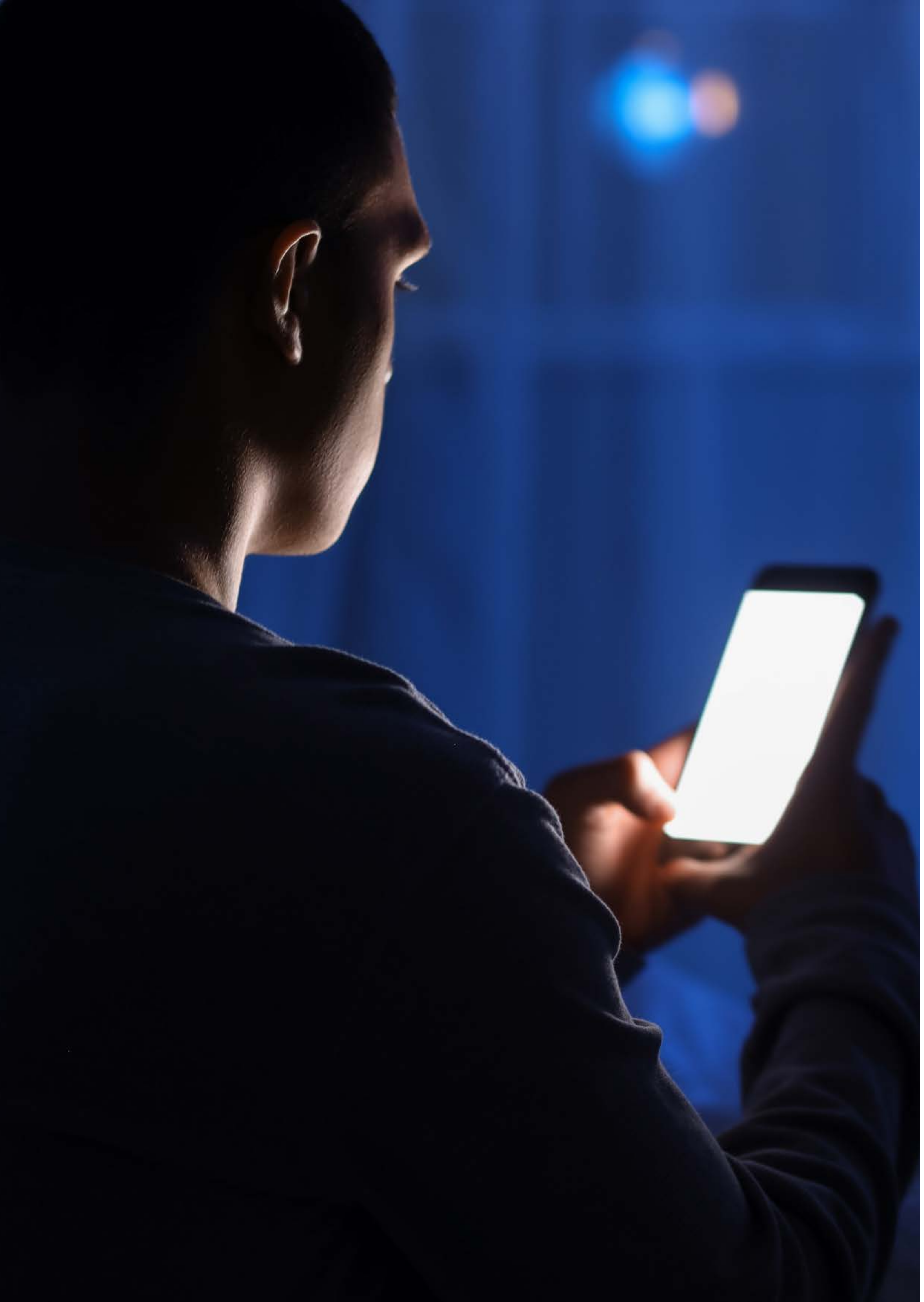


1	IT	24%
2	Education & research	21%
3	Goverment	12%
4	Think tanks & NGOs	5%
5	Transportation	5%
6	Consumer retail	5%
7	Finance	5%
8	Manufacturing	4%
9	Communications	4%
10	All others	16%

Figure 07
Critical industries are increasingly facing cyber threats, many of which are ranking among the top 10 most targeted sectors globally.[31]

Few organizations can consider themselves safe. Cyberattacks affects all sizes and sectors. In 2024, Microsoft reported that IT companies (24%), education and research institutions (21%), and government agencies (12%) were among the most affected. Healthcare providers, manufacturers, and financial institutions are also increasingly targeted.[31]

[30] (World Economic Forum, 2025). [31] (Microsoft, 2024)



Beyond the breach – The true cost of cyberattacks

Cyberattacks affect both systems and the people who rely on them.

Their immediate effects include the disclosure, alteration, or denial of information, products, or services provided in and through cyberspace. The most commonly reported damages are financial losses such as ransom payments, legal fees, operational disruptions, and higher compliance and insurance costs. These figures only capture part of the overall impact.

The broader consequences of attacks are best captured by the concept of cyber-harm: the material or immaterial impairment of a person's physical, financial, psychological, or social well-being from cyberattacks.[32] While cyber-harm can only be experienced by natural persons, this does not mean that attacks against organizations are harmless. On the contrary, when enterprises or public institutions are compromised, their losses result in indirect harm for employees, shareholders, end-users, and society at large.

Crucially, cyber-harm is not confined to the immediate aftermath of an attack. It can happen in the anticipation of an attack, as a consequence of it, and in the response that follows.[33] In the anticipation phase, individuals and organizations spend resources or miss opportunities as they work to avoid or defend against attacks. In the consequence phase, breaches materialize as disclosure, alteration, or denial of information and services. In the response phase, victims spend more time and resources on recovery and rebuilding. Together, these dimensions provide a more nuanced picture of who suffers from cyberattacks and how.

Private individuals bear harm throughout. In anticipation, some avoid services such as online banking or digital health records for fear of attack, while others invest time and money in defensive measures. When an attack happens, they may lose savings, suffer disclosure of sensitive data, or lose access to essential services. In response, they face long recovery times. This includes remediating stolen identities, resetting accounts, and coping with ongoing psychological stress and fear of revictimization.

Organizations also suffer losses that can cause harm for their stakeholders. In anticipation, they may scale back or delay digital initiatives, slowing innovation as perceived risks may outweigh its benefits. When incidents occur, they face ransom demands, theft of data or intellectual property, operational disruption, reputational damage, and regulatory scrutiny. In the response phase, the resources spent on forensics, insurance, and system rebuilds divert capacity away from growth and service delivery, affecting employees, customers, and shareholders.

Employees and shareholders suffer from these losses indirectly. Anticipation may bring heightened stress or training burdens as staff adapt to security protocols. Consequences can include layoffs, unsafe working conditions where productions systems are compromised or diminished dividends as companies absorb losses. In response, employees may lose trust in their workplace, while investors may see long-term value erode.

End-users suffer indirectly as well. Anticipatory harm may mean uneasiness about adopting digital services or higher prices as security costs are passed on. Consequence harms are most visible in outages and disclosures. Patients may be unable to access clinical systems, commuters stranded by disabled transport, or data breaches exposing private information. In recovery, many may need to cut their losses, change providers, or accept exclusion from digital platforms.

[32] (Agrafiotis et al., 2018; Ignatuschtschenko et al., 2016) [33] (Weber, 2024; Wright & Kumar, 2023)

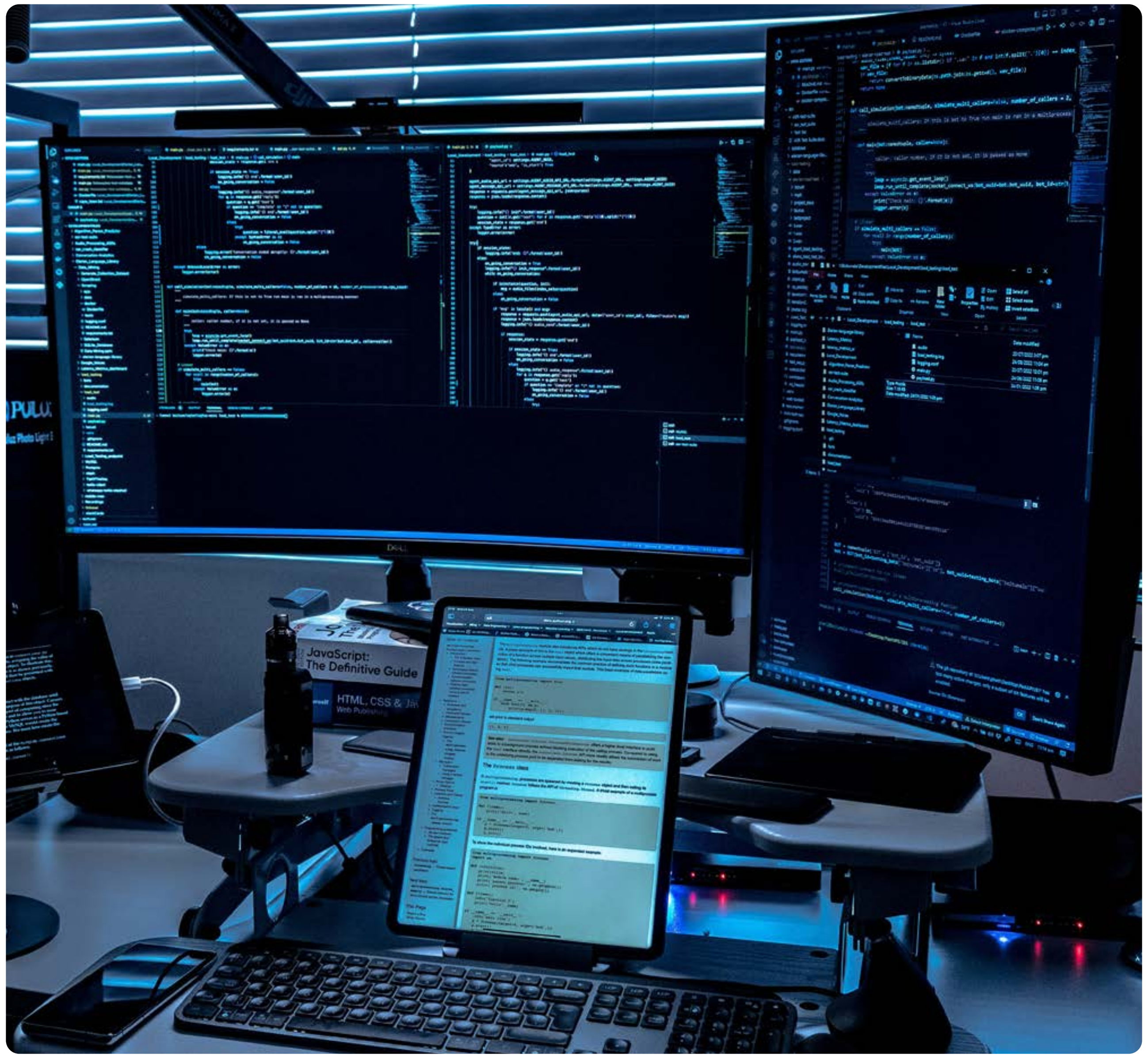
Research suggest annual material harm equals about

3%

of GDP in advanced economies

Finally, society absorbs the ripple effects. Anticipation creates heightened collective anxiety and digital exclusion, as people avoid participation. Consequences include disruptions to critical infrastructure, services or democratic processes. In response, trust erodes as repeated attacks weaken institutional credibility and reduce public willingness to rely on digital systems.

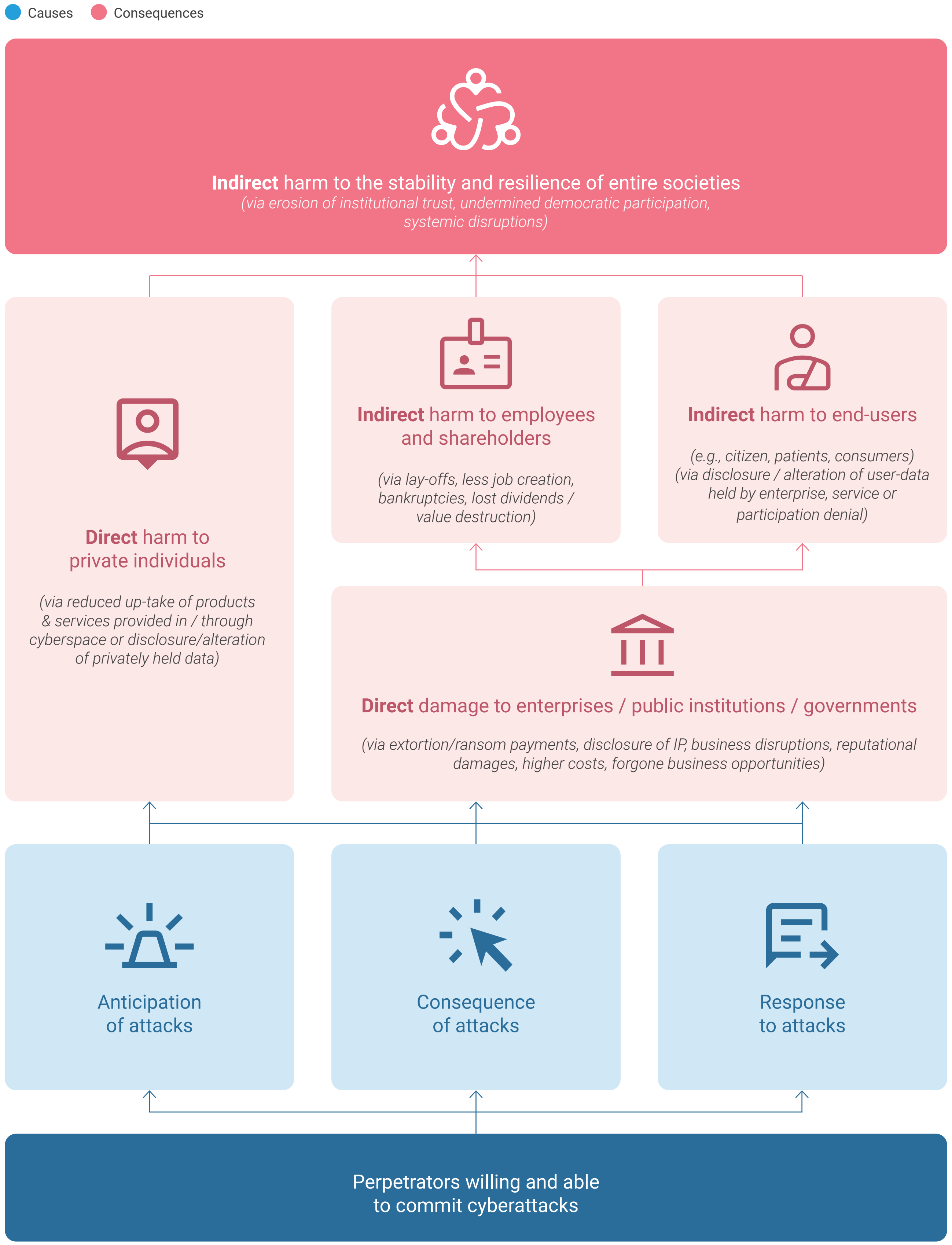
While the full extent of these harms is impossible to quantify, country-level estimates from crime research suggest annual material harm equals about 3% of GDP in advanced economies.[34] And yet, this figure still does not capture the full extent of the damage. It does, for example, not account for the psychological burden on victims, the long-term erosion of trust, or the missed opportunities as people and organizations retreat from digital engagement.



[34] Cybersecurity, and Infrastrucutre Security Agency (CISA), 2020; Dreyer et al., 2018; Smith et al., 2020; Bitkom e.V., 2020)

Figure 08

Overview of direct and indirect harm caused by cyberattacks across individuals, organizations, and societies[35]


● Causes
● Consequences
Indirect harm to the stability and resilience of entire societies
(via erosion of institutional trust, undermined democratic participation, systemic disruptions)
Direct harm to private individuals
(via reduced up-take of products & services provided in / through cyberspace or disclosure/alteration of privately held data)
Indirect harm to employees and shareholders
(via lay-offs, less job creation, bankruptcies, lost dividends / value destruction)
Indirect harm to end-users
(e.g., citizen, patients, consumers) (via disclosure / alteration of user-data held by enterprise, service or participation denial)
Direct damage to enterprises / public institutions / governments
(via extortion/ransom payments, disclosure of IP, business disruptions, reputational damages, higher costs, forgone business opportunities)
Anticipation of attacks
Consequence of attacks
Response to attacks
Perpetrators willing and able to commit cyberattacks

[35] (Agrafiotis et al., 2018; Ignatuschtschenko et al., 2016).

SPOTLIGHT

From blackouts to breaches: The scale, complexity, and cross-sector consequences of cyberattacks are also evident in high-profile real-world incidents:

2015
Ukraine – Power cut

In 2015, attackers infiltrated Ukraine's Kyivoblenergo power company using BlackEnergy malware hidden in a malicious Excel file. After months of surveillance, they remotely shut down substations, cutting power to 225,000 people for three hours. It was one of the first confirmed cases of a cyberattack triggering a physical blackout, widely attributed to Russian state actors.

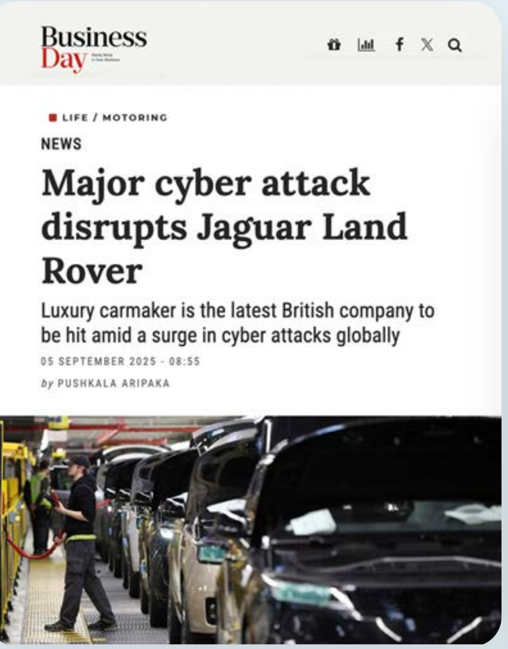
2021
Colonial Pipeline – ransomware attack

In 2021, the ransomware attack on Colonial Pipeline by the group DarkSide halted operations across a 5,500-mile fuel network. The five-day shutdown led to fuel shortages, grounded flights, panic buying, and price spikes across the southeastern US. The company paid a USD 4.4 million ransom in Bitcoin to regain control, highlighting the fragility of critical infrastructure and the economic cost of downtime.

2024
Change Healthcare – ransomware attack

In 2024, Change Healthcare was hit by BlackCat/ALPHV. Using stolen identities, attackers encrypted sensitive data and exfiltrated medical records of 100 million individuals. The breach paralyzed billing and care coordination nationwide, pushing smaller providers to the brink of collapse. A USD 22 million ransom was paid to restore operations, highlighting how cyberattacks can threaten data privacy, patient care, and financial viability.

World cyber news


Business Day

LIFE / MOTORING

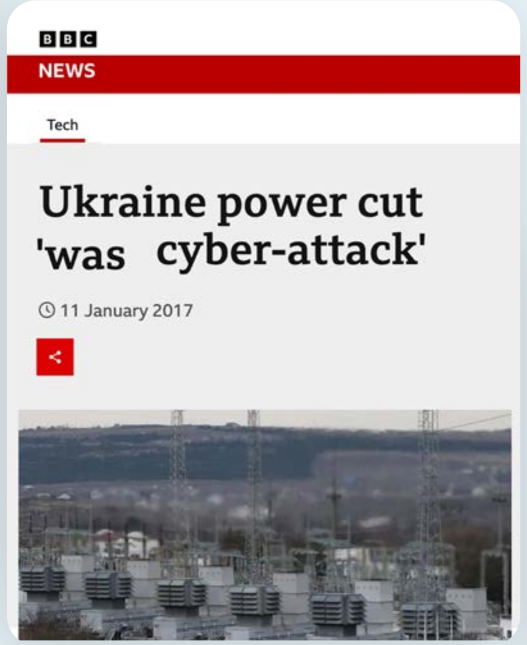
NEWS

Major cyber attack disrupts Jaguar Land Rover

Luxury carmaker is the latest British company to be hit amid a surge in cyber attacks globally

05 SEPTEMBER 2025 - 08:55

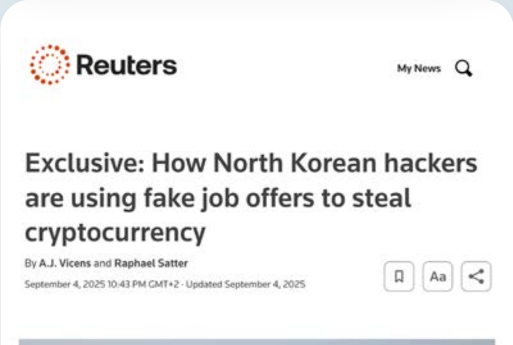
by PUSHKALA ARIPAKA


BBC NEWS

Tech

Ukraine power cut 'was cyber-attack'

11 January 2017

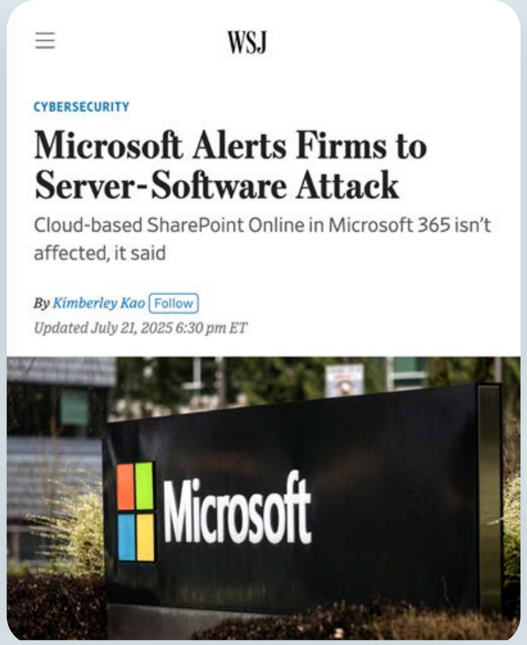

Reuters

My News

Exclusive: How North Korean hackers are using fake job offers to steal cryptocurrency

By A.J. Vicens and Raphael Satter

September 4, 2025 10:43 PM GMT+2 · Updated September 4, 2025


WSJ

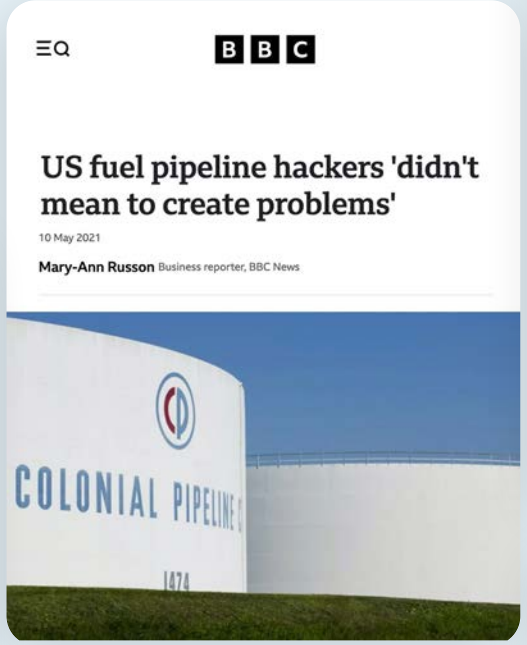
CYBERSECURITY

Microsoft Alerts Firms to Server-Software Attack

Cloud-based SharePoint Online in Microsoft 365 isn't affected, it said

By Kimberley Kao Follow

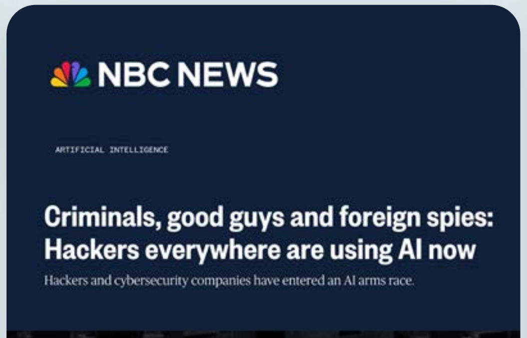
Updated July 21, 2025 6:30 pm ET


BBC

US fuel pipeline hackers 'didn't mean to create problems'

10 May 2021

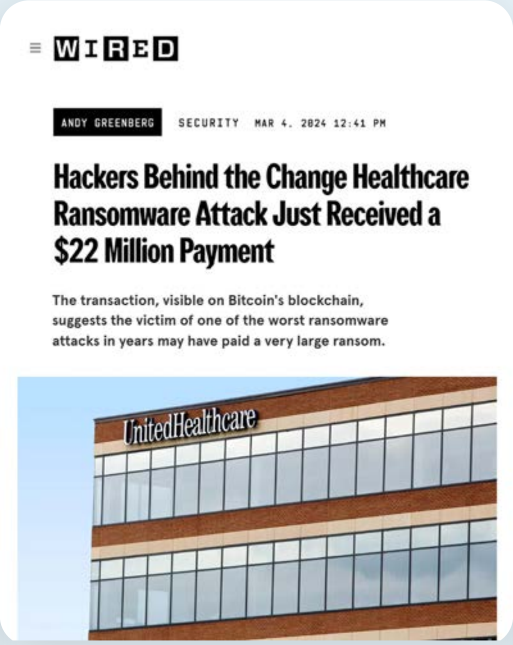
Mary-Ann Russon Business reporter, BBC News


NBC NEWS

ARTIFICIAL INTELLIGENCE

Criminals, good guys and foreign spies: Hackers everywhere are using AI now

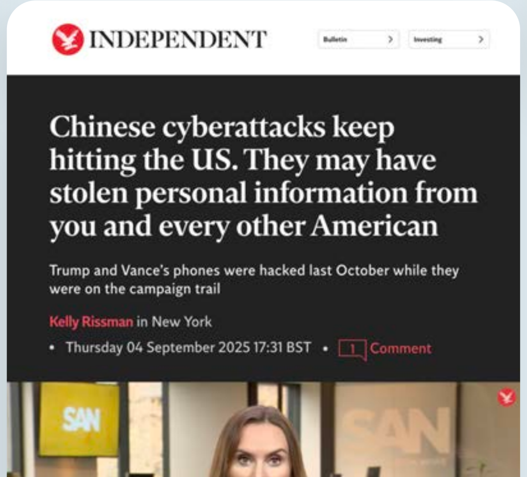
Hackers and cybersecurity companies have entered an AI arms race.


WIRED

ANDY GREENBERG SECURITY MAR 4, 2024 12:41 PM

Hackers Behind the Change Healthcare Ransomware Attack Just Received a $22 Million Payment

The transaction, visible on Bitcoin's blockchain, suggests the victim of one of the worst ransomware attacks in years may have paid a very large ransom.


INDEPENDENT

Bulletin

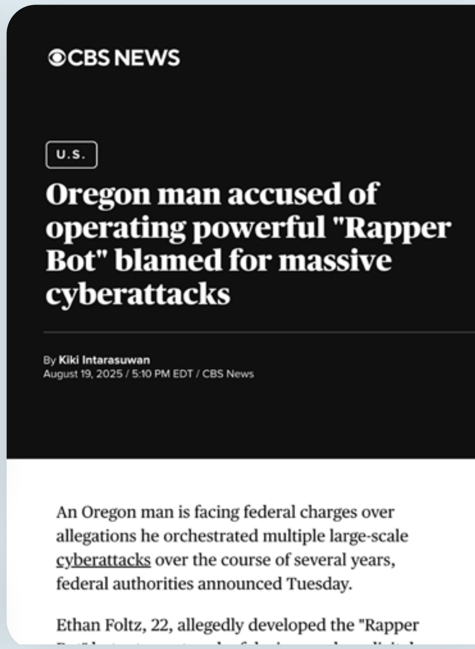
Investing

Chinese cyberattacks keep hitting the US. They may have stolen personal information from you and every other American

Trump and Vance's phones were hacked last October while they were on the campaign trail

Kelly Rissman in New York

• Thursday 04 September 2025 17:31 BST • 1 Comment


CBS NEWS

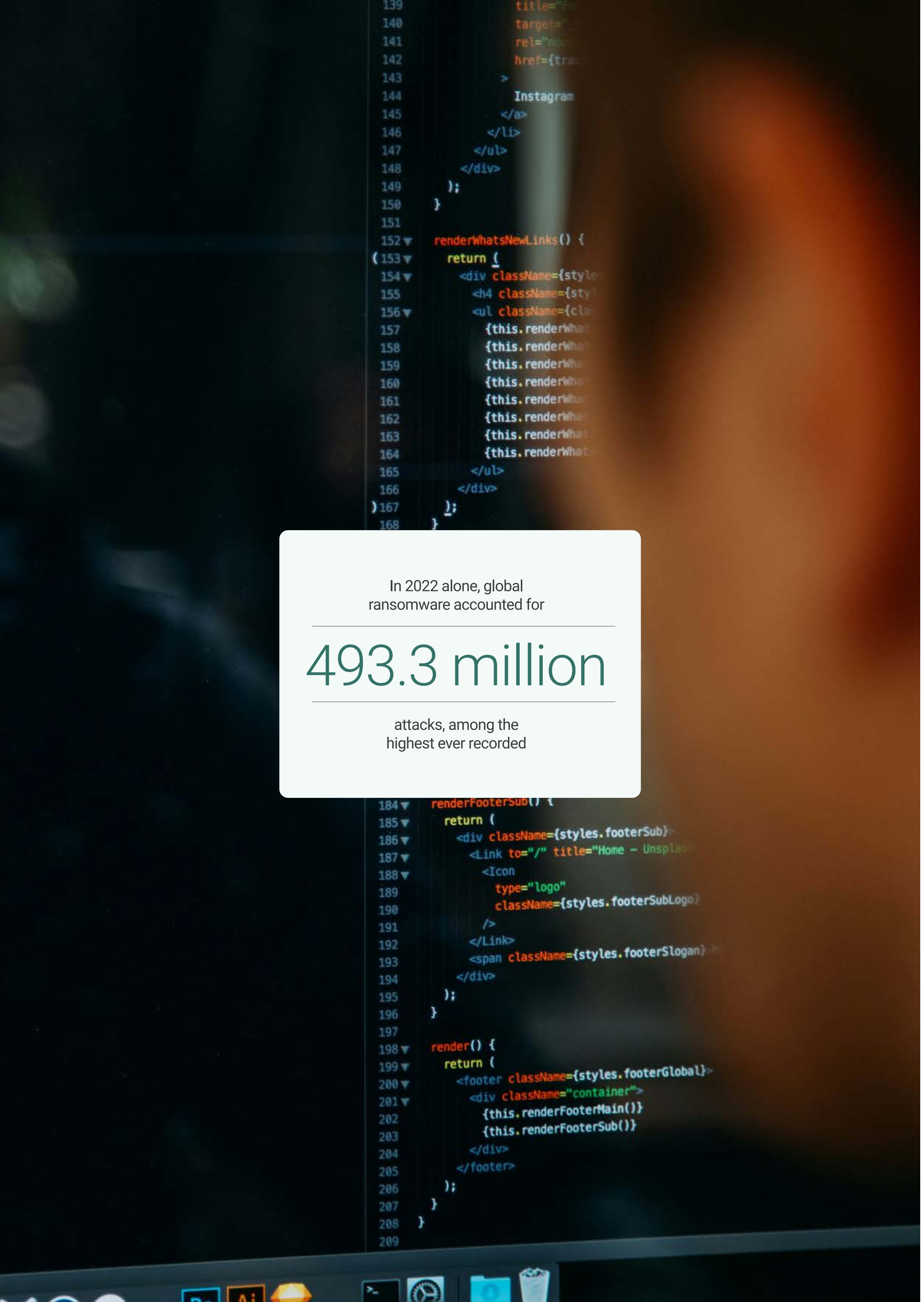
U.S.

Oregon man accused of operating powerful "Rapper Bot" blamed for massive cyberattacks

By Kiki Intarasuwan
August 19, 2025 / 5:10 PM EDT / CBS News

An Oregon man is facing federal charges over allegations he orchestrated multiple large-scale cyberattacks over the course of several years, federal authorities announced Tuesday.

Ethan Foltz, 22, allegedly developed the "Rapper



In 2022 alone, global ransomware accounted for

493.3 million

attacks, among the highest ever recorded

Cyberattacks unpacked – Tactics, actors and motivations

Cyberattack playbook: Four tactics shaping today’s threat landscape

Cyberattacks have become more destructive through deliberate methods. Refined techniques are now blended and deployed at scale to inflict maximum damage or extract maximum gains. While taxonomies differ, four recurring tactics dominate by prevalence and impact: service disruption through denial-of-service attacks, system compromise via malicious software (led by ransomware), unauthorized access through exploitation of identities or vulnerabilities, and human-factor manipulation through social engineering.[36]

Each tactic continues to evolve, with new subtypes reflecting greater sophistication, stronger focus on financial gain, growing leverage of complex supply chains, and the exploitation of increasingly distributed operations:

- **Availability attacks** disrupt access to digital services by overwhelming network or application endpoints such as login, search, or checkout functions using Denial-of-Service (DoS) or Distributed DoS (DDoS) techniques.[37] A growing trend is application-layer DDoS, which targets APIs and microservices that are harder to defend than traditional network-layer endpoints.[38] Microsoft mitigated 1.25 million DDoS attacks in H2 2024 alone across their customer database, a fourfold increase from the previous year.[39]
- **Malware-based attacks** are the most persistent and damaging forms of cyberattacks. They involve malicious software to steal data (spyware), encrypt files for ransom (ransomware), or disrupt systems with viruses, worms, or adware.[40] Among these, ransomware is the most prominent and disruptive attack type in recent years. ENISA[41] identifies ransomware as one of the most frequently reported category across EU sectors. The scale is staggering. In 2022 alone, global ransomware accounted for 493.3 million attacks, among the highest ever recorded.[42]
- **Hacking** targets flaws in software, firmware, and identity systems to gain unauthorized access. Techniques such as zero-day exploits and credential abuse are common.[37] As organizations shift to cloud-based systems, identities have become the new security perimeter, making identity-based attacks even more threatening. In 2024, Microsoft blocked over 600 million identity-based attacks every day. Over 99% of them targeted password based authentication systems.[43]
- **Social engineering attacks** exploit human behavior to bypass technical safeguards. Through phishing, vishing, and impersonation, attackers manipulate users into revealing credentials or performing unauthorized actions.[37] A fast-growing subset includes fraud and scams, such as business email compromise (BEC), invoice fraud, and so-called “tech-scams”, where attackers impersonate external IT providers. In 2024, BEC accounted for over half of all global social engineering attacks, while tech-scams grew faster than both malware and phishing between 2021 and 2023.[43]

Blending multiple techniques and exploiting weaknesses across entire supply chains has become the new norm.[36] In April 2025, attackers breached UK retailer M&S by socially engineering its IT helpdesk contractor, TCS, into handing over employee credentials. That move unlocked a full-scale intrusion: malware deployment, system encryption, data exfiltration, and a ransom demand.[44] This wasn’t an isolated case. Multi-stage attacks that combine social engineering, malware, extortion, and supply chain vulnerabilities to move toward their ultimate target are becoming standard. They make defending against attacks much harder.[37]

[36] (ENISA, 2024a; Verizon Business, 2025) [37] (Verizon Business, 2025) [38] (Chandramouli, 2019; F5, 2025) [39] (Microsoft, 2024) [40] (Verizon Business, 2025) [41] (ENISA, 2024a) [42] (SonicWall, 2023) [43] (Microsoft, 2024; Verizon Business, 2025) [44] (BlackFog, 2025)

Behind the breach: Geopolitics, espionage, and the cybercrime economy

Behind every cyberattack are identifiable actors ready to strike. In most incidents, those actors come from outside the target organization. Verizon's latest breach data shows that between 67% and 96% of breaches are caused by external parties, depending on the sector.[45] Their motives are clear. Financial gain drives more than 90% of recorded breaches across industries. A smaller but growing share, around 12 to 17%, is linked to espionage, usually by state-backed groups seeking intelligence or geopolitical advantage.[45]

These attackers are very different from the lone, opportunistic hackers of the early internet. What began as isolated acts has grown into an organized, professionalized, and specialized ecosystem.

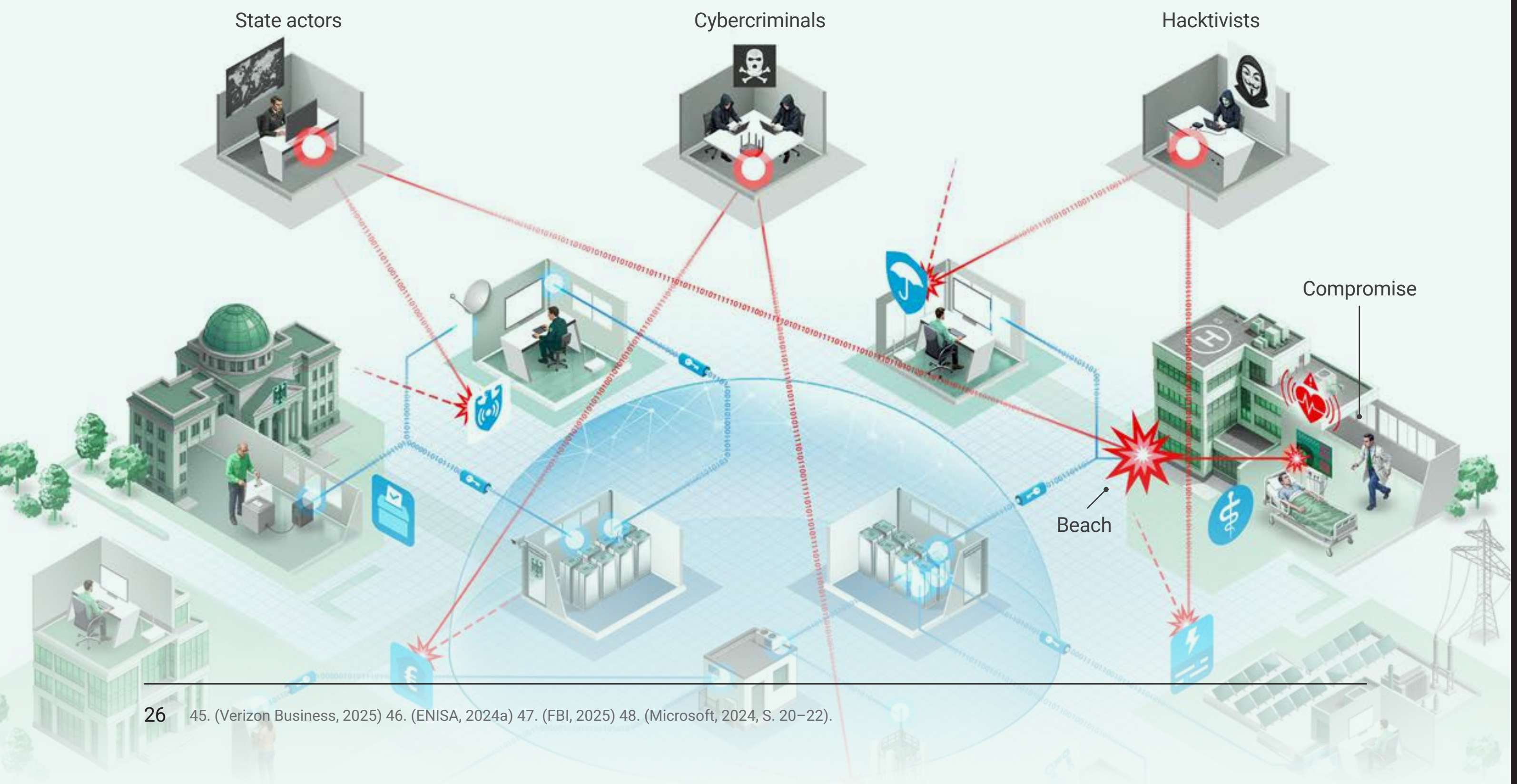
State-linked groups operate at one end of this spectrum. The European Union Agency for Cybersecurity[46] attributes 3% of documented incidents in 2023–2024 to state-nexus actors with certianty, but the true scale is unclear. A striking 62% of cases remain unattributed, and many are believed to involve covert state activity.[46] These groups are patient and well-resourced. They blend into normal network activity through techniques such as "living off the land" or "living off trusted sites" to avoid detection. Their focus is typically on espionage and disruption, with geopolitical or intelligence-gathering aims.

At the other end are cybercriminal groups, responsible for 27% of observed incidents.[46] Today, they run less like gangs and more like businesses. Their operations are based on a thriving ecosystem of initial access brokers who sell entry into networks, ransomware-as-a-service offerings that let affiliates scale attacks, and dark markets where stolen data, malware kits, and even customer support are traded[47] Together these dynamics have created a cybercrime supply chain that is as specialized and efficient as those in legitimate industries.

Hacktivists account for the remaining 8% of attributed incidents in ENISA's dataset. Driven by ideology and visibility rather than profit, their preferred tools, DDoS campaigns, website defacement, and public data leaks, often cause limited direct damage but shape perceptions and amplify uncertainty. ENISA recorded over 3,600 hacktivist incidents in Europe alone during 2023–2024, the majority tied to the Russia – Ukraine conflict.[46]

For all their differences, the boundaries between these groups are dissolving. Cybercriminals now use tools once reserved for intelligence services. State actors routinely draw on the criminal marketplace to buy access or outsource tasks. Hacktivists sometimes cloak or amplify state-sponsored agendas.[48]

Figure 09
Identifiable actors behind cyberattacks



[45] (Verizon Business, 2025) [46] (ENISA, 2024a) [47] (FBI, 2025) [48] (Microsoft, 2024, S. 20–22).

```
⚠<alert>

Ooops, your important files are encrypted.⚠
If you see this text, then your files are no longer accessible, be-
cause they have been encrypted. Perhaps you are busy looking for a
way to recover your files, but don't waste your time.

     Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and
easily. All you need to do is submit the payment and purchase the
decryption key:

parse(data)
     c, alert;-
{⚠
<alert>
```

12–17%

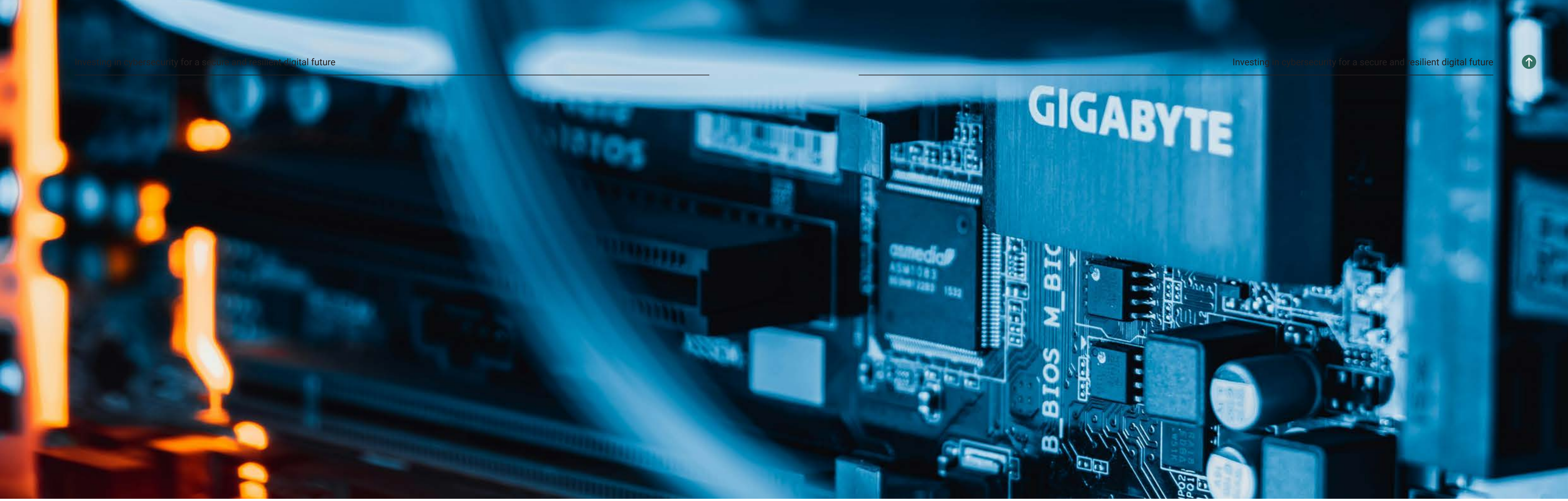
of cyberattacks are linked to state-backed groups seeking intelligence or geopolitical advantage

```
Please follow the instructions:

  ⚠ 1. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78MGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to
e-mail WOWSmith123456@posteo.net.⚠ Your personal installation key:

74f296-2NX1GM-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-KE6sSN-08t
izV-gUeUMa
```



Why attackers strike: The cyber equation

Although cybercriminals, hacktivists, and state-linked groups differ in resources and intent, none of them strike at random. Each considers what they stand to gain, what risks they face, and how easy the target looks. Their choices are shaped by motivation, deterrence, and opportunity.[49]

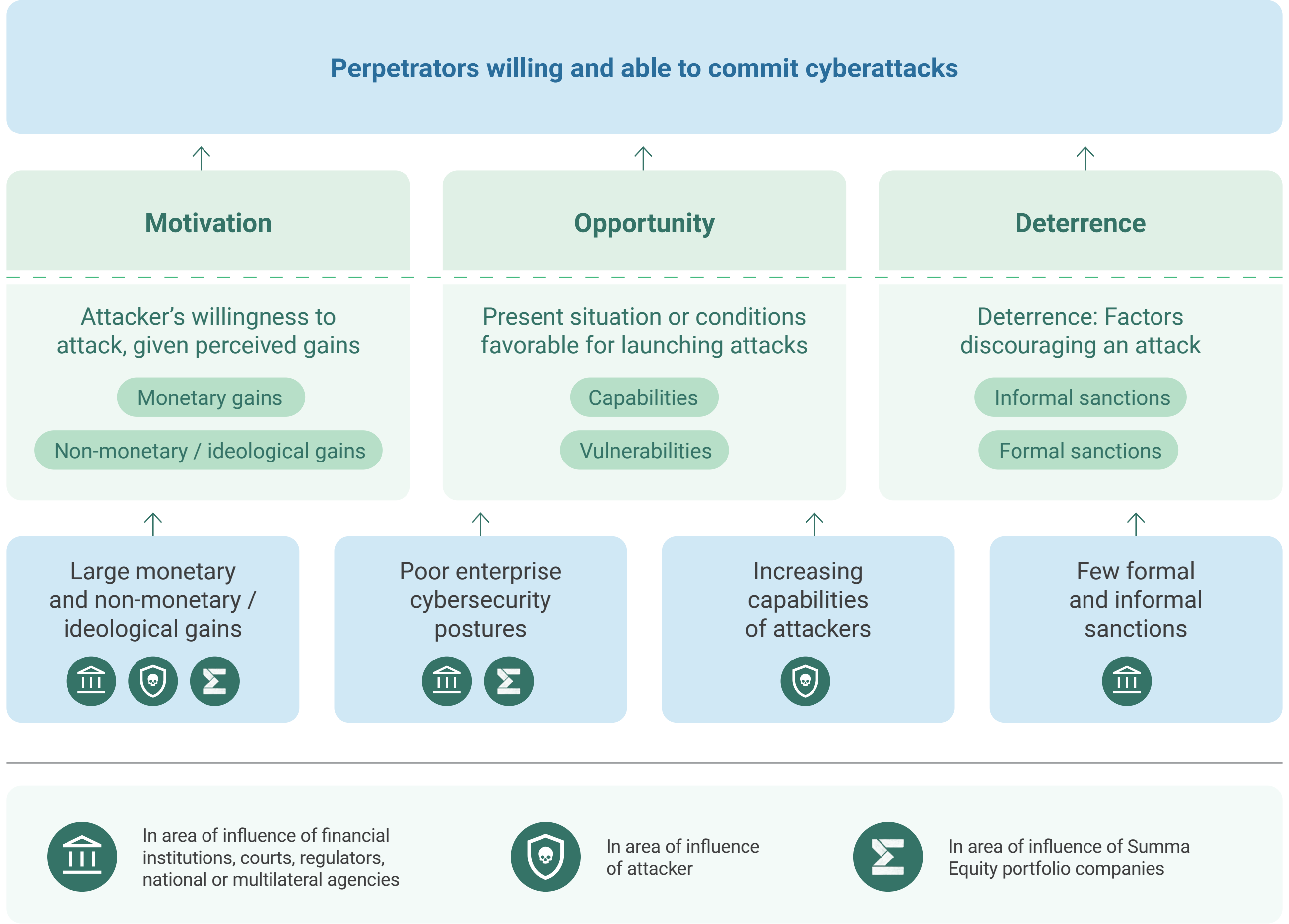
- **Motivation** is the perceived gain, financial or ideological. Cybercrime pays and attackers know it. With more high-value data and processes online, incentives to strike keep growing. Attackers now use mature monetization channels, from ransomware payouts to dark web markets, to quickly convert stolen assets into cash[50]
- **Deterrence** is the perceived cost of getting caught, through detection, attribution, or punishment. Today, deterrence is weak. Attackers operate with near impunity due to limited governance and cross-border enforcement. In the US, only 1 in 2,000 cybercrimes leads to prosecution, a rate of only 0.05%[51]
- **Opportunity** is the ease of execution, shaped by the balance between attack and defense. That balance now favors attackers. Criminal groups have professionalized, developing advanced exploits or buying tools and services such as ransomware and cyberattacks-as-a-service on dark web marketplaces.[52] At the same time organizations now lag in cybersecurity maturity, leaving attackers with growing ease of entry[53]

Crucially, each of these factors also represents an opportunity to prevent future attacks by diminishing motivation, strengthening deterrence, and reducing opportunities. While all three levers play a role, reducing opportunities by strengthening victims' defenses is the most directly addressable through market-based solutions. This is also where private capital can have the greatest impact, and is therefore the focus of the remainder of this report.

1 in 2,000

cybercrimes leads to prosecution in the US, a rate of only 0.05%

Figure 10
Overview of underlying causes of cyberattacks and the influence of various actors, like Summa portfolio companies, on the willingness and ability to conduct them[54]



Perpetrators willing and able to commit cyberattacks

Motivation

Attacker's willingness to attack, given perceived gains

Monetary gains

Non-monetary / ideological gains

Opportunity

Present situation or conditions favorable for launching attacks

Capabilities

Vulnerabilities

Deterrence

Deterrence: Factors discouraging an attack

Informal sanctions

Formal sanctions

Large monetary and non-monetary / ideological gains 🏛 🛡 Σ

Poor enterprise cybersecurity postures 🏛 Σ

Increasing capabilities of attackers 🛡

Few formal and informal sanctions 🏛

🏛 In area of influence of financial institutions, courts, regulators, national or multilateral agencies

🛡 In area of influence of attacker

Σ In area of influence of Summa Equity portfolio companies

49. (Canadian Minister of National Defence, 2022; Mandelcorn, 2013 o. J.; McKenzie, 2017) 450. (Ablon, 2018) 51. (Iftikhar, 2024; Pell et al., 2024; WEF, 2020) 52. (FBI, 2025) 53. (ENISA, 2024b).

54. (Canadian Minister of National Defence, 2022; McKenzie, 2017)

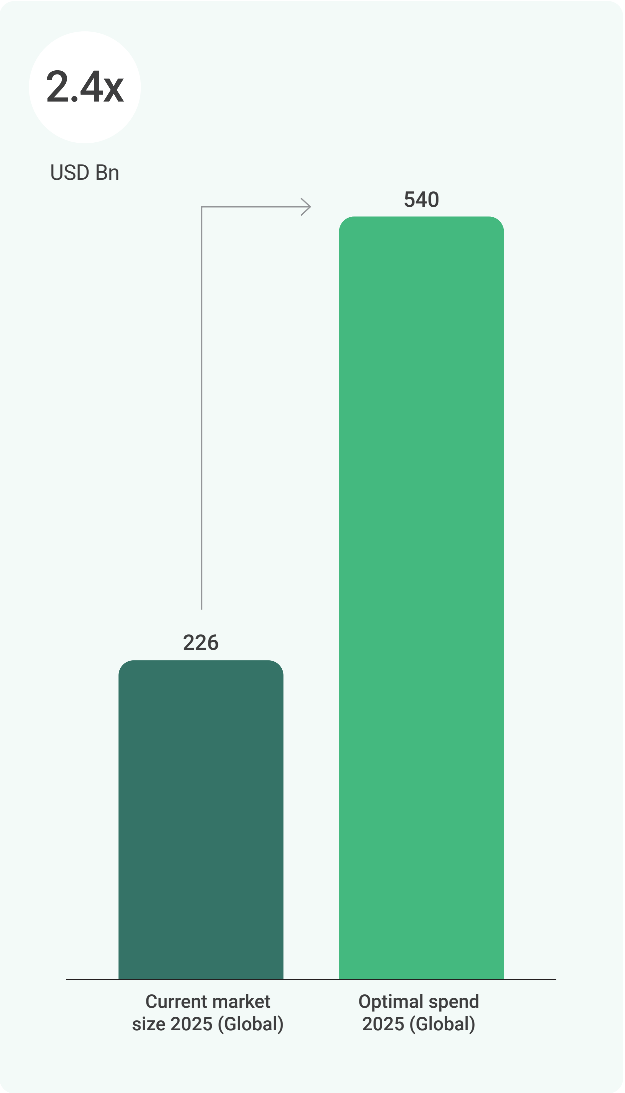
Too little, too late – The shortfall of cyber defenses

Attackers strike when incentives align and openings exist.

Motives cannot be reset overnight, and deterrence remains weak. The opportunity side of the equation, however, can be addressed. Today, opportunities abound because organizations' cybersecurity readiness remains well below what the current threat environment demands.

Using annual spend on cybersecurity products and services as a proxy for defensive capability, Summa and CEPS analysis suggests organizations invest only ~42% of the of the economically optimal level required to minimize expected damages from cyberattacks. Today, this is roughly USD 226 billion versus an optimal ~USD 540 billion. In other words, spending would need to more than double to align defenses with expected losses and the effectiveness of today's solutions. While the exact figure is sensitive to assumptions about expected losses and control effectiveness, the shortfall is substantial under any scenario.

Figure 11
Current global expenditure on cybersecurity products & services vs theoretical optimal expenditure (CEPS & Summa Analysis, based on prior work) [55]



[55] (Carfora & Orlando, 2024; Gordon et al., 2015; Gordon & Loeb, 2002; Naldi & Flamini, 2017).

While the aggregate shortfall is striking, it is not evenly distributed. Capability gaps vary widely across sectors and firm sizes and not every weakness is equally consequential for society.

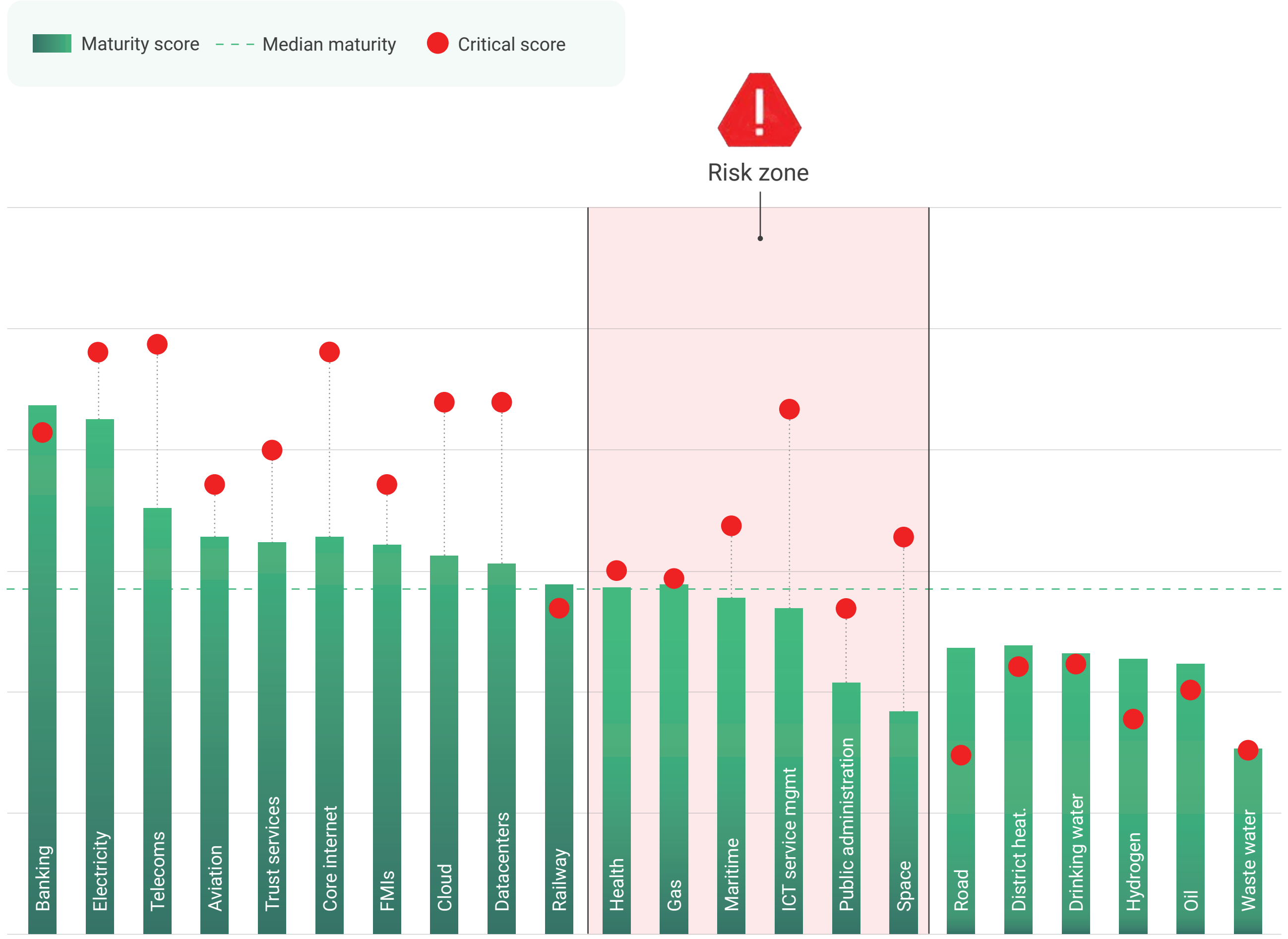
Some sectors carry outsized consequences when their defenses lag. ENISA's criticality-versus-maturity analysis shows that ICT service management, space, public administration, maritime, health, and gas all sit squarely in the risk zone, essential for society but insufficiently protected.[56] Weaknesses here create the conditions for widespread disruptions that undermine economic resilience, threaten public welfare, and compromise national security. Services with high criticality but low maturity such as drinking water and energy infrastructure, including gas, oil, and district heating show similar vulnerabilities.[57]

Variability is just as pronounced when viewed through the lens of organizational size. Small and mid-sized enterprises (SMEs) are increasingly targeted precisely because they lack the expertise, resources, and governance structures needed for adequate defense. Unlike large corporates, they often cannot sustain dedicated security staff or advanced tools.[58]

Their weakness, however, is everyone's problem. SMEs form the backbone of advanced economies, accounting for the majority of employment and output. Once overlooked, they are now attractive targets in their own right. They hold critical data, account for nearly all firms in global supply chains, and are a critical support to essential services. A compromised SME can serve as a stepping stone for adversaries to reach larger, more critical targets.[59]

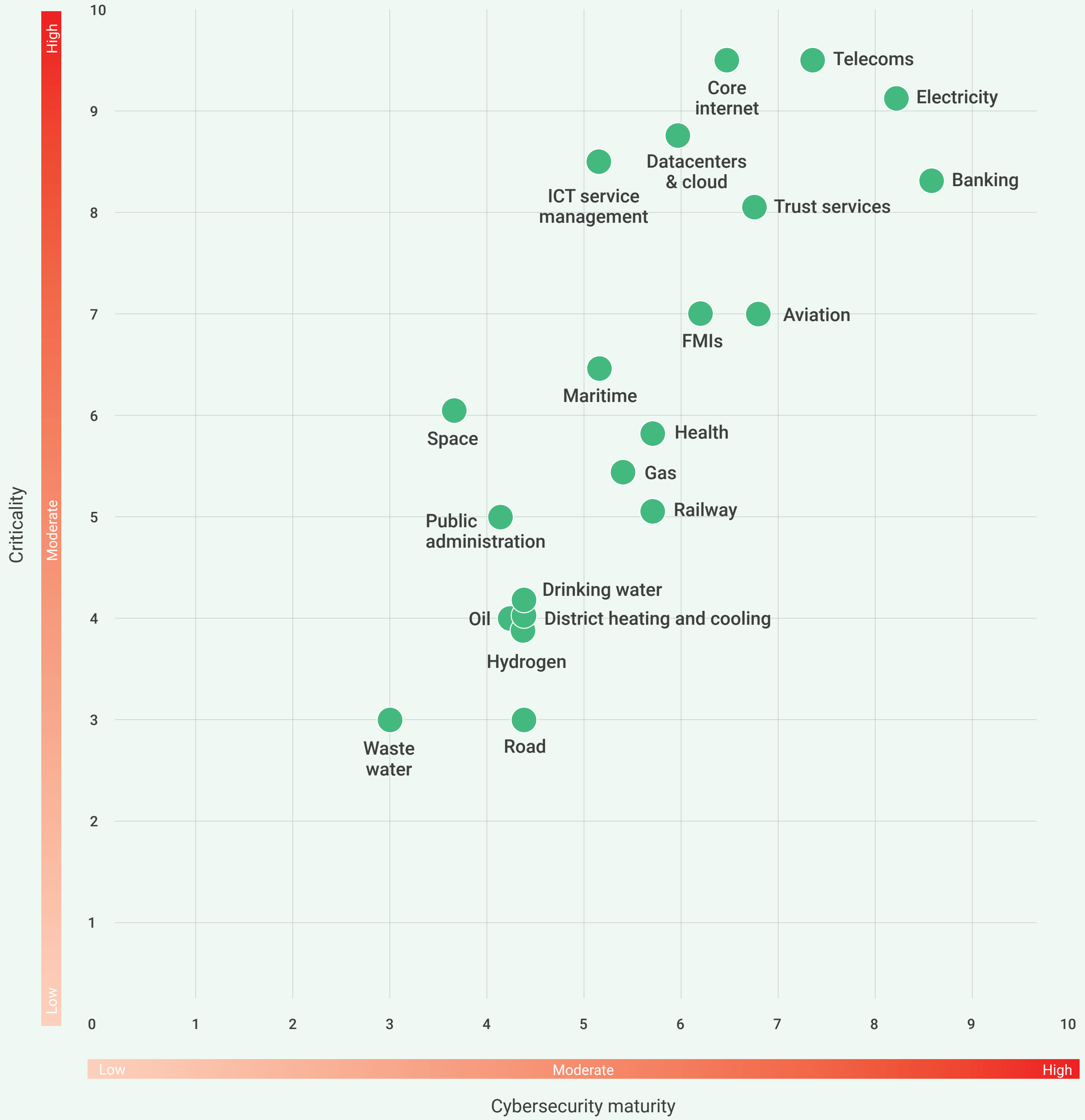
Taken together, these gaps point to a clear priority. Capabilities across the board must improve, but the greatest benefit comes from raising defenses in the most critical and vulnerable areas. Directing capital and capability to these points reduces the likelihood of severe outcomes for society and narrows the opportunity space for future attacks where it matters most.

Figure 12
Overview of EU sectors in risk zone (where criticality exceeds maturity) (ENISA, 2025a, S. 13)



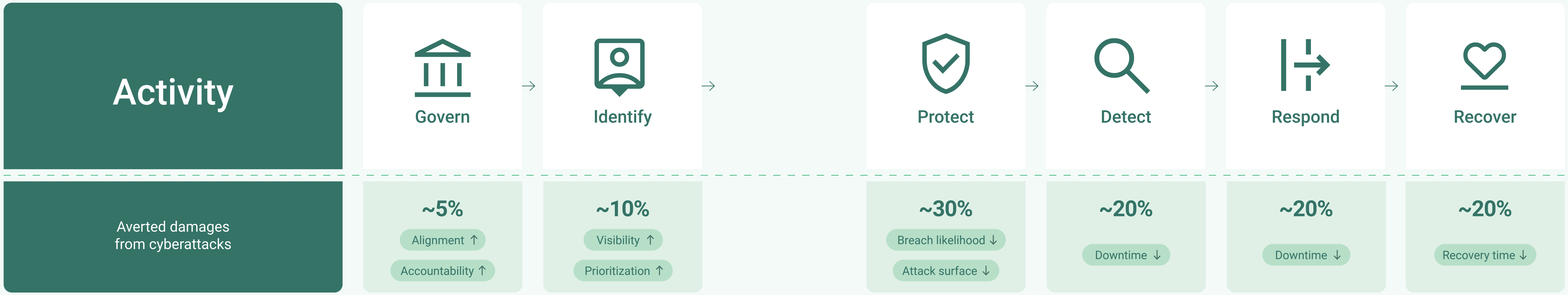
[56] (ENISA, 2025) [57] (Dubois, 2025) [58] (McKinsey, 2021) [59] (PurpleSec, 2024)

Figure 13
Cybersecurity maturity and criticality for society of EU sectors[60]



[60] (ENISA, 2025a, S. 8)

Figure 12
Six interdependent functions that determine whether organizations can prevent, withstand, or recover from attacks[61]



Where organizations lag: Core defenses demanding improvements

Closing the capability gap also requires looking beyond aggregate spending. Evidence shows the most critical weaknesses lie in a small set of core functions that ultimately determine whether organizations can prevent, withstand, or recover from attacks.

The US National Institute of Standards and Technology (NIST) frames them as six interdependent functions: govern, identify, protect, detect, respond, and recover. The first group, govern, identify, and protect, shapes strategy, assesses vulnerabilities, and implements controls to reduce the likelihood of attack. The second group, detect, respond, and recover, covers monitoring for anomalies, confirming and containing threats, and restoring systems to minimize the impact from an attack.[61]

Govern
Absent clear priorities, risk tolerances, and decision rights, cybersecurity devolves into policy drift and fragmented accountability. Still, many organizations lack this foundation. UK data shows that 30% of large and 43% of medium-sized have no formal cyber strategy.[62] Industry research shows a similar picture: more than two-thirds of boards report limited involvement, and nearly 60% of directors receive cyber training only “occasionally”.[63] Without clear standards, defined risk ownership, and integration with enterprise risk management, capabilities end up misaligned, inconsistently funded, and unsustainable, leaving blind spots for adversaries to exploit.

Identify
Without visibility into threats and vulnerabilities, security measures often miss the mark. Only a minority of organizations assess risk regularly: 8% of companies conduct cyber risk assessments monthly, while 40% do so annually. This lack of awareness has tangible consequences. The majority of breaches stem from unpatched, publicly known vulnerabilities, with most companies harboring high-risk flaws that could be fixed with a simple update.[64] When discovery is sporadic and remediation lags, attackers exploit the gaps.

Protect
Even when vulnerabilities are identified, weak protection leaves them exposed through single-factor logins, neglected endpoints, insecure APIs, or unencrypted data. Basic safeguards are inconsistent. The vast majority of account breaches could be prevented by Multi-Factor-Authentication (MFA), most breaches stem from unpatched systems, and only half of companies systematically encrypts sensitive data. When these fundamentals are ignored, adversaries exploit the vulnerabilities again and again.[65]

Detect & Respond
Because some vulnerabilities are features and not flaws, eliminating them entirely is impossible. This makes continuous monitoring and rapid incident response essential. Detection gaps remain stark. The average time to identify and contain a breach is 258 days, with most breaches discovered not by the victim but revealed by third parties or even the attackers themselves.[66] These delays lengthen breach lifecycles, increase disruption, and give adversaries more time to cause damage.

Recover
Without strong recovery capabilities, the fallout from a cyberattack can escalate into weeks or months of disruption. Yet, only half of organizations maintain and regularly test continuity or disaster recovery plans. 60% express uncertainty that their current backups would protect critical data in a crisis, while 30% have no confidence at all. Unsurprisingly, average recovery times exceed 100 days. When plans go untested and backups prove unreliable, downtime, not data loss, often becomes the primary driver of harm.[66]

258
days

The average time to identify and contain a breach

[61] (NIST, 2024) [62] (UK Home Office, 2025) [63] (PwC Hong Kong: Governance gaps in cybersecurity practices revealed: Urgent action needed, o. J.) [64] (State of Cybersecurity 2023 | ISACA, o. J.) [65] (Security at your organization - Multifactor authentication (MFA) statistics - Partner Center | Microsoft (w.y.) Learn, o. J.)

[66] (IBM, 2025)

Incentives, costs, and complexity: Systemic barriers to cyber resilience

Organizations are not simply failing to build security. They are responding to a system that discourages investment in it. The problems is less about ignorance and more about long-standing structures that shape incentives and trade-offs, which keep defenses weaker than society needs. Summa's approach begins with this recognition. Pointing out flaws is not enough. Lasting progress requires changing the system itself.

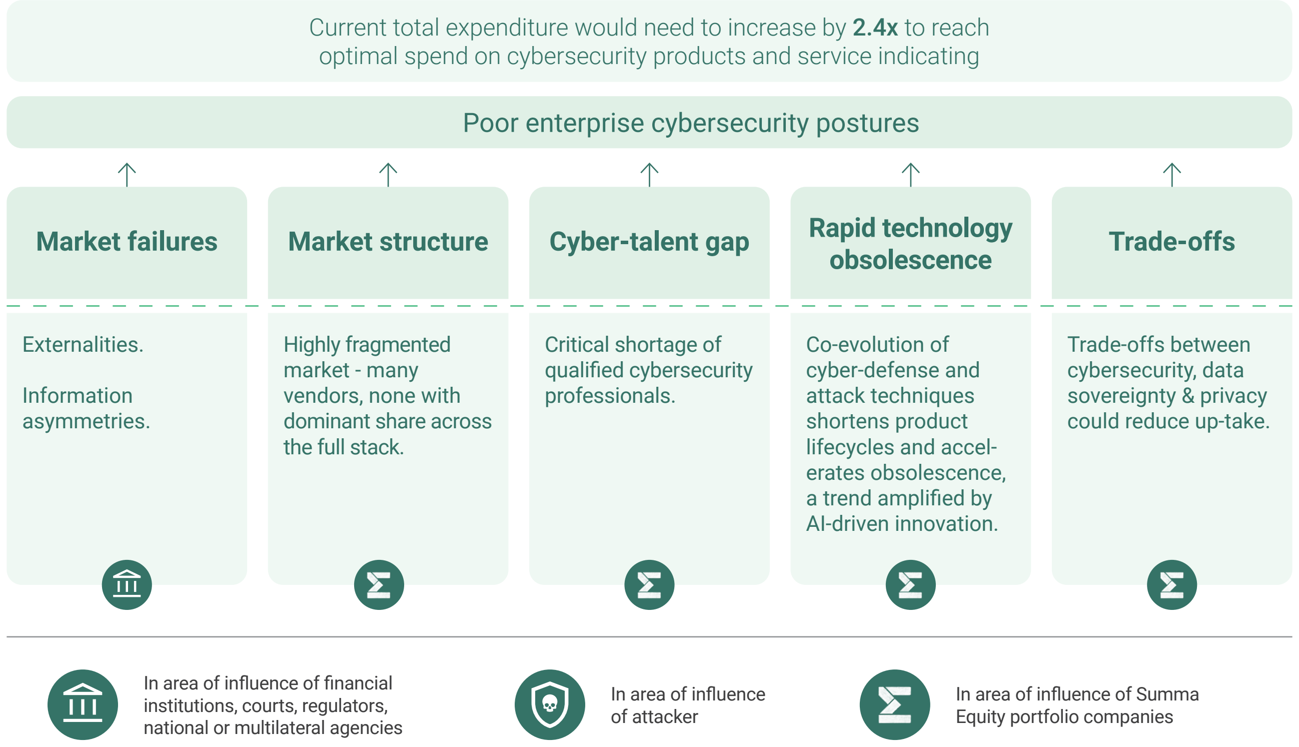
The first problem is incentives. Strong security protects not only the firm, but also its partners, suppliers, and customers. These benefits are rarely rewarded, while the costs of weak security can often be passed on to others. This creates a rational incentive to invest less than social needs.[67] The issue is made worse by information gaps between buyers and vendors. Buyers struggle to measure the real value of cybersecurity investments, so they often focus on price or basic compliance. Vendors then have little reason to deliver stronger products when higher quality does cannot reliably command a premium.[67]

Even when firms commit resources, structural inefficiencies in the cybersecurity industry reduce the impact. A global shortage of nearly four million cyber professionals makes it hard to hire and drives up costs, lowering returns on internal programs and labor-intensive services.[68] Security markets are also fragmented. Enterprises manage on average 83 tools from 29 vendors, creating integration costs and operational friction.[69] At the same time, defenders are locked in a constant arms race with attackers, now accelerated by AI. Security tools and controls lose effectiveness quickly, forcing continual reinvestment.[70]

Trade-offs add another challenge. Effective detection requires continuous monitoring, but this can clash with privacy regulations or labor norms. Data sovereignty concerns push firms to choose between operational efficiency and legal certainty. Especially in Europe, where dependence on foreign vendors is seen as a strategic vulnerability.[71] Faced with these tensions, many organizations hold back, limiting visibility and resilience in ways attackers exploit.

These choices are not irrational. They are predictable outcomes of structural constrains. The result is a stable but flawed equilibrium: incentives favor underinvestment, limited transparency weakens market discipline, high costs reduce returns, and trade-offs stall adoption of best practices. Breaking this cycle will take more than better tools. It will require systemic solutions that address the incentive failures, market inefficiencies, and structural barriers. Some solutions will involve regulatory intervention, while others will require innovation in products, services, and business models. Both are essential to closing the capability gap.

Figure 14
Systemic causes of insufficient cybersecurity postures.[72]



Current total expenditure would need to increase by **2.4x** to reach optimal spend on cybersecurity products and service indicating

Poor enterprise cybersecurity postures

Market failures	Market structure	Cyber-talent gap	Rapid technology obsolescence	Trade-offs
Externalities. Information asymmetries.	Highly fragmented market - many vendors, none with dominant share across the full stack.	Critical shortage of qualified cybersecurity professionals.	Co-evolution of cyber-defense and attack techniques shortens product lifecycles and accelerates obsolescence, a trend amplified by AI-driven innovation.	Trade-offs between cybersecurity, data sovereignty & privacy could reduce up-take.
🏛	Σ	Σ	Σ	Σ

🏛 In area of influence of financial institutions, courts, regulators, national or multilateral agencies

🛡 In area of influence of attacker

Σ In area of influence of Summa Equity portfolio companies

[67] (Gordon et al., 2015) [68] (World Economic Forum, 2024) [69] (How unified cybersecurity platforms add business value | IBM, o. J.) [70] (CEPS & Summa Equity, 2025; IBM, 2025) [71] (HarfangLab, 2025) [72] (Summa Equity Analysis, 2025).

SPOTLIGHT

Europe builds cyber-sovereignty amid US dependence risks.

The EU is raising its cybersecurity ambitions. Concerns over dependence on non-EU providers have grown, driven by geopolitical shifts and rising awareness of legal and technological risks. By harmonizing requirements across member states, enforcing strict risk management for both public and private actors, and promoting EU-based infrastructure and secure-by-design products, the EU is laying the foundation for a more autonomous and secure digital future.[73]

This ambition reflects the European Commission's view of cybersecurity as essential for trust in innovation, connectivity, and automation, as well as for protecting data, privacy rights, and freedom of expression.[73] As cyber threats intensify across critical sectors, the EU is accelerating its regulatory agenda. The focus is shifting from fragmented national strategies to a unified, sovereignty-driven cybersecurity framework aimed at strengthening digital resilience and reducing reliance on non-EU technology providers.[74]

The US has long led cybersecurity through private investment and globally platforms, while the EU has leaned on regulation, public coordination, and strategic initiatives but with lower investment. That is shifting. The Digital Decade Policy Program 2030 sets clear targets for fiber, 5G, and edge computing to reduce reliance on non-EU suppliers.[73] New initiatives such as the Cybersecurity Skills Academy and the Cybersecurity Blueprint aim to close the talent gap and improve cross-border coordination. These steps are not only reactive but part of a broader ambition to build resilience, digital sovereignty, and stability in an increasingly contested digital environment.

70–84% of European organizations, especially in Germany and France, see foreign cybersecurity dependence as a strategic risk. Many are considering European alternatives. Sovereignty and control are rising priorities, with 31% of organizations preferring on-premises solutions over cloud, citing concerns about foreign data access, legal assurance, and geopolitics.[75]

Markets are aligning. Amazon is developing a sovereign cloud in Germany with EU-based governance. Microsoft and Google are launching "air-gapped" services for European clients. Yet, US laws such as the Cloud Act remain a concern. Microsoft France recently confirmed that EU-stored data may still face US access, prompting new scrutiny from EU institutions.[76]

Together, these developments show a growing alignment of EU policy, regulation, and markets around the goal of cybersecurity self-reliance. Demand is rising for trusted products, secure data storage, and infrastructure that support European digital sovereignty.

Key regulations:

NIS2 Directive (in force since Jan 2023 - full implementation by Oct 2024): The NIS2 Directive mandates strict cybersecurity and incident reporting for 18 critical sectors, requiring robust risk management (including third-party risks), governance, training, and executive accountability. Organizations must register with national authorities, with penalties up to EUR 10 million or 2% of global turnover for non-compliance.[77]

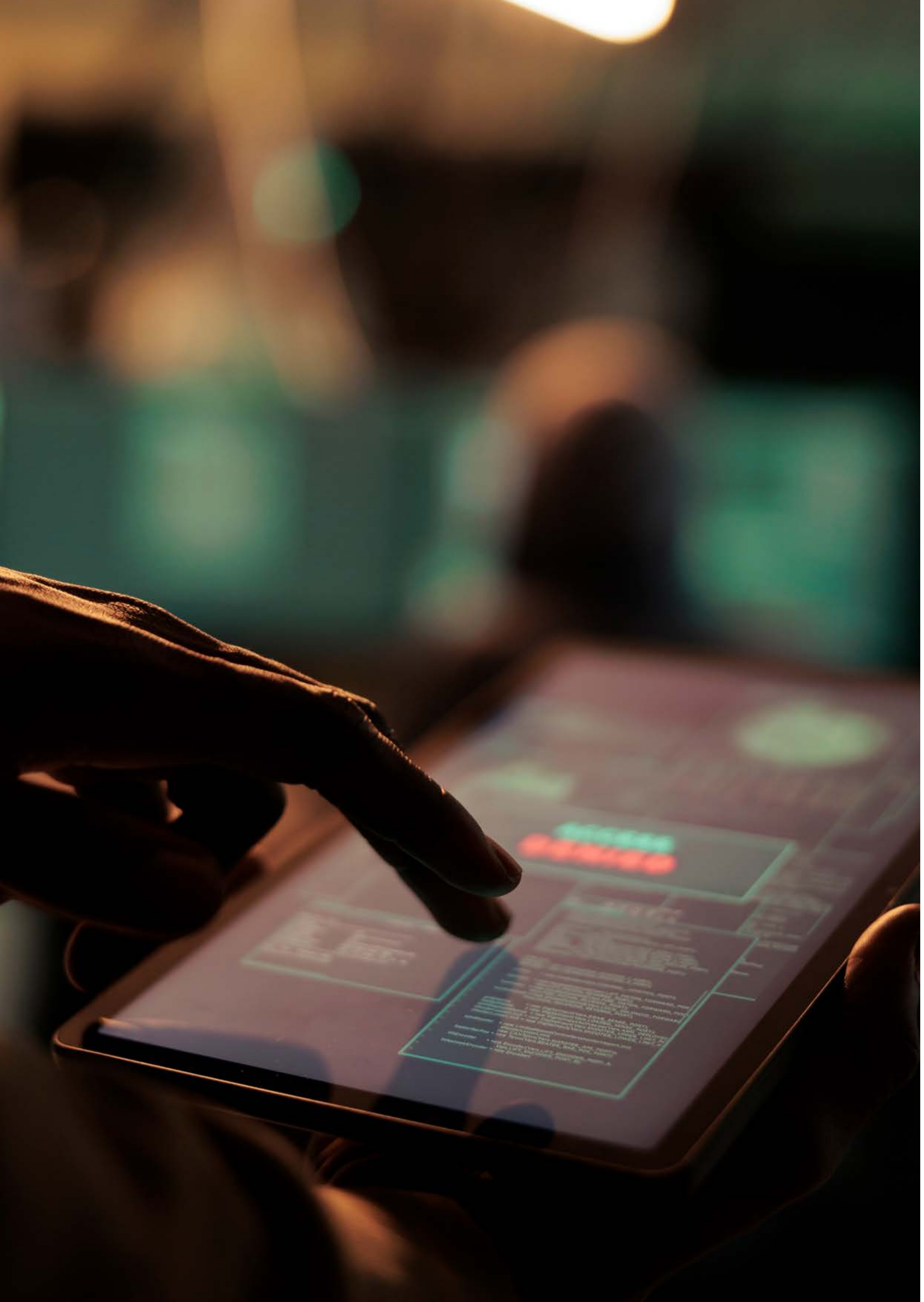
EU Cyber Resilience Act (adopted Oct 2024): Mandates built-in cybersecurity for digital products and connected devices, shifting responsibility to manufacturers and opening markets for secure-by-design solutions.[78]

DORA (enforced from Jan 2025): Applies to financial services and ICT providers, requiring operational resilience planning, third-party risk oversight, and cyber incident testing.[79]

[73] (European Commission, 2020) [74] (Dubois, 2025) [75] (HarfangLab, 2025) [76] (Moens, 2025; Wiggers, 2025) [77] (Deloitte, 2022) [78] (European Council, 2024) [79] (EIOPA, 2025)

70-84%

of European organizations, especially in Germany and France, see foreign cybersecurity dependence as a strategic risk.



System change: Envisioning a cybersecure future

What would a cybersecure future look like?

At Summa, we believe a cybersecure future is not just possible, it's critical. It's a future where individuals, businesses, and institutions can trust the digital systems they rely on every day. Where the availability, integrity, and confidentiality of information, products and services provided in and through cyberspace are not afterthoughts, but foundational. This requires a system change approach that addresses the complex and interdependent challenges of the entire cybersecurity ecosystem. It's a recognition that building a cybersecure future requires coordinated transformation across technology, governance, human behavior, and policy structures. This future vision is one where Europe leads with purpose, ensuring that digital progress goes hand in hand with democratic values, resilience, and sovereignty.

The future we want

1. **Culture that prevents.** Strong and widely embraced norms guide how we use cyberspace responsibly. Shaped through education, industry leadership, and public engagement, these norms reduce the motivation to exploit digital infrastructure for financial gain, ideological influence, or disruption.

2. **Rules that deter.** Clear regulations backed by credible enforcement reduce the incentives for misuse. International agreements, harmonized frameworks, and cross-border investigative capacity strengthen the certainty and severity of consequences for malicious activity.

3. **Systems that protect.** Organizations design, operate, and deploy connected services with security at the core. Vulnerabilities are identified and addressed continuously. Critical assets are protected and monitored. Response and recovery capabilities are always ready.

With motivation reduced, deterrence restored, and attack surfaces minimized, enterprises and public institutions can operate with greater confidence. Fewer and less severe cyberattacks mean less downtime, fewer reputational risks, and lower exposure to litigation. Resources once spent on damage control can be redirected toward innovation, accelerating product launches, improving customer experience, and unlocking new markets.

A cybersecure future benefits everyone

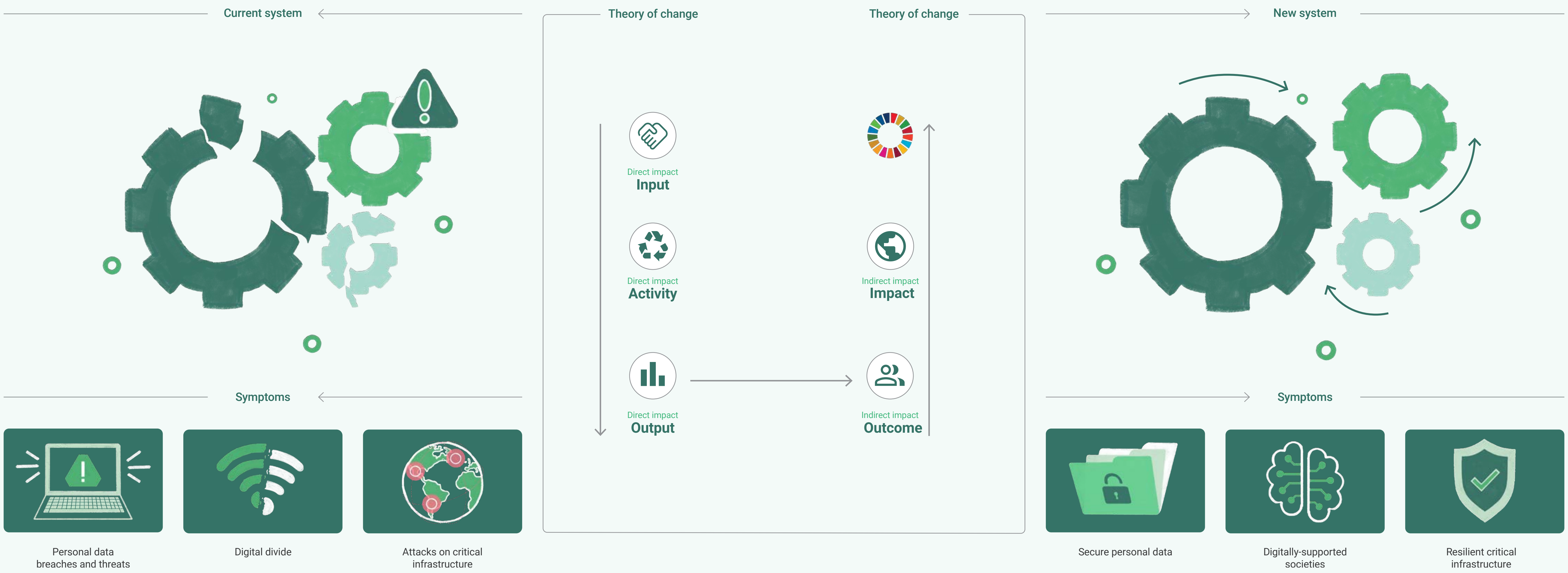
Employees benefit from stronger, more resilient organizations. When systems stay online and data remains protected, workplaces become safer, more stable, and better equipped to support long-term careers.

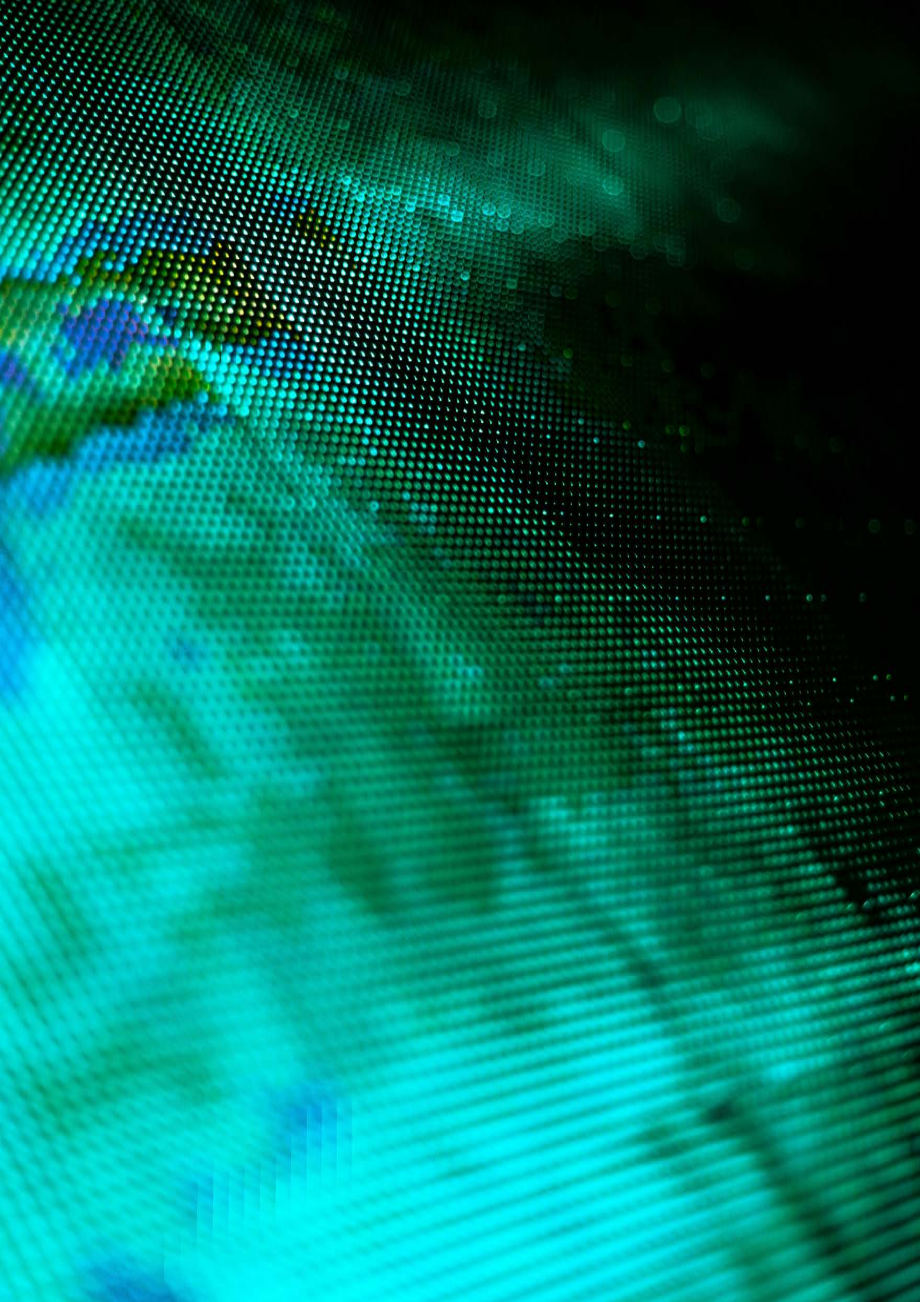
Shareholders gain from predictability and performance. Fewer disruptions mean strategic plans stay on track, and long-term returns are more resilient in the face of growing digital risk.

End-users rely on digital services they can trust. Fewer outages and stronger data protection keep essential services such as banking, healthcare, and public administration accessible and reliable. This builds confidence and encourages adoption of life-improving innovations.

Society moves faster on what matters. A secure digital backbone enables scaled deployment of digital government, smarter energy networks, sustainable supply chains, and circular industry models.

Figure 15
Theory of change – a framework to conceptualize the systems we aim to transform, envision their future state, and adopt a structured approach to tackling challenges.



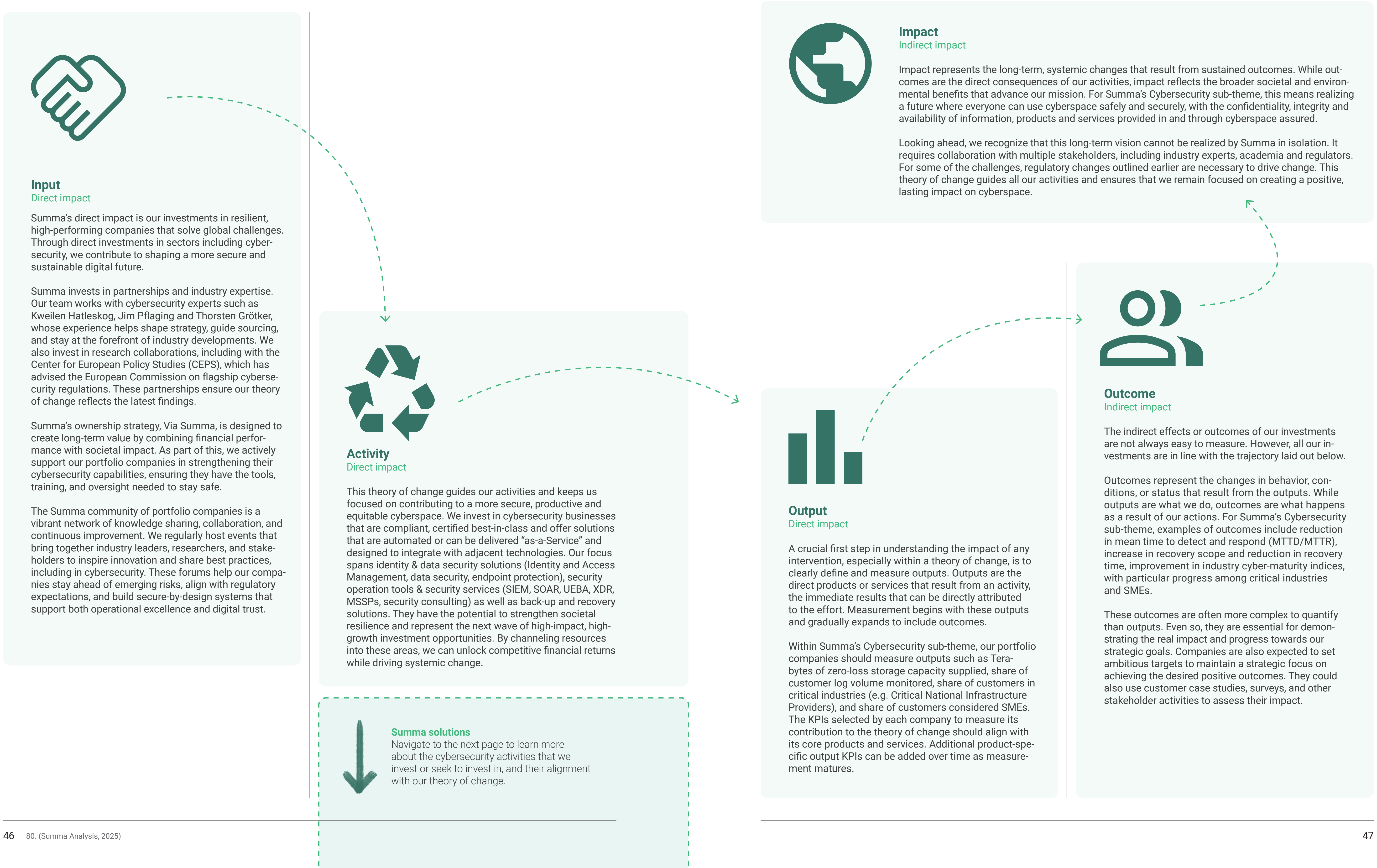


Theory of change – Connecting systems change to investment opportunities and measurable impact

To realize the digital future we want, cybersecurity must keep pace with growing threats – protecting the systems people and societies rely on every day.

At Summa, we believe that securing the digital future requires more than reactive measures – it demands a structured, impact-driven approach. Cybersecurity is not just a technical necessity; it's a foundation for trust, safety, and societal progress in an increasingly connected world. To ensure our actions lead to meaningful outcomes, we apply a theory of change framework that maps how our investments contribute to a safer digital environment. This framework helps us connect the dots between strategic decisions and real-world impact – from protecting critical infrastructure and reducing cyber-related losses, to enabling individuals and organizations to operate confidently in cyberspace. The following section outlines how we translate this vision into measurable change.

Figure 15
Summary of the theory of change for cybersecurity[80]



Input
Direct impact

Summa's direct impact is our investments in resilient, high-performing companies that solve global challenges. Through direct investments in sectors including cybersecurity, we contribute to shaping a more secure and sustainable digital future.

Summa invests in partnerships and industry expertise. Our team works with cybersecurity experts such as Kweilen Hatleskog, Jim Pflaging and Thorsten Grötker, whose experience helps shape strategy, guide sourcing, and stay at the forefront of industry developments. We also invest in research collaborations, including with the Center for European Policy Studies (CEPS), which has advised the European Commission on flagship cybersecurity regulations. These partnerships ensure our theory of change reflects the latest findings.

Summa's ownership strategy, Via Summa, is designed to create long-term value by combining financial performance with societal impact. As part of this, we actively support our portfolio companies in strengthening their cybersecurity capabilities, ensuring they have the tools, training, and oversight needed to stay safe.

The Summa community of portfolio companies is a vibrant network of knowledge sharing, collaboration, and continuous improvement. We regularly host events that bring together industry leaders, researchers, and stakeholders to inspire innovation and share best practices, including in cybersecurity. These forums help our companies stay ahead of emerging risks, align with regulatory expectations, and build secure-by-design systems that support both operational excellence and digital trust.

Activity
Direct impact

This theory of change guides our activities and keeps us focused on contributing to a more secure, productive and equitable cyberspace. We invest in cybersecurity businesses that are compliant, certified best-in-class and offer solutions that are automated or can be delivered "as-a-Service" and designed to integrate with adjacent technologies. Our focus spans identity & data security solutions (Identity and Access Management, data security, endpoint protection), security operation tools & security services (SIEM, SOAR, UEBA, XDR, MSSPs, security consulting) as well as back-up and recovery solutions. They have the potential to strengthen societal resilience and represent the next wave of high-impact, high-growth investment opportunities. By channeling resources into these areas, we can unlock competitive financial returns while driving systemic change.

Summa solutions
Navigate to the next page to learn more about the cybersecurity activities that we invest or seek to invest in, and their alignment with our theory of change.

Output
Direct impact

A crucial first step in understanding the impact of any intervention, especially within a theory of change, is to clearly define and measure outputs. Outputs are the direct products or services that result from an activity, the immediate results that can be directly attributed to the effort. Measurement begins with these outputs and gradually expands to include outcomes.

Within Summa's Cybersecurity sub-theme, our portfolio companies should measure outputs such as Terabytes of zero-loss storage capacity supplied, share of customer log volume monitored, share of customers in critical industries (e.g. Critical National Infrastructure Providers), and share of customers considered SMEs. The KPIs selected by each company to measure its contribution to the theory of change should align with its core products and services. Additional product-specific output KPIs can be added over time as measurement matures.

Outcome
Indirect impact

The indirect effects or outcomes of our investments are not always easy to measure. However, all our investments are in line with the trajectory laid out below.

Outcomes represent the changes in behavior, conditions, or status that result from the outputs. While outputs are what we do, outcomes are what happens as a result of our actions. For Summa's Cybersecurity sub-theme, examples of outcomes include reduction in mean time to detect and respond (MTTD/MTTR), increase in recovery scope and reduction in recovery time, improvement in industry cyber-maturity indices, with particular progress among critical industries and SMEs.

These outcomes are often more complex to quantify than outputs. Even so, they are essential for demonstrating the real impact and progress towards our strategic goals. Companies are also expected to set ambitious targets to maintain a strategic focus on achieving the desired positive outcomes. They could also use customer case studies, surveys, and other stakeholder activities to assess their impact.

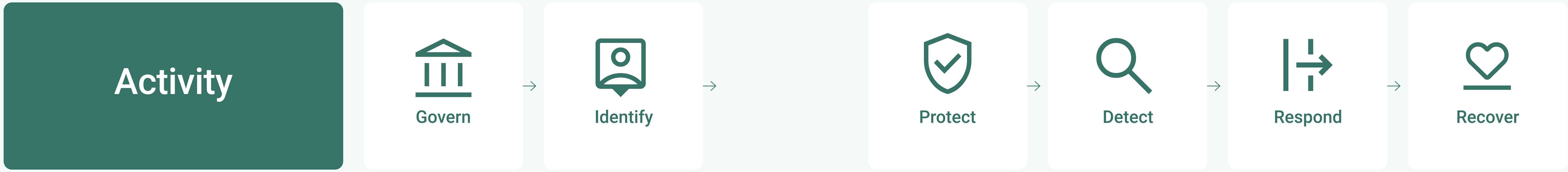
Impact
Indirect impact

Impact represents the long-term, systemic changes that result from sustained outcomes. While outcomes are the direct consequences of our activities, impact reflects the broader societal and environmental benefits that advance our mission. For Summa's Cybersecurity sub-theme, this means realizing a future where everyone can use cyberspace safely and securely, with the confidentiality, integrity and availability of information, products and services provided in and through cyberspace assured.

Looking ahead, we recognize that this long-term vision cannot be realized by Summa in isolation. It requires collaboration with multiple stakeholders, including industry experts, academia and regulators. For some of the challenges, regulatory changes outlined earlier are necessary to drive change. This theory of change guides all our activities and ensures that we remain focused on creating a positive, lasting impact on cyberspace.

[80] (Summa Analysis, 2025)

Figure 16
Summa's focus within the identified activities that can prevent, withstand, or help protect from attacks[56]



Activities we seek to invest in: Summa solutions

Achieving a cybersecure future will require coordinated action across society. Shaping cultural norms, setting clear rules, and ensuring credible enforcement are essential, but they lie outside Summa's investment mandate. Our focus is on enabling the safe design, operation, and deployment of connected products and services, an area where both public and private sector engagement is critical.

Today's gap is stark. Summa and CEPS analysis shows that, given expected annual losses and the effectiveness of current tools, organizations would need to more than double their cybersecurity spending to minimize the impact of attacks. Progress is required across all capabilities, and achieving it depends on technologies and services provided by cybersecurity vendors. This creates a strong opportunity for targeted, high impact investments.

Before turning to the specific solutions that address each capability gap, it is important to note the cross-cutting features we seek in any cybersecurity company. As discussed earlier, adoption is held back less by ignorance than by structural frictions: distorted incentives, scarce talent, fragmented tools, and trade-offs around privacy and sovereignty. We therefore prioritize firms whose products and services help overcome these barriers. We look for solutions that are independently certified as best-in-class to reduce information asymmetries. They should be automated or delivered "as-a-Service" to ease talent bottlenecks. They should also be designed to integrate with adjacent technologies so multiple needs can be met on fewer platforms. Finally, they must comply with European requirements to minimize perceived trade-offs against other desirable outcomes, including legal certainty and data sovereignty.

Govern
As discussed, weak governance leaves downstream controls fragmented and underfunded. We invest in firms that address this by providing security consulting services and governance, risk and compliance (GRC) tools that bring clarity to decision rights, accountability, and prioritization. Solutions such as compliance automation, automated policy management, and board-level reporting tools, turn cyber from ad hoc spending into managed enterprise risk, ensuring that investment in other functions is well directed and sustained.

Identify
Earlier we established how limited visibility leaves organizations blind to exposures they often only discover after a breach. Summa invests in firms that deliver security risk assessment and management services, continuous vulnerability and configuration testing, penetration testing, and external attack surface monitoring. Risk-based prioritization tools help organizations focus on fixing the most important risks, preventing many breaches still caused by known, unpatched flaws.

Protect
Gaps in basic safeguards highlighted earlier make prevention the most powerful way to limit attacker opportunities. We invest in companies that strengthen identity and access management, data protection, and web security through technologies such as multi-factor authentication, single sign-on, encryption, immutable archiving, API security, and modern web application firewalls. Managed Security Service Providers (MSSPs) extend these protections to smaller firms that lack in-house capacity. By closing the most common and recurring entry points, these solutions reduce breach probability, particularly in critical sectors and among SMEs.

Detect & Respond
Detection delays and inconsistent responses significantly amplify losses, even after an intrusion is identified. To solve this problem, we invest in companies that enhance security operations and management: SIEM, UEBA, and XDR platforms that correlate telemetry and SOAR tools that automate response playbooks. Managed Detection and Response (MDR) providers extend this capacity to companies of all sizes. By shortening dwell times and enabling swift containment, these solutions transform late discovery into early intervention, cutting both disruption and fallout.

LOGPOINT

Detect Respond

Logpoint delivers threat detection and response with a European-native SIEM and SOAR platform. As a trusted alternative to US providers, Logpoint aligns with Europe's data protection laws and sovereignty needs. The integration of Munnin's endpoint detection and XDR capabilities provides comprehensive, automated defense, helping over 1000 clients prevent, detect, and respond to cyber threats.

Recover
Summa focuses on closing recovery gaps, so firms aren't paralyzed long after attacks. We invest in solutions like immutable backups, air-gapped storage, Disaster Recovery as a Service (DRaaS) and business continuity planning. These ensure data integrity and enable recovery to happen within hours or days, instead of months. For instance, Summa's portfolio company, FAST LTA, provides sovereign and immutable storage for critical sectors like healthcare.

FAST LTA

Recover

Fast LTA offers high-security, immutable data storage for sensitive data in healthcare, government, and other critical sectors. Its solutions use WORM (Write Once, Read Many) technology and Air Gap architectures to ensure long-term data integrity and compliance against ransomware and data manipulation risks. The on-premise, energy-efficient infrastructure allows public institutions to maintain full control and digital sovereignty over their data within EU jurisdiction. The FAST LTA FLEX solution provides a cloud-like experience with pay-per-use billing while keeping primary data in the customer's own data center.

Detect

vyntra

vyntra combines financial crime prevention and transaction observability to redefine trust and transparency in financial services. By enabling financial institutions to detect and hinder fraudulent transactions and money laundering, they act as a deterrent to cybercriminals.

Unlocking the full potential of cybersecurity

Momentum is building. Rising attack volumes, stricter regulation and reporting requirements, greater litigation risk, and shifting consumer expectations are already driving organizations to improve their cybersecurity capabilities. As demand for talent, products, and services grows, supply must keep pace, supported by targeted investments in education, R&D, and infrastructure.

However, incremental progress is not enough. Achieving economy-wide resilience will require a step-change in capability. That means addressing market inefficiencies through government intervention and accelerating innovation across cybersecurity products, services, and business models.

Governments have a critical role to play. Regulatory standards and compliance mandates can drive investment. Certification and labelling schemes help overcome information gaps. Liability frameworks ensure accountability. Incident reporting and information-sharing requirements improve coordination.

Innovation must follow. Cybersecurity-as-a-Service offerings and automation can ease talent constraints. End-to-end platforms can replace fragmented point solutions. Scalable models must serve organizations of all sizes, especially SMEs and critical infrastructure. Clear and credible quality signals must help buyers choose what works.

This is not just a security imperative. It is a strategic opportunity to build a more resilient, sovereign, and competitive digital economy for Europe.

Image: Fast LTA

SPOTLIGHT

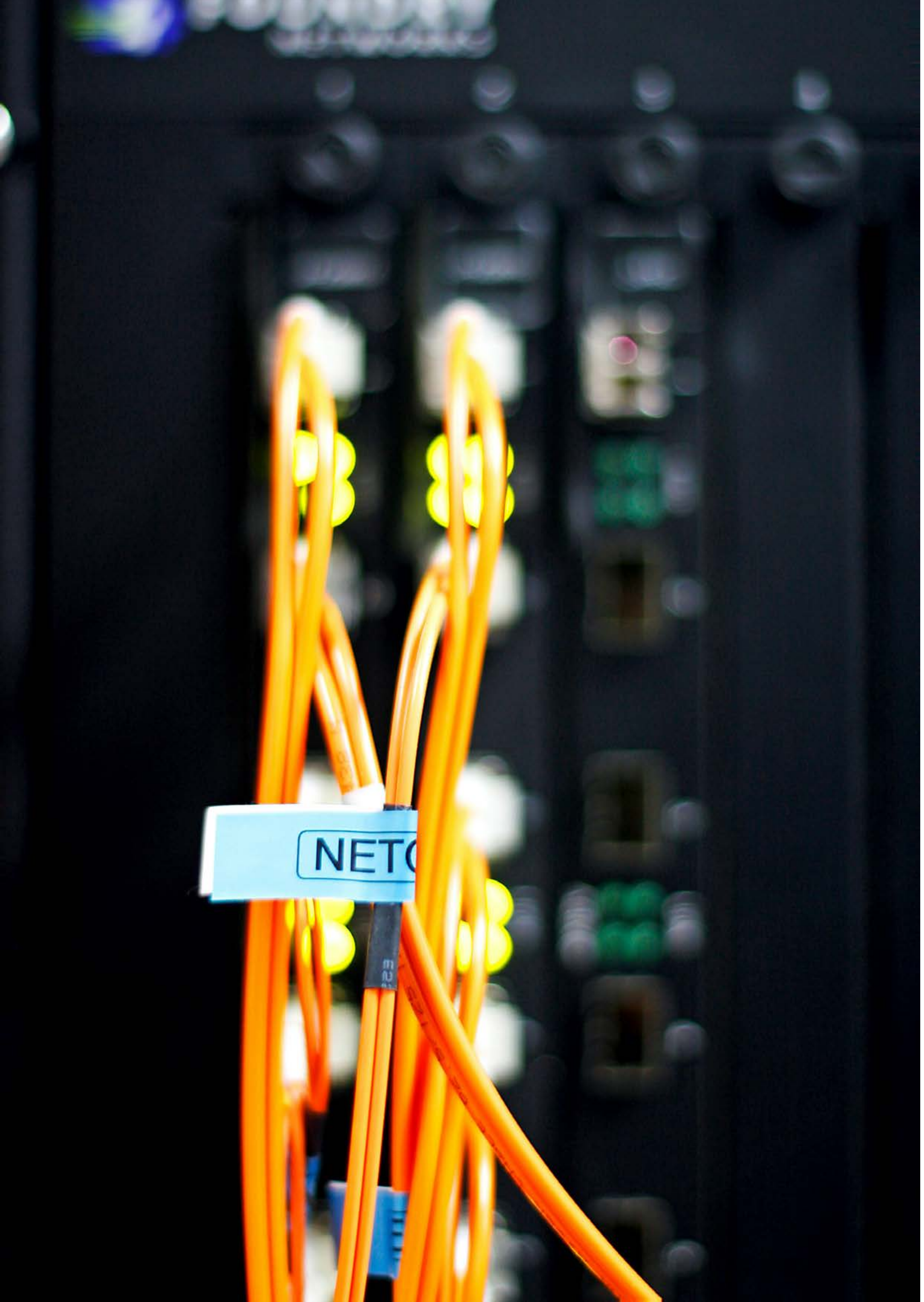
Embedding cybersecurity across the portfolio

Cybersecurity is not a siloed concern, it requires action across multiple levels. While this report focuses on the investment opportunity, Summa also works hands-on with its portfolio companies to strengthen their cyber resilience.

We equip boards and management teams with targeted training, track cybersecurity maturity through our annual sustainability data collection, and support implementation of key safeguards. This includes cybersecurity policies, employee training, attack simulations, backup solutions, and insurance coverage.

Because cybersecurity needs vary by business model and evolve rapidly, we maintain an active dialogue with our portfolio companies to ensure they have the right competencies in place.

Our Via Summa Compliance framework already covers core policies and procedures. From 2025, this includes cybersecurity, governance standards, accountability, and continuous improvement across the portfolio.



End notes

Summa sees cybersecurity not just as a risk to be managed, but as one of the most compelling investment opportunities of the decade.

The current trajectory of digitalization presents growing systemic risks. Without decisive action, cyber threats will continue to undermine trust, disrupt operations, and erode the resilience of critical infrastructure. This is no longer a distant possibility. It is a rapidly unfolding reality.

Summa views this inflection point as both a challenge and a catalyst. The urgency for transformation creates strong conditions for innovation, scale, and competitive returns. By investing in solutions that address the root causes of cyber vulnerability, we can deliver both impact and financial performance.

Inaction is not an option. We must transition toward secure-by-design systems, resilient digital infrastructure, and trusted data environments. This shift demands investment across the cybersecurity value chain. From identity and access management to threat detection, and recovery capabilities.

With cybersecurity spending expected to increase fourfold until 2040, the sector offers strategic importance and strong market potential. Summa's investments in Logpoint and FAST LTA reflect this opportunity. Logpoint provides European organizations with trusted tools to detect and respond to threats, while FAST LTA helps public institutions keep sensitive data safe and under their control. Both companies show how cybersecurity solutions can deliver impact, support digital sovereignty, and offer compelling commercial value.

This transition requires overcoming legacy practices, navigating regulatory complexity, and scaling new technologies. Summa is committed to driving systemic change. By aligning capital with high-impact cybersecurity solutions, we can build a resilient digital economy that delivers long-term value for organizations, individuals, and society.
This is not just about mitigating risk. It is about shaping a secure and resilient future.

References

1. Sommerset I., Wiik-Nielsen J., Oliveira V.H.S, Moldal T., Bornø G., Haukaas A. and Brun E. Norwegian Fish Health Report 2022, Norwegian Veterinary Institute Report, series #5a/2023, published by the Norwegian Veterinary Institute in 2023

Ablon, L. (2018). Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data. RAND Corporation. https://doi.org/10.7249/CT490

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1). https://doi.org/10.1093/cybsec/tyy006

BEA. (2022). New and Revised Statistics of the U.S. Digital Economy, 2005–2021. https://www.bea.gov/sites/default/files/2022-11/new-and-revised-statistics-of-the-us-digital-economy-2005-2021.pdf

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. The Geneva Papers on Risk and Insurance - Issues and Practice, 40(1), 131–158. https://doi.org/10.1057/gpp.2014.19

BlackFog. (2025, Juni 12). Marks & Spencer Breach: How A Ransomware Attack Crippled a UK Retail Giant. https://www.blackfog.com/marks-and-spencer-ransomware-attack/

Canadian Minister of National Defence. (2022). An introduction to the cyber threat environment. Communications Security Establishment = Centre de la sécurité des telecommunications.

CEPS, & Summa Equity. (2025, März 12). CEPS Contribution to Cybersecurity Publication Summa Equity—Final Report. Available upon request.

Chandramouli, R. (2019). Security Strategies for Microservices-based Application Systems (No. NIST Special Publication (SP) 800-204). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-204

Cisco. (2024). Cisco Annual Internet Report—Cisco Annual Internet Report (2018–2023) White Paper. Cisco. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

CPS. (2018). Cybercrime—Prosecution guidance. https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

UK Home Office. (2025). Cyber security breaches survey 2025.
https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breachessurvey-2025

Cybersecurity, and Infrastrucutre Security Agency (CISA). (2020). COST OF A CYBER INCIDENT: SYSTEMATIC REVIEW AND CROSS-VALIDATION.

Cyberspace, n. (2023). In Oxford English Dictionary (3. Aufl.). Oxford University Press. https://doi.org/10.1093/OED/7100956222

Deloitte. (2022). How should organisations prepare for the revised EU policy on cybersecurity? | Deloitte Finland. https://www.deloitte.com/fi/fi/services/consulting-risk/perspectives/how-should-organisations-comply-with-the-revised-eu-policy-on-cy.html

Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J., & Winkelman, Z. (2018). Estimating the Global Cost of Cyber Risk: Methodology and Examples. RAND Corporation. https://doi.org/10.7249/RR2299

Dubois, L. (2025, Juni 10). EU to 'step up' on cyber security as dependence on US laid bare. Financial Times. https://www.ft.com/content/9ee8ad1f-65e9-49ea-a3a4-ead3a0c0da25

EIOPA. (2025). Digital Operational Resilience Act (DORA). https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

ENISA. (2024a). 2024 Report on the State of the Cybersecurity in the Union. https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

ENISA. (2024b). ENISA threat landscape 2024: July 2023 to June 2024. Publications Office. https://data.europa.eu/doi/10.2824/0710888

ENISA. (2025). ENISA NIS360 2024. https://www.enisa.europa.eu/publications/enisa-nis360-2024

European Commission. (2020). The EU's Cybersecurity Strategy for the Digital Decade | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Commission. (2025). 2025 State of the Digital Decade package | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/2025-state-digital-decade-package

European Commission. Joint Research Centre, Baldini, G., Barrero, J., Draper, G., Duch-Brown, N., Eulaerts, O., Geneiatakis, D., Joanny, G., Kerckhof, S., Lewis, A., Martin, T., Nativi, S., Neisse, R., Papameletiou, D., Hernandez Ramos, J. L., Reina, V., Ruzzante, G. L., Sportiello, L., Steri, G., & Tirendi, S. (2020). Cybersecurity, our digital anchor: A European perspective. Publications Office. https://data.europa.eu/doi/10.2760/967437

European Council. (2024). Cyber resilience act: Council adopts new law on security requirements for digital products. Consilium. https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products

Eynon, R., Deetjen, U., & Malmberg, L.-E. (2018). Moving on up in the information society? A longitudinal analysis of the relationship between Internet use and social class mobility in Britain. The Information Society, 34(5), 316–327. https://doi.org/10.1080/01972243.2018.1497744

F5. (2025). API Security Risks and Challenges. F5, Inc. https://www.f5.com/company/blog/api-security-risks-and-challenges

FBI. (2025). The FBI and International Law Enforcement Partners Intensify Efforts to Combat Illegal DDoS Attacks [Page]. Federal Bureau of Investigation. https://www.fbi.gov/contact-us/field-offices/anchorage/fbi-intensify-efforts-to-combat-illegal-ddos-attacks

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. Journal of Information Security, 06(01), 24–30. https://doi.org/10.4236/jis.2015.61003

HarfangLab. (2025, Juli 3). European businesses are rethinking digital dependencies and placing increased importance on sovereignty in cybersecurity. https://harfanglab.io/press/european-businesses-are-rethinking-digital-dependencies-and-placing-increased-importance-on-sovereignty-in-cybersecurity/

Houngbonon, G. V., & Liang, J. (2017). Broadband Internet and Income Inequality. HAL Open Science.

IBM Institute for Business Value, 2025. From: https://www.ibm.com/thought-leadership/institutebusiness-value/en-us/report/unified-cybersecurity-platform

IBM. (2025). Cost of a data breach 2025. https://www.ibm.com/reports/data-breach

Iftikhar, S. (2024). Cyberterrorism as a global threat: A review on repercussions and countermeasures. PeerJ Computer Science, 10, e1772. https://doi.org/10.7717/peerj-cs.1772

Ignatuschtschenko, E., Roberts, T., & Cornish, P. (2016). Cyber Harm: Concepts, Taxonomy and Measurement. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2828646

IMF. (2024a). Global Financial Stability Report, April 2024: The Last Mile: Financial Vulnerabilities and Risks. International Monetary Fund. https://doi.org/10.5089/9798400257704.082

IMF. (2024b). Rising Cyber Threats Pose Serious Concerns for Financial Stability. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability?utm_source=chatgpt.com

Mandelcorn, S. M. (2013). AN EXPLANATORY MODEL OF MOTIVATION FOR CYBER-ATTACKS DRAWN FROM CRIMINOLOGICALTHEORIES.

McKenzie, T. M. (2017). Is cyber deterrence possible? Air University Press, Air Force Research Institute.

McKinsey. (2021). Organizational cyber maturity: A survey of industries | McKinsey. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/organizational-cyber-maturity-a-survey-of-industries

Michael Chertoff, Latha Reddy, Marina Kaljurand. (2019). GCSC Advancing Cyberstability. Global Commission On the Stability of Cyberspace (GCSC).
Microsoft. (2024). Microsoft-Bericht über digitale Abwehr 2024. https://www.microsoft.com/de-de/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Moens, B. (2025, Juli 21). Can Europe break free of American tech supremacy? Financial Times. https://www.ft.com/content/5e25c397-61d1-4b48-b5c5-65561a4c9df2

NIST. (2020). Cybersecurity Risk: Glossary. https://csrc.nist.gov/glossary/term/cybersecurity_risk

NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (No. NIST CSWP 29; S. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

OECD. (2012). The Impact of Internet in OECD Countries (OECD Digital Economy Papers). Organisation for Economic Co-Operation and Development (OECD). https://doi.org/10.1787/5k962hhgpb5d-en

OECD. (2024). OECD Digital Economy Outlook 2024 (Volume 2): Strengthening Connectivity, Innovation and Trust. OECD Publishing. https://doi.org/10.1787/3adf705b-en

Office for National Statistics (UK). (2020). Crime in England and Wales—Office for National Statistics. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2020

Oxford University Press. (2023). Oxford English Dictionary (3. Aufl.). Oxford University Press. https://doi.org/10.1093/oed/7100956222

Pell, S., Wilde, G., & Landi, E. (2024). Lawfare Daily: Law Enforcement Hacking as a Tool Against Transnational Cyber Crime. Lawfare. https://www.lawfaremedia.org/article/lawfare-daily-law-enforcement-hacking-as-a-tool-against-transnational-cyber-crime

PurpleSec. (2024). 2024 Cybersecurity Statistics: The Ultimate List Of Stats, Data & Trends. https://purplesec.us/resources/cybersecurity-statistics/

PWC. (2024). 2025 Global Digital Trust Insights. PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html

PwC & Institute/HKCGI. (2023). Governance gaps in cybersecurity practices revealed: Urgent action needed. https://www.pwchk.com/en/press-room/press-releases/pr-191023.html

Ryng, J., Guicherd, G., Saman, J. A., Choudhury, P., & Kellett, A. (2022). Internet Shutdowns: A Human Rights Issue. The RUSI Journal, 167(4–5), 50–63. https://doi.org/10.1080/03071847.2022.2156234

Smith, Z. M., Lostri, E., & Lewis, J. A. (2020). The Hidden Costs of Cybercrime.

SonicWall. (2023, Februar 21). 2023 SonicWall Cyber Threat Report: Shifting Front Lines. SonicWall. https://www.sonicwall.com/news/2023-sonicwall-cyber-threat-report-casts-new-light-on-shifting-front-lines-threat-actor-behavior

Bitkom e.V. (2020). Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt. https://www.bitkom.org/sites/main/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf

State of Cybersecurity 2023 | ISACA. (o. J.). Abgerufen 20. August 2025, von https://www.isaca.org/resources/reports/state-of-cybersecurity-2023

UNESCO. (2019). UNESCO's internet universality indicators: A framework for assessing internet development. UNESCO.

United Nations. (2022). Internet shutdowns: UN report details 'dramatic' impact on people's lives and human rights. OHCHR. https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human

Verizon Business. (2025). 2025 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

Verleysen, C. (2016). Cybercrime: A theoretical overview of the growing digital threat. Universität Tübingen. https://doi.org/10.15496/PUBLIKATION-23063

Weber, C. (2024). Kosten und Schäden durch Cyber- Kriminalität in Deutschland.

WEF. (2020, Januar 21). Why we need to partner in the fight against cybercrime? World Economic Forum. https://www.weforum.org/stories/2020/01/partnerships-are-our-best-weapon-in-the-fight-against-cybercrime-heres-why/

Wiggers, K. (2025, Juni 3). AWS establishes new German corporate presence to advance European sovereign cloud. TechCrunch. https://techcrunch.com/2025/06/03/aws-establishes-new-german-corporate-presence-to-advance-european-sovereign-cloud/

World Bank. (2024). Digital Progress and Trends Report 2023. The World Bank. https://doi.org/10.1596/978-1-4648-2049-6

World Economic Forum. (2024). WEF_Strategic_Cybersecurity_Talent_Framework_2024.

World Economic Forum. (2025). Global Risks Report 2025. Forum Publishing.

Wright, D., & Kumar, R. (2023). Assessing the socio-economic impacts of cybercrime. Societal Impacts, 1(1–2), 100013. https://doi.org/10.1016/j.socimp.2023.100013

Investing to solve
global challenges

SUMMA EQUITY