N°2 | October 2025

s:fi KNOWLEDGE

Swiss Finance Institute Roundups

Hacking the Basics of Cybersecurity

Editorial

Cyber threats are projected to cost over USD 10 trillion in 2025, making them one of this decade's fundamental challenges. In this SFI Roundup, experts from academia and industry examine the most critical vulnerabilities and the priority responses. The financial sector remains particularly vulnerable due to decades-old legacy systems and cascading effects on interconnected payment networks. Rather than relegating cybersecurity to IT departments, boards must recognize it as a strategic concern requiring continuous investment and cultural change, where every employee understands their defensive role. As ransomware gangs and state-sponsored actors blur together, and centralized cloud providers create dangerous single points of failure, the path forward requires not just better technology but reimagining how we balance efficiency with resilience in our hyperconnected world.

We wish you an informative and thought-provoking read.

Prof. François Degeorge
Managing Director

Contributors

Alain Beuchat
Alain Beuchat was Chief Information Security Officer at Lombard Odier, responsible for cyber resilience, information security strategy, and regulatory compliance across the organization, until his retirement in June 2025. He is also a member of the Swiss Academy of Engineering Sciences' (SATW) Cybersecurity Advisory Board. He holds a Master of Science in Electrical Engineering from EPFL, the Swiss Federal Institute of Technology in Lausanne.

Marc Henauer
Marc Henauer is the Senior Political and International Affairs Officer at the Swiss National Cyber Security Centre (NCSC). Previously, he led the Swiss MELANI Operation and Information Centre, where he coordinated the monitoring of cyber threats and advanced Switzerland's cyber situational awareness. At the NCSC, he focuses on national and international cybersecurity policy development. He holds a Master of Arts in Foreign Service and National Security Studies from Georgetown University.

Anastasia Kartasheva
Anastasia Kartasheva is an SFI Faculty Member and Associate Professor at the School of Finance, as well as Director at the Swiss Institute for International Economics and Applied Economic Research, at the University of St.Gallen. Before taking her current position, she worked as an economist at the Bank for International Settlements (BIS). She holds a PhD in Economics from the *Université Toulouse Capitole*.

Olivier Scaillet
Olivier Scaillet is an SFI Senior Chair and Professor of Finance and Statistics at the University of Geneva. His research focuses on econometric theory and its applications in finance and insurance. In addition to his academic work, he shares his risk management and modeling expertise with several Swiss-based banks. He holds a PhD in Applied Mathematics from the *Université Paris Dauphine*.

Beat Schär
Beat Schär is Head of IT Security and Architecture at the Swiss National Bank (SNB), where he oversees the design and implementation of secure IT frameworks, aligns the institution's cybersecurity strategy with national and international regulatory standards, and contributes to cross-departmental efforts to safeguard critical systems. He holds a Master of Applied Science in Information Technology and Electrical Engineering from ETH Zurich, the Swiss Federal Institute of Technology in Zurich.

Fabian Schär
Fabian Schär is an SFI Faculty Member and Assistant Professor for Distributed Ledger Technology and Fintech at the University of Basel. He is a visiting researcher at the International Monetary Fund (IMF), a technical advisor to the Committee of Payments and Markets Infrastructure, and an invited expert for numerous central banks, the Bank for International Settlements (BIS), the Financial Stability Board (FSB), and the G20. He holds a PhD in Economics from the University of Basel.

October 2025 (interviews and data as of September 2025)

The Essentials

What is cybersecurity, and how is it structured?

Beat Schär: Cybersecurity refers to the protection of information technology (IT) systems, networks, and data from unauthorized access, damage, or disruption. While the technical foundations—such as protecting confidentiality, integrity, and availability—are common across organizations, the specific priorities and risks depend on the nature of the business. For example, a wealth manager depends on secure customer data; a central bank requires system security, availability, and independence; a manufacturer relies on the integrity of automated production lines; and an online store needs secure payment processing and uptime during peak traffic. In today's economy, nearly every industry relies on interconnected IT systems, making cybersecurity a core strategic concern—albeit one that looks different from one company to the next.

Alain Beuchat: Confidentiality, integrity, and availability form the foundation of cybersecurity. They are deeply interconnected: It is common to see trade-offs, tensions, and complementary or cascading failures among them. Confidentiality protects a user's identity and ensures they can access the right data. Integrity protects data and systems from unauthorized modification. Availability ensures that users can access the data and infrastructure when they need to. Cyberattacks can target all three components: Phishing attacks attempt to obtain login credentials, giving hackers unauthorized access to data. Ransom attacks aim to disrupt data integrity and confidentiality. Distributed Denial-of-Service (DDoS) attacks flood servers, making websites unavailable to legitimate users. To put these three components of cybersecurity into practice, organizations implement layered security controls, such as encryption, access management, DDoS and malware protection, system monitoring, and incident response plans that specifically address risks to confidentiality, integrity, and availability.

How does cybersecurity fit into the broader security puzzle?

Fabian Schär: Fabian: As soon as two pieces of hardware or software interact, they become vulnerable to attacks, and cybersecurity needs to step in. Security, in its broadest sense, is about protecting against threats. These threats can take many forms—physical, digital, emotional, or institutional. While cybersecurity focuses on defending IT systems and data from digital attacks, it has a ripple effect on other areas of security, including national security, economic security, and personal security.

Marc Henauer: At its core, cybersecurity is about managing different types of risk across our economy and society. It is worth noting that cybersecurity is not an extra layer of processes that someone can choose to adopt; rather, it changes how existing processes are executed. For example, in the past, critical information was mostly sent via sealed letters or telegraphs. Now, it is sent through instant messaging systems. Cybersecurity has not created messaging itself, but rather adjusted how it is done today to ensure it remains secure.

Olivier Scaillet: In the banking sector, the Basel Committee on Banking Supervision offers helpful guidance by classifying risks into three main categories: credit risks, market risks, and operational risks. Cyber risk falls under operational risks. However, it stands out due to its malicious intent, higher likelihood of occurrence, potential for hidden and prolonged disruption, and ability to spread through digital interconnectedness. These characteristics show that traditional operational risk frameworks are insufficient. Cyber risk requires dedicated, forward-thinking strategies in management oversight, regulatory design, and risk insurance.

Anastasia Kartasheva: From an insurance standpoint, cybersecurity risk is also viewed as an operational risk due to its impact on data confidentiality, integrity, and availability, as well as on IT infrastructure. These risks can involve unauthorized access, leading to data breaches, malware attacks, and internal system errors that compromise data security. Unlike other risks, such as health risks or the risk of a natural disaster, there has been limited development of methods to transfer cybersecurity risks. As a result, firms have minimal insurance protection against cybersecurity risks, leaving them largely to fend for themselves when dealing with the consequences of an attack.

How do cyberattacks differ between opportunistic and targeted actors?

Alain Beuchat: Most cyberattacks are opportunistic, not targeted. Attackers scan the internet for known vulnerabilities, exploit them, and then figure out who the victim is. Once they have gained access, the attackers—often working in multiple layers—decide on the ransom amount based on the victim's size and sensitivity. It has to hurt, but not so much that the victim cannot pay. Targeted attacks are different, involving long-term surveillance, strategic intent, and often geopolitical motives. These operations—often tied to nation-state actors—can take months or even years to prepare and typically focus on government agencies or critical infrastructure. Both types of threats coexist, and understanding their logic is crucial for mapping risks and planning responses. A strong defense starts with knowing not just how attackers operate, but also why.

What recent figures best illustrate the scale of today's cyber threats?

Olivier Scaillet: Experts predict the global cost of cybercrime will surpass USD 10 trillion in 2025, a huge leap from USD 3 trillion in 2015. While these staggering figures are tough to confirm, they underscore the massive scope of the issue and its alarming growth rate. With cyberattacks and overall vulnerability on the rise, some projections suggest the cost could hit USD 25 trillion by 2027. Consequently, cybersecurity and cyber risk have become major concerns for governments, businesses, and individuals alike.

What recent cybersecurity incidents do you think best illustrate the state of the field?

Olivier Scaillet: One of the most damaging attacks is likely the 2017 NotPetya attack. From an operational risk standpoint, it forced the affected companies to shut down for weeks, disrupting their ability to produce goods and services. This ripple effect hit their customers, who suffered significant losses—four times greater than the directly affected companies. These operational risks were worse for customers with few alternative suppliers or those relying on highly specialized goods. From a reputational risk perspective, the breach led customers to end business relationships with the directly affected companies over time. Even a year after the attack, customers were more likely to cut ties with those companies, showing a long-term erosion of trust and reliability. Customers restructured their supply chains to partner with companies with stronger cybersecurity profiles, indicating that the attack harmed the reputation of affected suppliers as reliable business partners. The NotPetya attack is one of the most sophisticated attacks to date and underscores the widespread consequences such attacks can carry over time.

Anastasia Kartasheva: The Colonial Pipeline shutdown of 2021 serves as a textbook example. The company, which supplies nearly half of the fuel consumed on the United States' East Coast, experienced a ransomware attack. As a precaution, they shut down their systems. Even though they paid a ransom of approximately USD 4.4 million in Bitcoins just a day after the attack, it took them nearly a week to resume full service, resulting in fuel shortages in several states, panic buying, and prices at the pump that jumped by up to 10 cents per gallon. The impact of an attack like this one that exploits just one compromised password on critical infrastructure can be significant, affecting the lives of millions. It is also essential to consider the "small" cost of the ransom, compared to the total economic and social costs associated with the shutdown.

Marc Henauer: The Viasat attack, which occurred on the same day as Russia's invasion of Ukraine in 2022, aimed to disrupt the satellite communications used by thousands of Ukrainians, including military and government agencies. This attack, targeted at Ukraine, had spillover effects far beyond anything that could have been predicted. The scope of collateral damage was vast, with approximately 6'000 wind turbines malfunctioning in Germany, fixed broadband users across Europe experiencing outages and requiring hardware replacements, and satellite telephone users in Morocco and the United Kingdom facing connectivity issues.

Alain Beuchat: The CrowdStrike incident of 2024, caused by a routine software update, resulted in more than 5'000 flights being canceled, hospitals postponing non-emergency procedures, and banks worldwide experiencing online banking outages. Although there is no evidence that the CrowdStrike incident was a result of malicious activity, its scale of disruption exceeds that of any cyberattack that has ever occurred and highlights the vulnerability of centralized IT systems. Such incidents emphasize the interdependency of our cyber systems: A glitch, whether ill-intentioned or accidental, can impact not only a single computer, but also the functioning of a device connected to an IT network many time zones away. In addition to the abovementioned incidents, we continue to observe a high volume of cyberattacks targeting organizations and their third-party suppliers. Many of these breaches stem from the absence of fundamental cybersecurity practices, such as inconsistent patch management or the lack of multi-factor authentication.

Core Concepts

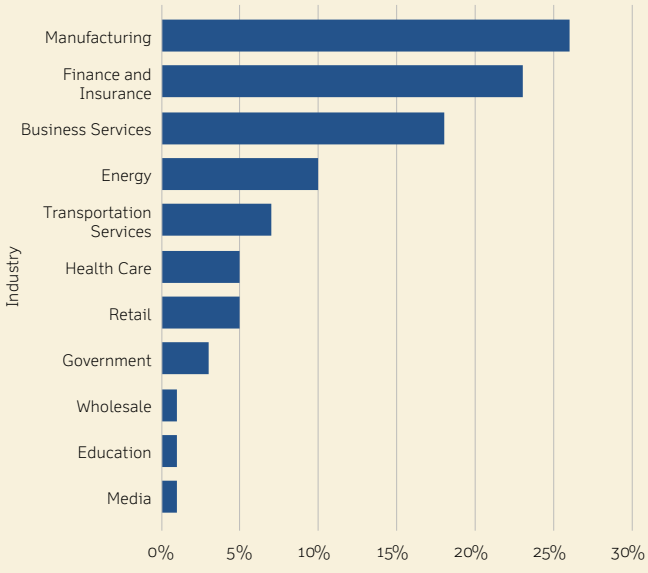
How are cybersecurity functions structured and implemented?

Beat Schär: Cyber risk management is often organized into three lines of defense: risk ownership, risk oversight, and independent auditing. The first, risk ownership, involves identifying, evaluating, and mitigating cybersecurity risks related to the company's specific context. Internal cybersecurity specialists usually support these activities. The second, risk oversight, involves monitoring whether risks are effectively identified and managed. This responsibility usually falls to the company's internal risk department. The third, independent auditing, provides an external assessment of cybersecurity controls, policies, and risk management practices. This three-tier approach minimizes blind spots, ensures checks and balances across organizational functions, and aligns cyber risk management with broader governance and compliance standards.

Who are the main attackers and the prime victims of cyberattacks?

Marc Henauer: Attackers are highly rational and opportunistic, targeting victims who cannot afford top-notch security but who have enough financial resources to pay the ransom. Their victims include almost anyone connected to a network, from large corporations and government agencies to small businesses, educational institutions, research institutions, nonprofits, NGOs, and individuals. Anyone with valuable infrastructure and data, along with financial resources, can become a target. A notable example is the 2017 breach of a casino's network, where hackers exploited a poorly secured internet-connected fish tank thermometer to extract 10 GB of data from the casino's high-roller database. This incident has since become a classic example of how even the most trivial smart device can become a gateway to sensitive information if not properly secured.

Anastasia Kartasheva: There is a complex web of attackers and victims, and they do not all operate on the same battlefield. On the attacker side, we typically see China, North Korea, and Russia as key players at the nation-state level, with intricate schemes driven by strategic, political, or financial motives. At an individual level, the hackers are often teenagers, especially American ones, who are fluent in English and skilled at social engineering. Their actions tend to be aggressive and focused on specific economic sectors for weeks at a time, with goals ranging from prestige to activism to financial gain. We need to remember that employees can also pose a significant cybersecurity threat and cause considerable damage, whether intentionally or through negligence. On the victim side, government agencies and critical infrastructure operators are prime targets for nation-state hackers, while financial institutions and individuals are generally the victims of financially motivated cybercriminals. Meanwhile, corporations, media outlets, and government institutions are targeted by ideological hackers, or hacktivists.



Note: This figure shows the distribution of cyberattacks across industries in 2024.
Source: IBM X-Force

Which cyberattack vectors are currently most prevalent, and how have they evolved?

Fabian Schär: With the rise of artificial intelligence, social engineering has become increasingly sophisticated. Hackers are using more data and more advanced models to create targeted and sophisticated attacks. Gone are the days of obvious mistakes like typos and grammatical errors. Supply chain attacks have also evolved, with hackers infiltrating many organizations by targeting their software providers. The SolarWinds attack, believed to be linked to the Russian government, is a prime example. In this case, hackers inserted malicious code into a trusted software update, gaining access to thousands of high-profile targets, including U.S. government agencies and Fortune 500 companies. The risk of cyberattacks grows daily, as software and companies become more connected and as we increasingly rely on cloud solutions and third-party services.

What motivates different categories of threat actors—from nation-states to hacktivists—to launch cyberattacks?

Anastasia Kartasheva: They have many different motivations. The current unstable global landscape has made it clear that propaganda, misinformation during elections, and attacks on key infrastructure are being used to gain political or military advantage. Industrial sabotage is also a major concern, particularly for companies with a large international presence that have less direct control over their employees, are more vulnerable to global operations and supply chains, and must navigate multiple complex regulatory systems. Tackling these various threats is an ongoing challenge that presents numerous difficulties, including working with the right third parties, acquiring technical expertise, educating staff, and addressing insider threats.

Fabian Schär: It is also important to consider the time frame. Attacks with short-term horizons are mostly driven by financial gain, while those with long-term horizons have strategic or political motives. The hacking and explosion of thousands of Hezbollah's pagers and walkie-talkies last year, which killed over 40 people and injured more than 3'500, highlights just how sophisticated and well-planned these attacks can be. Nowadays, almost any electronic device can be vulnerable to a cyber incident.

What core principles guide effective cybersecurity governance today?

Beat Schär: Cybersecurity is an ongoing daily responsibility. By taking a risk-based approach, companies can implement effective cybersecurity governance. To begin, they need to conduct a thorough risk assessment to gain a comprehensive understanding of their vulnerabilities, assets, and exposure to cyber threats. Once a risk assessment has been done, management needs to prioritize security measures, take necessary actions, and accept overall responsibility for their decisions. Open internal communication is crucial to promoting good conduct among all staff and to ensuring they are aware of both potential threats and expected behaviors. The risk assessments should then be regularly updated, based on evaluations of cyber threats and the company's growth.

Marc Henauer: Under Swiss civil law, the board of directors and executive board are responsible for managing risk. While there is still room for improvement, companies are becoming more aware of the cyber risks they face. However, it is tough to tell which companies are ahead of the curve and which are falling behind. On the one hand, some small to medium-sized businesses, especially those that are heavily automated or digitalized, have a lot of expertise in this area. On the other hand, some large companies have suffered significant losses and disruptions. For instance, the Danish shipping company Maersk experienced severe capacity issues throughout its global operations in 2017 due to the NotPetya cyberattack, while the pharmaceutical giant Merck is estimated to have lost around USD 900 million in lost sales, operational disruptions, and recovery costs. In the world of cybersecurity, scale is not everything. Whether you are the attacker or the defender, it is often agility and ingenuity that give you an edge, reminding us that size alone does not guarantee victory.

What can be the impacts of major cybersecurity breaches?

Olivier Scaillet: Large-scale cybersecurity breaches can have far-reaching consequences. A study of major U.S. companies listed on the public market found that in the short term, cyberattacks lead to lower returns, higher trading volume, reduced liquidity, and wider bid-ask spreads. However, over time, these companies tend to boost their cybersecurity investments, while their market value and overall performance remain relatively steady. Research on financial institutions shows that cyberattacks can result in losses of up to 50% of annual net income, due to direct financial costs, operational disruptions, and damage to their reputations. Additionally, some breaches can have a ripple effect across financial markets, increasing systemic risk.

Anastasia Kartasheva: Reputational damage is a major concern, especially when sensitive data is compromised. The scope of exposed information can be huge, ranging from tax records and income statements to medical histories, biometric identifiers, location data, and intellectual property. While the impact varies, the costs of reputational harm and litigation are often among the highest. It is crucial to recognize how interconnected companies are—cyber incidents rarely stay isolated and can have far-reaching effects that are tough to control. In the end, each company must not only manage its cybersecurity, but also decide whether paying a ransom is worth it when under attack, considering the potential consequences of refusing to pay.

Fabian Schär: One often overlooked impact of a cyberattack is psychological: anxiety. Just as someone may feel uneasy for a long time after a physical break-in, even after the locks have been changed, a similar unease can linger after a cybersecurity breach. When a hacker infiltrates an organization's IT systems, a sense of violation may remain even after stronger preventive measures are put in place. This lingering doubt—whether another attack will occur—can subtly affect behavior, trust, and decision-making within the organization.

Beat Schär: Major cybersecurity breaches can have significant operational, financial, and reputational consequences. In the financial sector, a severe incident may jeopardize regulatory standing and erode public trust. For example, in Switzerland, the Swiss Financial Market Supervisory Authority (FINMA) has the authority to revoke banking licenses in cases where institutions fail to meet risk management requirements, including those tied to cybersecurity. In the United States, regulatory approaches continue to evolve, with discussions around the balance between mandatory disclosures and effective cybersecurity practices. Some industry associations have raised concerns that certain rules might unintentionally complicate incident response. Despite differing views, regulation generally aims to enhance resilience and accountability throughout the system.

What are the challenges and incentives around inter-organizational threat intelligence sharing?

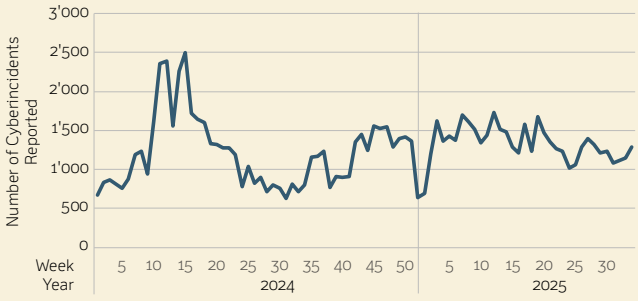
Fabian Schär: Put simply, the answer is "trust." It is logical for companies to work together on cybersecurity and to share their best practices, but to do so means revealing a lot about their internal workings in a competitive landscape where allies and rivals are often the same. A government-led effort, where information is shared in a more anonymous and consolidated way, could be better than direct, one-to-one exchanges.

Alain Beuchat: Having the right information is key, as it raises awareness and helps organizations gauge their risk of being a potential target and prepare for various threats. There are two main channels for acquiring this information: You can buy it from a third party, which allows you to tailor the search for information to your organization, or you can share information among market partners through open source intelligence (OSINT). Using a combination of the two channels is the most effective approach. Another important aspect is the establishment of trusted relationships through these exchanges; such relationships enable the rapid and effective sharing of relevant information in the event of a cyberattack.

Anastasia Kartasheva: One major step forward in improving the sharing of cyber risk information internationally was the Financial Stability Board's (FSB) creation of a lexicon defining cyber terms in 2018. With a common understanding of the differences between alerts, attacks, events, incidents, risks, and threats, it became possible to gather and compare data. However, cyber information can also give attackers an edge. Cyberattackers are highly intelligent and use various tactics to gather information on their potential targets. For example, our local government stores vast amounts of sensitive data, including household wealth. A targeted attack based on stolen tax records on a specific household is bound to be more profitable than a random attack. Overall security relies on the strength of the weakest link.

Marc Henauer: At the national level in Switzerland, the recently implemented Cyber Security Ordinance requires critical infrastructure operators to report cyberattacks to the National Cyber Security Center (NCSC) within 24 hours of discovery and to submit a complete report within 14 days. This rule represents a significant step forward in improving the visibility of such incidents. The Ordinance currently covers public transportation companies, energy suppliers, federal, state, and local authorities, hospitals, and drinking water suppliers, as well as other sectors such as the financial industry. Any attack compromising the confidentiality, integrity, availability, or traceability of information must be reported, including malware successfully installed on a system, encryption trojans, DDoS attacks, and unauthorized access to computer systems through security vulnerabilities. The NCSC analyzes these reports and provides support where needed. By drawing insights from this data, we will gain a better understanding of the global threat landscape. We will be able to identify patterns of attacks on critical infrastructure early on and to alert other potential victims in a timely manner, allowing them to take appropriate preventative and defensive measures. Although it is still too early to gauge the benefits of this process, I strongly believe this regulatory shift toward better intelligence sharing will lead to many success stories.

Cyberincidents Reported to the National Cybersecurity Centre



Note: This figure shows the weekly number of cyberincidents reported to the National Cybersecurity Centre (NCSC) from January 2024 to September 2025.

Sources: National Cybersecurity Centre (NCSC)

Digital Exposure

How should the cost of and responsibility for cybersecurity be shared between the public and private sectors?

Anastasia Kartasheva: Like traditional security, cybersecurity has noticeable spillover effects that often impact the general economy. However, I would be cautious about suggesting that the public sector should fund cybersecurity, due to the potential moral hazard that may arise. There is a big difference between allowing the government to regulate construction in disaster-prone areas, for example, and overseeing cybersecurity. Each company needs to set its own strategy and to decide how much it is willing to invest to reduce its risks.

Marc Henauer: The online world is basically an extension of the physical world, with its good and bad aspects. As in real life, the government has a responsibility to try to create a better, safer environment. However, it is not required to fully achieve this ambitious goal, nor can it be blamed for failing to do so. Just as people are expected to lock their doors and to insure their homes in the real world, it is up to private individuals and companies to protect their digital environment with the appropriate cybersecurity measures.

Fabian Schär: For the best results, each party should focus on its area of expertise. The public sector should prioritize securing key infrastructure, regardless of ownership, while the private sector needs to ensure seamless operations at both the company and industry levels. The regulator's role is to provide clear guidelines on minimum requirements and the overall direction of the economy. It is also essential to encourage collaboration and sharing among various parties, including academics, companies, and government agencies, in whatever format works best.

What do market trends—such as mergers, acquisitions, and the rise of one-stop cloud solutions—reveal about how the industry is responding to cyber threats?

Beat Schär: The push toward consolidation, whether through mergers or a reliance on a few dominant cloud providers, reflects an attempt to streamline organizations and IT systems. Fewer systems simplify management, but they also concentrate risk—making life easier not only for the users, but for the attackers as well. Cloud solutions, though efficient and scalable, come with daily security challenges due to their complex configurations; they are the focus of ever-evolving threats. Diversifying across systems or running parallel clouds improves resilience, but these measures are costly and difficult to manage. As a handful of providers increasingly dominate the market, this centralization creates a dangerous dependency: If one provider fails or is breached, the consequences could be widespread. Ultimately, whether through integration or diversification, each approach brings its own cybersecurity trade-offs.

How does cybersecurity risk exposure differ between the financial and non-financial sectors?

Marc Henauer: Banks were at the forefront of integrating IT into their core operations, starting as early as the 1950s. Initially, computers supported ledger management and accounting, but over time, critical functions such as batch processing, secure financial messaging, ATMs, online banking, and electronic trading were added. This early adoption has created fragmented and legacy-heavy infrastructures. That said, the financial sector tends to adopt structured replacement cycles more consistently than many non-financial industries. IT systems in both the financial and non-financial sectors tend to grow organically—often without a long-term roadmap or regulatory framework defining what infrastructure to include over the coming decade.

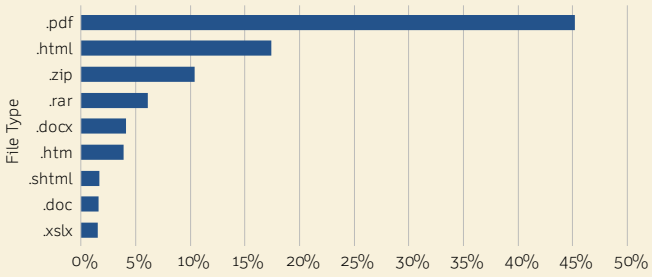
How have organizations improved their preparedness for cyberattacks, and what challenges remain?

Alain Beuchat: Firms have made significant progress in establishing basic cyber hygiene protocols and in selecting the right security tools. In theory, the basics are clear: promptly patch known vulnerabilities, deploy anti-malware protection and monitoring, enforce multi-factor authentication, and ensure backups are stored securely. In reality, however, these seemingly simple steps are hard to implement on a large scale. The challenge lies in doing so consistently across all systems. What makes cyber defense operationally tough is not so much a lack of knowledge, but the sheer complexity of implementing defenses across large networks. Human error, fragmented processes, and delayed patching continue to create vulnerabilities—even when defenses are in place. Real preparedness is less about having the right checklist and more about applying it consistently and quickly.

Olivier Scaillet: As cybersecurity measures grow more complex and expensive, IT departments face mounting pressure to deliver business value. Organizations must carefully decide what to protect, how to protect it, and what they can afford not to protect—decisions inherently fraught with risk and uncertainty. At the same time, management and boards must stay vigilant, as cyber incidents carry significant governance implications. Research shows that successful attacks increase the likelihood of executive turnover, especially for Chief Investment Officers and Chief Information Security Officers, and can even prompt board-level changes when gaps in oversight or preparedness are exposed. These challenges underscore that it is not just regulatory bodies, but also shareholders who hold leadership accountable for cybersecurity failures.

Beat Schär: State-sponsored attacks are getting more sophisticated. Hackers are sneaking malicious code into software updates from trusted third-party providers, making it a discreet way to target a wide range of victims. These attacks show how trusted partners can become a threat and emphasize the importance of zero-trust architecture principles and strict third-party risk management. Since these attacks are highly complex, the chances of early detection or avoiding them are very low. This complexity underscores the need for continuous vigilance, proactive threat modeling, and scenario-based simulations to test and improve organizational resilience.

Marc Henauer: Management must understand that cybersecurity skills are highly specialized, requiring time and effort to grasp the implications and recognize the scenarios. Every employee has a role in cybersecurity, so educating your staff is crucial. When it comes to communication, you need more than just external and top-down internal communication—you also need effective channels that allow end-users to report suspicious IT issues from the bottom up. Ultimately, cybersecurity preparedness must be embedded across the entire organizational culture and not be confined to the IT department.



Note: This figure shows the distribution of malware delivery methods by file type in 2024.
Source: IBM X-Force

What recent cybersecurity investment trends have been most influential in shaping industry practices?

Marc Henauer: There is a growing understanding that ongoing testing is crucial. This testing must cover both technical and procedural aspects, including attack simulations. By broadening the testing environment to include more than just cybersecurity experts, we can ensure that communication—vital for reassuring third parties, investors, and regulators—is also addressed and improved. Artificial intelligence is being used more frequently to enhance security functions and to simulate attacks. The investment in cybersecurity and the cost of cyber incidents are becoming increasingly clear in financial statements, through rising operational expenses and the fallout from cyber incidents.

Fabian Schär: Alongside testing, snapshots and multiple backups form a solid defense against contamination issues and ransomware attacks that could wipe out an entire system. However, it seems that many small and medium-sized enterprises, which are highly susceptible to these risks, have not put a backup system fully in place. While backups and snapshots are not a complete solution for cybersecurity, they do provide a straightforward and cost-effective way to safeguard IT infrastructure from a large portion of today's threats. They do not, however, protect against attacks like data extortion or double extortion, where data is first encrypted and then the attacker demands a ransom to keep it private.

How do financial institutions decide how much to invest in cybersecurity, and what factors shape those decisions?

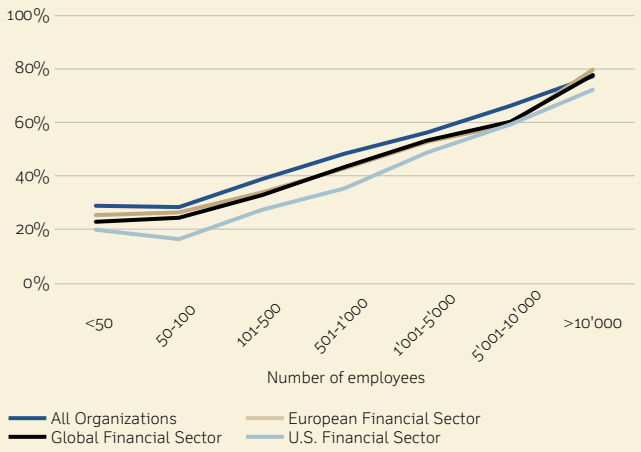
Olivier Scaillet: Put simply, cyber investment decisions are driven by how much financial institutions perceive themselves to be exposed to cybersecurity risk. An analysis of U.S.-listed companies shows that this perception is influenced by several factors, including past cyberattacks, firm and industry characteristics, governance quality, and regulatory or market pressure. Interestingly, companies with higher cybersecurity risk tend to outperform their peers by about 10% annually—yet they underperform sharply when cyber risks materialize. This difference suggests that a distinct cyber risk factor exists and is priced by the market. Financial institutions, given their critical role and heightened exposure, must recognize this evolving threat and ensure that their cybersecurity investments are both proactive and proportionate to their risk profile.

Marc Henauer: It is likely that past experiences, management, and board interests all play a significant role in these decisions. Financial regulators also have a major influence, by establishing the basic requirements for what needs to be done. A key factor in enhancing cybersecurity is having a long-term plan that outlines the financial investments made over time, enabling management to track progress and key milestones.

What are the potential consequences of a cyberattack on core banking or financial messaging systems?

Fabian Schär: Commercial banks must ensure they are serving their customers by handling financial transactions, such as payments, around the clock. Top global banks process up to 100 million transactions daily, including wire transfers, credit card payments, and mobile transactions. When a major bank's core banking system is targeted, it immediately impacts the market, causing money to flow erratically in both financial and real-world markets until alternative banks step in. The primary clearing and settlement system is the backbone of every financial system. Any issue with a messaging network or settlement system—like SWIFT, TARGET2, Fedwire, or the SIX Interbank Clearing system—can have far-reaching consequences and spark panic across the financial sector and the real world, with no regard for international borders.

Known-Exploited Vulnerability Exposure by Firm Size: Economy-Wide and Financial Sector



Note: This figure shows the share of organizations with at least one Known-Exploited Vulnerability (KEV) detected in their infrastructure in 2023, disaggregated by firm size. It includes an economy-wide benchmark covering all sectors, along with aggregated figures for the global financial sector and its European and U.S. components. Firm size categories are defined by number of employees.

Source: Bitsight

How do financial institutions quantify cyber risks for effective management?

Beat Schär: Given the many moving parts and unknowns, accurately quantifying these risks requires considerable extra effort and may provide limited benefits. A broad, scenario-based approach is likely the most effective way to assess the situation and appears to be the standard. Since communicating about cybersecurity is already complex and quantitative cyber risk management is still in its early stages, it is best to keep updates to top management clear and concise.

What cybersecurity risks are introduced through third-party service providers?

Alain Beuchat: Using third-party service providers, whether cloud vendors, outsourced IT, or software providers, has become essential. However, doing so adds a new layer of risk that is increasingly tough to manage. Regulators expect us to apply the same level of controls to our providers as we do within the bank. In reality, this means ongoing audits, lengthy vendor questionnaires, and regular follow-ups to enforce standards beyond our direct perimeter. As outsourcing grows, so does the attack surface. For financial institutions, this poses a dual challenge: enforcing controls on external parties while maintaining internal accountability.

What are the limitations and likely developments in the cyber insurance market?

Beat Schär: Assessing the impact of a cyberattack is relatively easy, but determining the likelihood of being targeted is extremely complex. This complexity makes it tough to accurately gauge your overall risk. One practical approach is to compare your cybersecurity setup with that of your industry peers and aim to surpass them—the goal, as with many risk management areas, is to stay ahead of the curve. That being said, we need to be realistic: Any insurance policy has its gaps, and cyber insurance is no different. Another concern for an insurer is concentration risk—some cloud providers individually account for a substantial share of global computing capacity. This level of concentration raises serious questions about how insurers can manage their exposure to systemic risk in such a highly interconnected digital ecosystem.

Alain Beuchat: The cyber insurance market is maturing rapidly, but so too is our awareness of its limits and liabilities. In earlier years, cyber policies were cheap and loosely underwritten. Today, insurers conduct rigorous due diligence, ask detailed technical questions, and are quick to challenge claims. Their concern is not only cost, but reliability. If an attack on a firm traces back to a misconfigured machine or outdated anti-malware, insurers may invoke exclusions and reduce payouts—regardless of the firm's overall good practices. In many cases, the reputational and client losses that truly hurt are not covered by insurance at all. As premiums rise and exclusions tighten, some institutions are beginning to treat cyber insurance as a last resort, rather than as a cornerstone of their risk strategy.

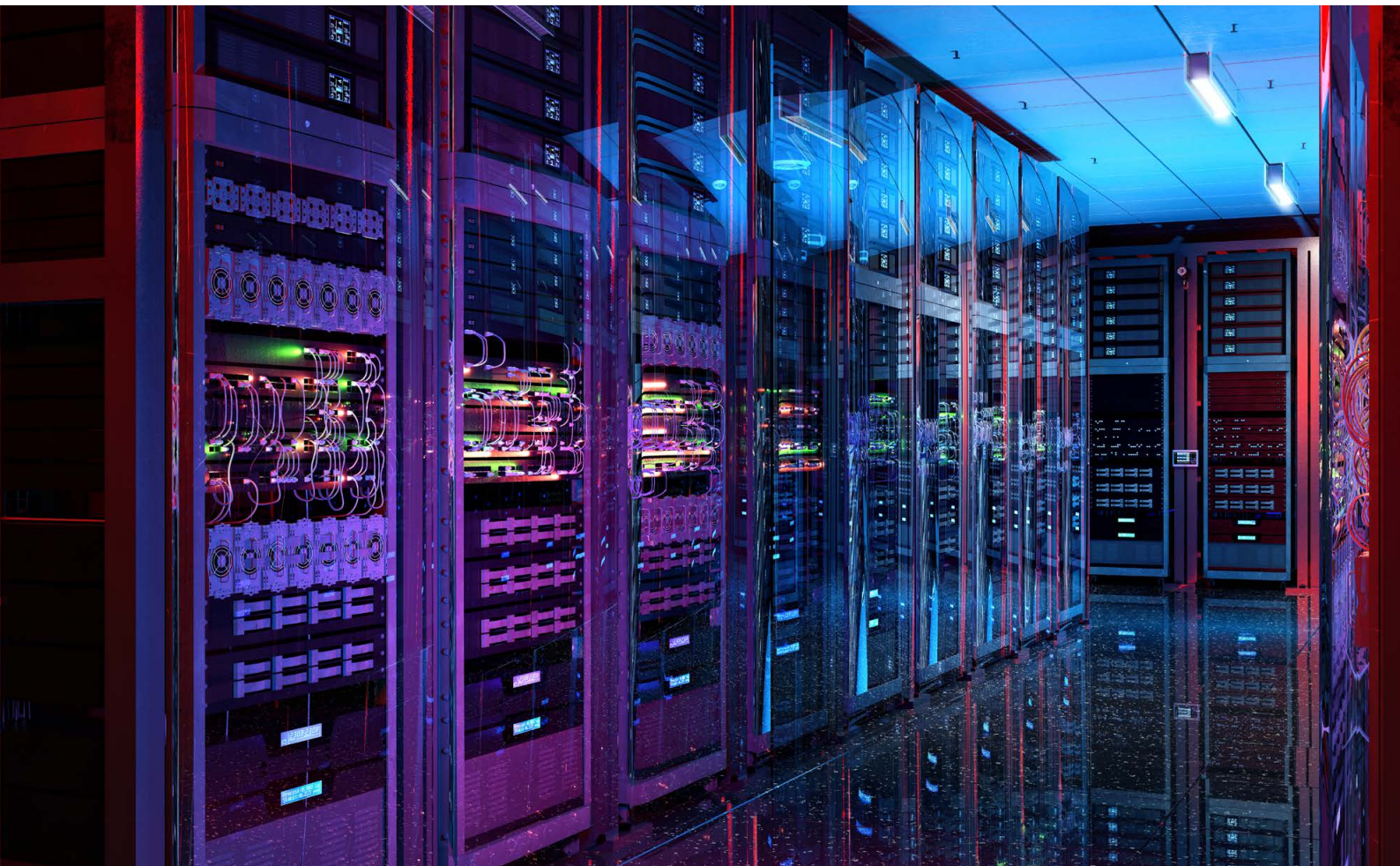
Anastasia Kartasheva: Cyber risks are influenced by a mix of heavy-tailed loss distributions, uncertain models, and uneven information. Unlike traditional insurable risks, cyber events can be worldwide, fast-paced, and deliberately adaptive—making them particularly tough to forecast and model. Their high cost and changing nature add more complexity. These traits pose major challenges for insurers, but also imply that the market holds some potential. New solutions include the creation of information intermediaries that evaluate a company's cyber resilience, similar to how credit ratings work in bond markets.

Olivier Scaillet: The cyber insurance market is taking shape as a distinct sector. One way to understand this evolution is by looking at the balance between investing in internal cybersecurity and transferring risk through insurance. Insurers now not only offer coverage, but also help organizations manage their cyber risks directly or through third parties. As these models develop, I expect growing pressure on reinsurance, due to the rising cost and complexity of cyber exposures. This trajectory may ultimately lead to global risk-sharing mechanisms, such as insurance syndications or secondary markets for cyber risk, similar to what is happening with catastrophe bonds. These risk-sharing mechanisms would allow investors to trade cyber-linked securities and would expand capacity beyond traditional insurance.

Looking forward, what advanced strategies should financial institutions adopt to effectively mitigate attacks?

Marc Henauer: Financial institutions have a deep understanding of the cybersecurity landscape and how the interconnected financial system operates, as well as its potential vulnerabilities. Whether large or small, any bank can have a ripple effect on the broader banking and financial infrastructure. They also know how reputational damage affects everyone. If one bank is severely hit, the entire financial industry feels the impact. There is no individual gain to be had here. This fact motivates them to collaborate proactively and to communicate openly and efficiently.

Olivier Scaillet: Looking ahead, financial institutions need to adopt advanced, layered defense strategies—such as artificial intelligence-powered threat detection, zero-trust frameworks, and continuous employee training—to stay ahead of increasingly sophisticated cyber threats. But beyond protecting themselves, banks are uniquely positioned to seize emerging business opportunities in the cybersecurity space. As cyber risk becomes a measurable and priced asset, financial institutions can take the lead in developing and offering innovative financial products, such as cyber risk tranching modeled after Collateralized Debt Obligations (CDOs). By structuring risk into layers that absorb losses based on severity, banks can facilitate market-based diversification, offer tailored cyber insurance-linked instruments, and help clients hedge cyber exposures. In doing so, they move from being passive targets to being active market makers in the evolving cyber risk economy.



Frontiers

Do decentralized finance (DeFi) initiatives make things more secure or more vulnerable from a cybersecurity standpoint?

Fabian Schär: Decentralized and centralized finance have distinct cybersecurity risk profiles, with neither one being clearly superior. On the one hand, decentralized systems offer certain security advantages—most notably, the inability of any single actor to unilaterally alter the public ledger, thereby eliminating many attack vectors common in centralized architectures. On the other hand, they introduce unique vulnerabilities. For example, DeFi systems rely heavily on private keys, and if a user loses or exposes theirs, they have no recourse: Their assets can be irreversibly stolen, and attackers may even use their compromised identity to create new smart contracts. The fundamental appeal of DeFi lies in its trustless nature, streamlined processes, and faster transactions—features that can be highly advantageous from a business perspective. Yet the absence of intermediaries also shifts the burden of risk onto the individual. Users must not only secure their keys, but also navigate a complex system where protections common in traditional finance, such as transaction reversals or dispute resolution, are largely absent. In this sense, DeFi expands the range of possibilities, but also introduces a new class of cybersecurity and operational risks that must be understood and actively managed.

Olivier Scaillet: Like any technological innovation, there are upsides and downsides. Research has found that ransomware attacks are the most common type of cyberattack, with a small number of advanced ransomware gangs dominating the scene. These gangs have become sophisticated corporations with elaborate names, offices, call centers, and franchising operations. They typically receive ransom payments in cryptocurrencies and must launder the proceeds through complex schemes. Since Bitcoin is traceable, attackers prefer more obscure cryptocurrencies, like Monero or Zcash. There is anecdotal evidence that when victims insist on paying in Bitcoin, gangs charge a 20% premium. It is unlikely that a solution can be found to prevent cryptocurrencies from being used in cybercrime, as banning all cryptocurrency use in a country would eliminate its benefits and put the country at a technological disadvantage.

What are the differences in terms of cybersecurity risks between central bank money, commercial bank money, and crypto assets?

Anastasia Kartasheva: Stealing electronic money or assets is only half the battle. The other half is cashing it in. The 2016 Bangladesh Bank heist is a prime example, where hackers infiltrated the central bank's IT system and accessed its SWIFT network to send fake transfer instructions totaling USD 951 million. About USD 81 million was sent to the Philippines and then laundered through a complex and costly network of shell companies and casinos. Interestingly, the remaining transfers, worth over USD 850 million, were caught because a typo in the message raised suspicions. While it is relatively easy to convert unregulated assets like Bitcoins in countries with weak regulation, doing so is a risky and murky process, and the end user likely ends up with "funny money."

How does artificial intelligence exacerbate cybersecurity threats?

Anastasia Kartasheva: Artificial intelligence is a double-edged sword. Attackers have become much smarter. The days of sending out massive emails with random addresses, typos, and poorly designed logos are long gone. Meanwhile, defenders can leverage artificial intelligence to strengthen their team and automate their defenses. The industry is looking to deploy artificial intelligence tools across the IT system. Raising awareness on today's and tomorrow's threats, and educating users everywhere, is crucial.

Fabian Schär: The rapid development of deepfakes, driven by deep learning systems, is particularly concerning to me. The only defense mechanism I can think of nowadays is cryptographic signatures. Nowadays, we have thousands of hours of videos featuring key politicians available online. It is relatively straightforward for an artificial intelligence model to impersonate that person and have them say whatever one wishes. I believe we will soon find ourselves in a world where speeches are no longer delivered in person but are scripted and presented by an artificial intelligence system, with the message cryptographically signed to ensure authenticity.

How do financial institutions today manage cybersecurity threats using artificial intelligence?

Fabian Schär: It is tough for financial firms to stay ahead in this game for two main reasons. First, the competition is very fast-paced. Second, banks often have long lifespans, which means they are stuck with complex legacy systems that are difficult to secure effectively. Artificial intelligence will increasingly help them detect suspicious activities and enable quicker responses. However, attackers seem to be gaining the upper hand here.

Olivier Scaillet: Several exciting developments are occurring. Artificial intelligence provides numerous benefits, such as efficiency, scalability, and adaptability in cybersecurity. These advantages facilitate the identification of potential fraudulent activities based on customer behavior patterns, anticipate threats by learning from historical data, and enable automated response systems that isolate issues and reduce response times. However, everything we know today will need to be adjusted when quantum computing becomes the new standard.

What is the realistic timeline for threats from quantum computing to appear?

Anastasia Kartasheva: Computational power and speed are crucial in the cyber world. Some experts predict that more sophisticated attacks from quantum computers will become the standard within the next decade. Yet, despite cyberattacks being, by definition, carried out on computers, there is always a human element involved. Computational ability is not the only factor; both attackers and defenders will need to boost their skills as we progress.

What specific steps should financial institutions take to prepare for quantum-resistant cybersecurity in the future?

Fabian Schär: Banks always need to prepare for future challenges. In my opinion, they must enhance their understanding of both the current system and the emerging system. Today's banking IT framework is a consolidated model that was established in the 1950s and has undergone numerous mergers and acquisitions. Unlike many other sectors, the significance of a centralized system is crucial in the banking industry and the legacy issue is substantial. J.P. Morgan Chase, for example, is the result of over 1'200 predecessor institutions.

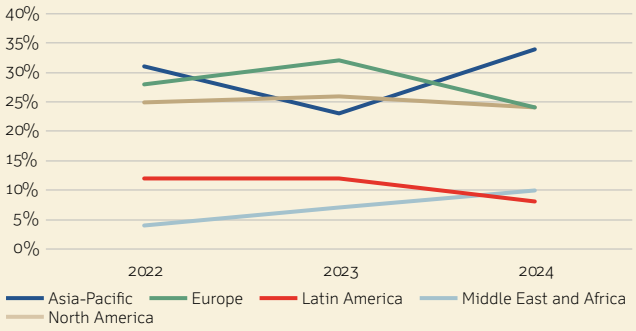
Olivier Scaillet: There are several steps involved in preparing for a quantum future. First, banks need to compile a clear inventory of their current cryptographic blocks to understand their configuration and vulnerabilities. Next comes the development phase, where they collaborate with system vendors and internal system owners to thoroughly test the new quantum technology. Then there is the phase of replacing the old technology with the new one. The current approach to addressing post-quantum cryptography (PQC) risks and the potential weaknesses of the new PQC-resistant algorithms is to combine both the old and new methods by implementing hybrid protocols that apply both technologies simultaneously.

How marked are the differences across countries and industries in terms of their means to ensure cybersecurity?

Fabian Schär: Differences across countries and industries are significant—and are often rooted in history, geography, and institutional design. In the financial sector, for example, newer financial centers often enjoy a structural advantage: Their systems were built in an era of global markets and electronic trading, enabling more modern IT foundations. In contrast, long-established banks frequently rely on legacy systems, sometimes several decades old, which are difficult and costly to overhaul. This creates complex patchworks that are harder to secure and maintain. At a country level, while the Western world generally enjoys stronger cybersecurity capabilities, variations persist. Some countries attract heightened geopolitical attention and are thus more frequent targets of cyberattacks—most notably the United States. Others, like Switzerland, benefit from having a more neutral geopolitical stance, well-resourced institutions, and strong public-private cooperation. These differences shape both exposure and resilience in the face of evolving threats.

Anastasia Kartasheva: Cybersecurity readiness varies not only by country but also by sector, firm, and individual, depending on how clearly responsibilities are defined and how well resources are aligned. In some jurisdictions, the public sector has taken the lead by establishing clear standards, funding coordination centers, and facilitating the sharing of threat intelligence. In others, especially in emerging markets or transitional economies, firms are often left to fend for themselves, with limited guidance or regulatory clarity. This situation leads to uneven protection: While some large firms have world-class defenses, others—particularly smaller firms and state-owned institutions—remain highly vulnerable, due to constrained budgets and fragmented systems. Ultimately, the effectiveness of a cybersecurity framework depends as much on national governance and institutional maturity as it does on technology or spending.

Distribution of Cyberattacks per Geographic Region



Note: This figure shows the distribution of cyberattacks across geographic regions from 2022 to 2024. In 2024, the most targeted countries within each region were the United States (86% of North America), Japan (66% of Asia-Pacific), Saudi Arabia (63% of the Middle East and Africa), Brazil (53% of Latin America), and the United Kingdom (25% of Europe).

Source: IBM X-Force

How would you describe the role that international standards play in cross-border cybersecurity efforts?

Marc Henauer: International standards play a crucial role in enabling cross-border cybersecurity cooperation by offering a common language, shared expectations, and technical benchmarks for risk management. While implementation varies by region and sector, these standards—such as ISO 27001 (from the International Organization for Standardization) and the Cybersecurity Framework from the U.S. National Institute of Standards and Technology (NIST)—help reduce fragmentation and enable collaboration among governments, industries, and supply chains. Much like climate policy, cybersecurity needs global alignment in principle, but turning that into coordinated action remains a complex challenge. True progress depends on reciprocity and trust across borders and sectors, not on imposing one-size-fits-all models. The risk of losing key institutions like MITRE, a nonprofit research organization, which maintains shared infrastructure such as the Common Vulnerabilities and Exposures (CVE) identifiers, reveals the fragility of centralized systems and underscores the need for resilient, distributed, and cooperative approaches to global cybersecurity governance.

Beat Schär: International standards are immensely valuable as benchmarks, helping organizations assess where they stand and how to improve. The existence of diverse initiatives across sectors and countries offers a rich source of insight into the challenges others face and the solutions they apply. In the field of cybersecurity, no single actor has all the answers—continuous learning from one another is not just helpful, it is essential.

Final Byte

What role should corporate and executive boards and regulation play in shaping cybersecurity governance?

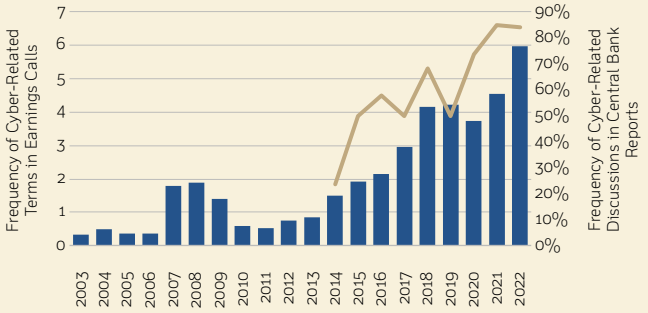
Alain Beuchat: Recent Swiss regulations require board-level approval of cybersecurity strategies. However, board engagement in cybersecurity is more than a compliance requirement—it is increasingly a matter of strategic survival. In other words, formal involvement does not always translate into effective oversight. Many directors struggle to grasp just how deeply their organizations rely on IT infrastructure—let alone understand the complexities of cyberdefense. While they are generally aware of the impact cyberattacks can have, often through media coverage, it remains difficult for them to connect these threats to the specific vulnerabilities and realities of their own organization. Bridging this gap requires more than briefings. Board members need to have enough baseline knowledge to be able to ask meaningful questions, challenge trade-offs, and understand what their firm's risk profile really implies. Until boardrooms develop deeper cyber fluency, governance will lag behind the pace of the threat.

Olivier Scaillet: In the Swiss context, regulatory bodies like FINMA play a crucial role in shaping cybersecurity governance, especially in the financial sector. While some institutions are ahead of the curve, due to stronger resources or a deeper understanding of cyber risks, regulation remains relatively light in areas such as cloud solutions and supply chains. A key next step would be to clarify the roles and responsibilities of all management levels in the case of a cybersecurity failure, helping to promote greater accountability from the leadership. At the same time, corporate and executive boards must not see cybersecurity as just a technical issue delegated to their IT teams. Boards should be regularly informed about both incidents and major developments, and conduct routine exercises to ensure that they are prepared to make sound decisions under pressure. Cybersecurity affects nearly every aspect of business and society, so directors have a duty to engage early and proactively—rather than waiting until a crisis forces them into action.

Anastasia Kartasheva: Having a well-developed contingency plan is essential. The plan should address key questions, such as how quickly systems can be restored, whether the attacker still has access, what losses might be covered by cybersecurity insurance, and whether regulatory sanctions or fines could follow. There is no one-size-fits-all solution, but proactive education of corporate leadership on cybersecurity risks is critical.

Fabian Schär: Like many things, taking sensible steps can be helpful, but going too far can have the opposite effect. If mandatory cookie banners on websites have taught us anything, it is that regulatory compliance often checks the box—without truly protecting the vault. Ultimately, neither firms nor individuals can outsource responsibility—regulation sets the floor, not the ceiling, for effective cybersecurity.

Cybersecurity Mentions by Firms and Central Banks



Note: This figure presents two measures of institutional attention to cybersecurity between 2003 and 2022. The bars show the frequency of cybersecurity-related terms (e.g., cybersecurity, cyberattack, cyber threat, data loss, malware, ransomware) in corporate earnings calls, standardized per 10'000 sentences (left axis). The line indicates the share of financial stability and annual reports issued by G20 central banks that include substantive discussion of cybersecurity (right axis).

Sources: Advisen, NL Analytics, and International Monetary Fund (IMF)

How do you see regulation shaping the financial sector's ability to manage cyber risk?

Marc Henauer: Switzerland's NCSC is crucial in boosting the country's cyber resilience. Its work centers on four main goals: improving threat understanding, enabling prevention, minimizing incident impact, and securing digital products and services. A recent milestone was the introduction of a 24-hour reporting requirement for cyberattacks on critical infrastructure, designed to generate more accurate data and inform smarter regulation. This new reporting requirement will lead to clearer threat intelligence, more targeted support, and a stronger foundation for managing cyber risk in a coordinated national framework. It will be interesting to see how this requirement unfolds over time.

Fabian Schär: While it is difficult to draw definite conclusions, past experience suggests that cybersecurity regulations in the financial sector have generally been effective. However, even the most robust regulatory frameworks and technical safeguards cannot eliminate the risk of human error; ongoing education and awareness are therefore essential. Looking ahead, mandatory reporting requirements and increased data transparency will likely continue to shape regulatory standards, enhancing our collective understanding of cyber threats. That said, meeting rapid reporting deadlines—such as within 24 hours—remains challenging, as firms often need more time to fully assess the scope of an incident, especially when coordinating with external parties.

Olivier Scaillet: Everyone in the financial sector knows we need to focus on when the next attack will happen and how to minimize its impact, not on whether it will happen. While it might seem frustrating, facing this tough reality allows companies and the industry to prepare. Within companies, there should be honest talks about how quickly they can recover from an attack; between companies, there should be a conversation about limiting common risks by using a wider range of hardware and software. While regulations can enforce many of these measures, they have limited power to make the industry adopt different systems. I am concerned about the steady decline in the number of providers and the lack of a viable way to reverse this trend.

What kinds of emerging cybersecurity threats will most significantly impact society in the next decade?

Fabian Schär: Over the next few years, advances in artificial intelligence, big data, and quantum computing will elevate our cybersecurity to the next level. I firmly believe that we should tap into the full potential of bounty programs to transform "bad guys" into "good guys." Ransomware attacks are often driven by financial gain, so it is logical for companies to reward individuals who help improve their security, rather than paying ransoms to stay afloat. The cat-and-mouse game has been around since ancient times, and there is no reason to think the future will be any different—just the tools will evolve.

Anastasia Kartasheva: The finance sector will face an increasingly complex set of cybersecurity threats over the next decade, driven by growing digital interdependence and global exposure. A core challenge will be verifying the identity of third parties—whether firms or individuals—particularly across borders where digital standards and regulations differ. At the same time, the attack surface will expand, due to the proliferation of connected devices, the consolidation of IT systems, and widespread cloud adoption. These trends, combined with advances in artificial intelligence, machine learning, and quantum computing, will empower more sophisticated adversaries. Together, they will force a fundamental rethinking of trust, verification, and resilience in cybersecurity.

Swiss Finance Institute

With support from its founders—the Swiss banking industry, the Swiss Confederation, and leading Swiss universities—the Swiss Finance Institute (SFI) competitively promotes world-class research and teaching in banking and finance in Switzerland. By combining academic excellence with practical experience SFI contributes to the strengthening of the Swiss financial center.

Editor and contact
Dr. Cyril Pasche
Senior Director Publications and Topic Development
+41 22 379 88 25
cyril.pasche@sfi.ch

swiss:finance:institute

Walchestr. 9, CH-8006 Zurich, T +41 44 254 30 80
c/o University of Geneva, 42, Bd du Pont d'Arve, CH-1211 Geneva 4, T +41 22 379 84 71
www.sfi.ch

Version 10/2025