SPEECH

The Quick and the Dead: building up cyber resilience in the financial sector

Introductory remarks by Fabio Panetta, Member of the Executive Board of the ECB, at the meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures

Frankfurt am Main, 8 March 2023

The proliferation of cyber threat actors combined with an increase in remote working and greater digital interconnectedness is raising the risk, frequency and severity of cyberattacks.[1] Increasingly, cyber criminals are launching ransomware attacks and demanding payment in crypto. Cyberattacks related to geopolitical developments – Russia's aggression against Ukraine in particular – have also become a more common feature of the cyber-threat landscape.

The Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) has played a key role in protecting the security and integrity of the financial system from these threats. The last three years have shown that we can work under adverse conditions towards a common goal. Our financial infrastructures have proven their resilience to cyber threats. But this does not mean we can become complacent or any less vigilant in the face of cyber threats. We simply cannot afford to fall behind the curve: cybersecurity must be the backbone of digital finance.

Today I will take stock of the ECRB's work. I will then discuss current cyber threats and emerging risks before outlining the implications for our work in the future.

The contribution of the Euro Cyber Resilience Board

The ECRB brings together private and public stakeholders across pan-European financial infrastructures, critical service providers, central banks and other authorities. This offers a unique prism through which the ECRB can identify and fix any weaknesses which cyberattacks could potentially exploit in order to propagate, which in turn would cause systemic ripples throughout the European financial ecosystem.

Let me give three examples of why the ECRB is such a useful forum for cooperation.

First, in the area of information sharing, the ECRB's Cyber Information and Intelligence Sharing Initiative (CIISI-EU)[2] allows members to exchange information about cyber threats and mitigation in a secure and trusted group environment.

Second, the ECRB has established a crisis coordination protocol that facilitates cooperation and coordination, allowing members to exchange and respond to major cyber threats and incidents.

Third, in the area of training and awareness, the ECRB conducts joint assessments and training sessions to increase common knowledge and understanding. A key pillar of the ECB's cyber strategy for financial infrastructures is the TIBER-EU framework for threat-led penetration testing, also known as red teaming. In June 2022 the ECRB organised a dedicated roundtable on TIBER-EU where members shared their experience of these kinds of exercises.[3]

In view of their systemic role in the financial system, we will continue to focus on pan-European financial infrastructures. Nonetheless, financial infrastructures are increasingly interdependent through horizontal

and vertical links and common participants. They are also reliant on information and communication technology and on third-party service providers. As a result, these infrastructures are exposed to common risks and vulnerabilities through which cyberattacks could propagate swiftly if they are not rigorously managed. The ECRB allows us to join forces to address these risks on a sector-wide level.

Adapting to a constantly changing cyber threat landscape

Let me now turn to the cyber threat landscape.

Threats are becoming increasingly complex. Recent attacks call for constant vigilance at an operational level, and the continuous reassessment of regulatory and oversight frameworks to see whether they need to be updated.[4] Significant but unpredictable shifts can occur at any time. We must therefore be prepared to understand them and to adapt quickly in order to mitigate the financial ecosystem's susceptibility to cyberattacks.

The ECRB has identified supply chain attacks and ransomware as key threats in the current environment, and artificial intelligence (AI) as an emerging threat. We have also witnessed how geopolitical developments, most recently Russia's aggression against Ukraine, have weaponised cyberspace. The most prominent examples are distributed denial-of-service (DDoS) attacks against government and financial entities.[5]

Let me discuss the key current and emerging threats in more detail.

Supply chain attacks

The financial ecosystem's reliance on third-party products and services is a key risk, especially when financial entities outsource critical functions to them. An attack on these third parties or on their products and services can disrupt and harm the financial infrastructures that rely on them, with spillovers to interconnected entities.

When such third-party products and services are widely used in the financial ecosystem, a cyberattack can have widespread, possibly systemic effects by having an impact on multiple financial entities at once. That is why cyber threat actors target these third parties. In so doing, they can compromise numerous financial entities simultaneously.

The recent cyberattack on the third-party provider ION Cleared Derivatives shows how an attack on one software provider may cascade onto their clients. In this specific case, the disruptions to the trading and clearing of financial derivatives remained limited, but we cannot ignore scenarios where the attacks could have propagated quickly, disrupting the financial system.

This case signalled the need for financial entities to review their third-party providers, the providers of these third-parties, their cyber resilience levels and the systemic impact that may ensue from a cyberattack on any of these providers. In particular, it is vital to assess critical service dependencies on third-party products and services which could be disrupted or even terminated as a result of a cyberattack. Mitigating measures need to be put in place.

Against this background, the G7 recently updated its Fundamental Elements for Third-Party Cyber Risk Management in the Financial Sector[6]. In addition, the ECRB set up a working group in 2022 to support third-party cyber risk management.

We must have a cyber resilience mindset at all times. The question we must ask is not if a cyberattack will happen, but whether we are ready to respond when it happens. Over the past year, the ECRB has worked on a conceptual model for how the financial infrastructure ecosystem could manage such a crisis if it occurred. It has also developed protocols and networks aimed at supporting a collective, consistent and comprehensive response to a cyber crisis by stakeholders.

Ransomware

The proliferation of ransomware is one of the most significant challenges currently facing financial entities. Not only may ransomware attacks result in financial loss, they may also severely disrupt operations. Even after a ransom is paid, there is no guarantee the decryption key will actually work or that the stolen data will not be publicly disclosed or further misused to extort victims' customers, for example.

Ransomware attacks are growing more sophisticated and damaging, which in turn may enable ransomware threat actors to obtain even more resources. 2022 was one of the most active years for ransomware activity.[7] However, it was also the first year that the majority of victims of ransomware attacks decided not to pay up[8], which indicates that the approach towards ransomware attacks is changing.

Authorities globally are stepping up their efforts to counter ransomware. For instance, the G7 issued Fundamental Principles on Ransomware Resilience in October 2022[9].

We need to tackle ransomware attacks from various angles.

First, every firm must be ready to repel ransomware attacks, either through the use of proper cyber hygiene practices or by ensuring that data is backed up regularly and is kept up-to-date and tamper-proof.

Second, enforcement agencies need to conduct forensic analyses, locate attackers and join forces to prosecute them.

Third, crypto-assets – especially unbacked crypto-assets, which are used to make ransomware payments owing to the anonymity and money laundering possibilities they offer[10] – need to be strictly regulated.[11] Similarly, crypto-asset transfers must be traceable.

The proposed EU Regulation for Markets in Crypto-Assets (MiCA) and revision to the Regulation on information accompanying transfers of funds, which extends the "travel rule"[12]to crypto-assets, are important steps. However, to be effective and prevent regulatory arbitrage, regulation must be stepped up globally.[13]Implementation of the Financial Action Task Force (FATF) guidance for crypto-assets and its enforcement at international level are therefore crucial.[14]

In addition, all firms need to have the highest level of cyber controls in place to prevent attacks from being successful and to detect and recover from ransomware attacks. Moreover, insurance firms can lend their support by obtaining assurances from their clients that they have high-level cyber resilience plans in place before providing cyber risk insurance policies, thus ensuring that these very same policies do not lower firms' incentives to prepare for cyberattacks.

Artificial Intelligence (AI)

Even if we do not realise it, the use of artificial intelligence (AI) is already widespread. We use AI every day, including on our phones, in our homes and at the workplace. And firms use it to harness big data.

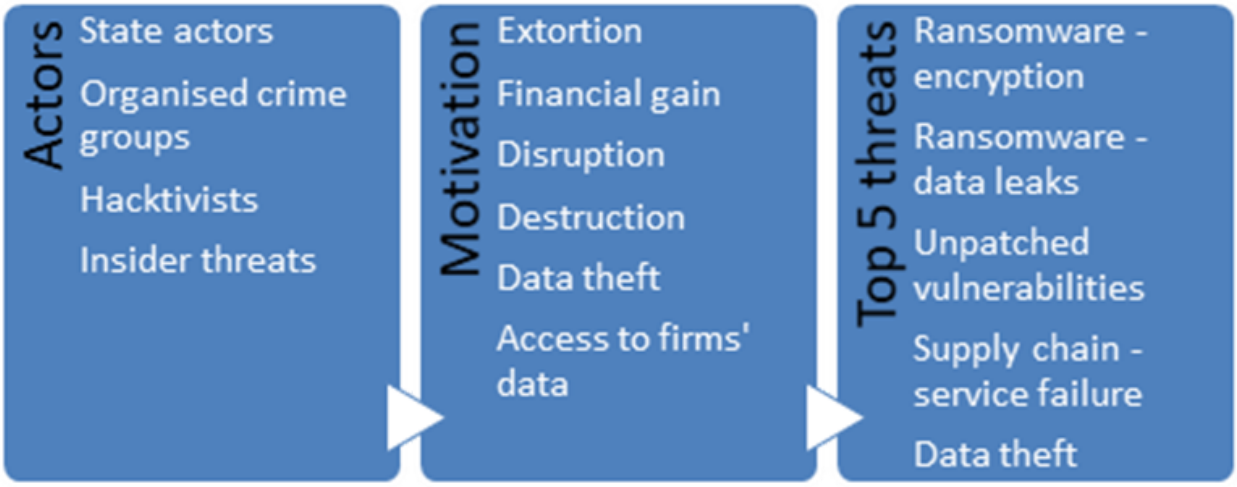
AI can help to strengthen cybersecurity, for instance, by improving the detection of highly sophisticated cyberattacks through its ability to identify abnormal system behaviour compared with an established baseline. This is the kind of potential that we need to leverage.

But AI can also multiply cyber risks by, for instance, helping malicious individuals, even those who have limited or no technical skills, draft very convincing phishing emails or identify topics that will achieve the maximum engagement from those being targeted. To make matters worse, AI can even create and fix code that can be used to exploit and compromise the endpoint.[15] This opens up new possibilities for malicious individuals to use AI to launch cyberattacks. Although AI development firms try to install safeguards to prevent its unethical use, they can be circumvented.

The risks from AI need to be clearly understood and addressed through regulation and oversight. By exchanging information among its members and organising roundtables and training, the ECRB is in a strong position to raise awareness of risks at an early stage and accumulate knowledge of these types of threats. For its part, the European Commission has proposed a Regulation on artificial intelligence that aims to address some of the key risks associated with AI.[16]

Chart 1

Cyber threat landscape for financial market infrastructures in Europe



Note: Threats are arranged in descending order of estimated severity.

Conclusion

As we realised some years ago, cyber threats are here to stay. Many highly-adaptable threat actors exist who will systematically try to exploit any weakness or vulnerability for illegal purposes. Existing threats are becoming more dangerous and new threats are on the horizon. We therefore need to adapt our operational and cyber resilience frameworks constantly at the individual level as well as collectively through strict regulation, enforcement and prosecution. Future cooperation between public and private institutions will also be crucial. The ECRB can make a decisive contribution to this effort in relation to the financial system.

1.

See Forbes (2022), "The Pandemic's Lasting Effects: Are Cyber Attacks One of Them?", 20 July.

2.

See European Central Bank (2020), "Cyber Information and Intelligence Sharing Initiative (CIISI-EU). Cyber information and intelligence sharing: a practical example".

3.

See European Central Bank (2022), "Key takeaways from the ECRB roundtable on red teaming (TIBER-EU)".

4.

See Financial Times (2023), "The financial system is alarmingly vulnerable to cyber attack", 6 February.

5.

See Reuters (2023), "Russian 'hacktivists' briefly knock German websites offline", 25 January.

6.

See "G7 Fundamental Elements for Third-Party Cyber Risk Management in the Financial Sector", October 2022.

7.

See Techcrunch (2022), "Ransomware is a global problem that needs a global solution", November.

8.

See Security Week (2023), "Ransomware revenue plunged in 2022 as more victims refuse to pay up", January.

9.

See "G7 Fundamental Elements of Ransomware Resilience for the Financial Sector", October 2022.

10.

According to recent reports, ransomware attackers extorted at least €430 million in 2022, while the number of ransomware strains saw a sharp increase. The actual amount extorted may be even higher, as may the number of attacks. See "The 2023 Crypto Crime Report", *Chainalysis*, February 2023.

11.

See Panetta, F. (2022), "Crypto dominos: the bursting crypto bubbles and the destiny of digital finance", keynote speech at the Insight Summit held at the London Business School, 7 December.

12.

The "travel rule" requires that information on the source of the asset and its beneficiary travels with the transaction and is stored on both sides of the transfer. See European Parliament (2022), "Crypto-assets: deal on new rules to stop illicit flows in the EU", 29 June.

13.

See Panetta, F. (2023), "Caveat emptor does not apply to crypto", *Financial Times*, 4 January.

14.

See Financial Action Task Force (2021), "Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers", October.

15.

See Forbes (2023), "Does ChatGPT pose a cybersecurity threat? Here's the AI bot's answer", February.

16.

See European Commission, "Regulatory framework proposal on artificial intelligence". The proposed rules will address risks specifically created by AI applications, propose a list of high-risk applications, set clear requirements for AI systems for high-risk applications, define specific obligations for AI users and providers of high-risk applications, propose a conformity assessment before the AI system is put into service or placed on the market, propose enforcement after such an AI system is placed in the market, and propose a governance structure at European and national level.