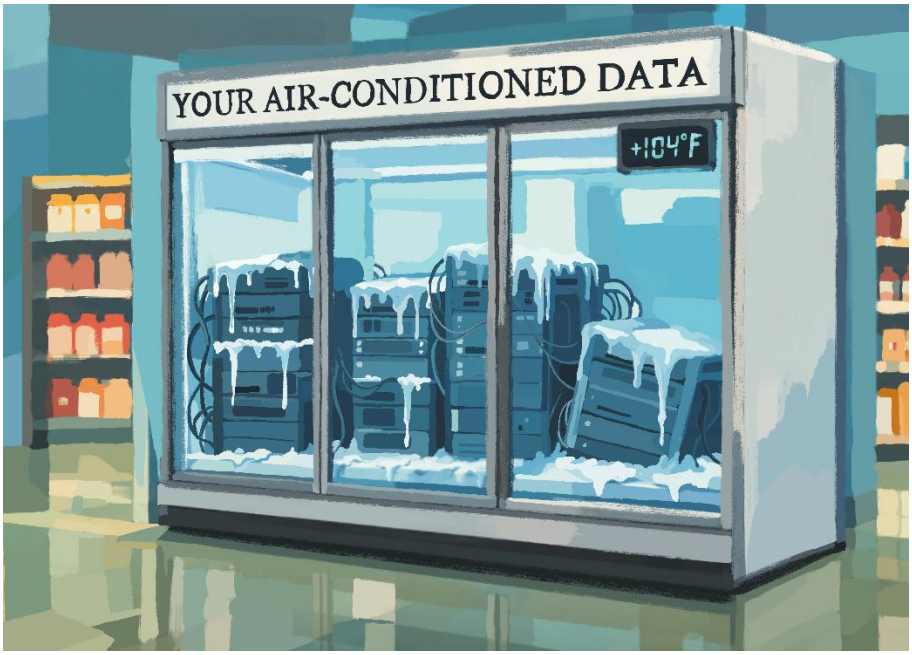
All hands on deck to tackle cyber risk

Agnès Bénassy-Quéré, November 2026



The large-scale cyberattack on supermarket and hospital fridges in October served to highlight the very real cyber risk facing our societies. This risk affects all connected systems, and the financial sector is a prime potential target, as recent examples have shown.

Under Europe's Digital Operational Resilience Act (DORA), European banks are required to continuously assess and protect their IT systems, carry out regular security and penetration tests, assess the resilience of their external service providers, and promptly report any major incidents they may experience.

For 2025, the European supervisory authorities recorded 3,383 major incidents affecting the IT systems of European financial institutions, 10% of which were cybersecurity-related. This means that, on average, there was nearly one cyberattack every day in Europe. In France, the *Autorité de contrôle prudentiel et de résolution* (ACPR – Prudential Supervision and Resolution Authority) and the Banque de France received reports of around 40 major cyber incidents believed to have been perpetrated by cybercriminals (Banque de France, 2026).

In addition to direct damage (inaccessibility of services, data theft, embezzlement and other fraudulent activities), this type of attack has an indirect economic cost. For example, financial transactions become impossible when a payment system crashes. Disruptions to wholesale payments trigger a liquidity shock that spreads across financial institutions, posing a risk of a liquidity crisis (Eisenbach et al, 2021). For non-financial corporations, disruption to retail payments can lead to immediate loss of income and put cash flow under strain, particularly if banks are no longer able to provide liquidity facilities. Furthermore, reputational damage can be significant for the financial sector, by casting doubt on the security of data and assets held with financial intermediaries.

In 2024, the International Monetary Fund (IMF) identified three main risks to financial stability:

- A loss of confidence, which could ultimately lead to bank runs;
- The disruption of critical services or a key institution, for which there is a lack of short-term substitutes;
- The spread of a cyber incident affecting an institution via its interconnectedness through technological linkages (using the same software) or financial linkages with other players in the sector.

These disruptions may affect the financial sector through market dysfunction, increased asset price volatility, impaired access to financing, and payment system incidents. Such turmoil may in turn trigger a liquidity crisis or a credit crunch, which would weigh on the real economy, which is already hampered by the disruption of payments or access to critical infrastructure.

There are several factors that increase financial institutions' exposure to cyber risk, including:

- The concentration of third-party service providers, particularly in the areas of software, cloud platforms and artificial intelligence tools. This risk is compounded by widespread institutional reliance on a small number of essential service providers (Pendleton et al., 2024). In 2025, the 14-hour outage of Amazon Web Services demonstrated how the failure of a single technology provider can have significant economic and operational consequences, extending far beyond the financial sector alone. This reliance on a small number of suppliers makes cyber risk difficult to diversify compared with other operational risks (Biener et al., 2015).
- The worsening geopolitical environment exposes these companies to increased threats of hostile action and requires them to step up their preparedness. Furthermore, given their strategic importance, certain major service providers may be subject to pressure, sanctions or export restrictions, which could lead to difficulties in accessing certain critical services This growing fragmentation exacerbates operational and financial stability risks.

While risks have clearly increased, such attacks are nothing new, and financial institutions have long been investing in protecting their information systems, which, paradoxically, makes them less vulnerable than other sectors (Aldasoro et al., 2020). Moreover, several international initiatives are in place to reduce the vulnerability of the financial sector.

G7 Coordination

The financial sector is particularly interconnected, both within Europe and with the rest of the world. That is why, since 2019, the G7 has conducted three cross-border coordination exercises in response to a hypothetical attack affecting one of the G7 countries and spreading to the others. The most recent one took place between March and May 2026 under the French presidency of the G7. The aim was to test the G7 authorities' ability to share critical information rapidly, act in a coordinated manner and communicate jointly to minimise damage and restore normal operations as quickly as possible. Coordinated communication reduces the risk of panic, particularly on social media

Co-chaired by the United Kingdom and the United States, the G7 Cyber Expert Group of the Finance Track promotes the harmonisation of cyber-resilience strategies to protect the integrity and stability of the financial sector. To this end, the group disseminates best practices within the sector, with a view to improving response mechanisms to potential attacks, protecting systems

during an attack, ensuring service continuity during a disruption, and subsequently reconnecting the systems and restoring normal operations. It is the responsibility of the different national authorities to adapt these best practices and to ensure that they are implemented by financial institutions and their service providers.

Experts stress the importance of maintaining impeccable “IT hygiene” which, among many other measures, involves updating systems as and when the exposure of equipment to the internet and the active exploitation of vulnerabilities increase. This approach must be accompanied by sufficiently forward-looking management of system obsolescence, a strict access rights management policy, the use of strong authentication mechanisms for access to critical systems, rigorous network segmentation, measures to strengthen the configurations of the various systems and equipment, and data encryption. Naturally, these measures must be rounded out by regular user awareness-raising campaigns and the implementation of immutable, offline backups.

These measures, designed to protect systems, must be supplemented by processes that enable attacks to be detected effectively and responded to as quickly as possible. It is also important to be able to restore systems and operations quickly once an incident has been resolved, particularly where an organisation has been compromised. These procedures are regularly tested as part of business continuity and recovery plans.

Lastly, in addition to securing companies’ own information systems, it is important to ensure the cyber-resilience of key service providers – software, telecommunications, cloud services, etc.

AI and post-quantum computing

The emergence of "cutting-edge" artificial intelligence is exacerbating risks by increasing both the speed and the scale of attacks. Automating the search for vulnerabilities and ways to bypass security measures makes systems more vulnerable. This observation led the European Systemic Risk Board to issue a warning specifically addressing such risks, which it classified as systemic (ESRB, 2026).

At the same time, the growth in crypto-asset trading, particularly via unhosted wallets (i.e. those managed by individuals themselves, rather than on trading platforms), is facilitating the emergence of a fully-fledged cybercrime services industry.

In the coming years, the advent of quantum computers will exponentially increase the available computing power, enabling potential attackers to break the cryptographic keys that protect systems. That is why the financial sector must prepare by transitioning to post-quantum cryptography, in particular by upgrading the encryption and digital signature solutions that protect its data, communications and transactions. In January 2026, the G7 Cyber Expert Group published a roadmap aimed at steering the financial sector’s transition towards post-quantum cryptography solutions. Meanwhile, a second group, bringing together national security agencies, produced a document setting out the practical steps to be taken to begin the post-quantum migration.

The interconnectedness of IT systems makes it essential to coordinate efforts in the area of cybersecurity: cyberattackers exploit the least secure points in the network, such as outdated software or institutions and service providers with weaker defences. The Cyber Expert Group therefore recommends adopting a common timetable for the roll-out of post-quantum cryptography by 2035 at the latest – a deadline currently regarded as the target by specialists in the field – whilst prioritising the most vulnerable systems so that these can be protected by 2030 (see Chart)

Chart. Common timetable for the roll-out of post-quantum cryptography



Source: G7-CEG-Quantum-Roadmap.pdf

***

While multilateral coordination faces significant challenges, it is interesting to note that, on specific and technical issues where there is a clear common interest, convergence remains possible and does yield results. When it comes to cyber risk, all hands are on deck. The emergence of new technologies that facilitate the circumvention of the safeguards of information systems, the proliferation of cyberattacks and, lastly, the financial rewards for the perpetrators, will require stronger crews and their international coordination, despite rough seas that may discourage them.