Digitalisation poses new security challenges for payment systems

23 May 2018 – Bank of Finland Bulletin 2/2018 – Financial stability

Tatu Laine
Senior Economist

Reliable payment and settlement systems are basic requirements for maintaining financial stability and fostering economic activity. The smooth functioning of society would quickly become disrupted if businesses and households were to lose trust in payment services or the accuracy of bank account balances, for example.

Sound payment systems and securities clearing and settlement systems (i.e. financial market infrastructures) lie at the foundation of any stable financial system. Cyber risks are increasingly cited as a major source among the overall risks to the financial system. Consequently, developing effective strategies to address emerging cyber threats is a key component of managing financial stability.[1] 'Cyber risk' generally refers to any risk of disruption or damage caused by the misappropriation or exploitation of an organisation's IT systems.[2] In practice, this could mean, for example, bank account information becoming compromised, impairing the use of any and all services that rely on such data. As financial markets become increasingly confined to the digital operating environment,

1. Bank of Finland Bulletin 2/2015: Could a cyberattack lead to financial crisis? (https://www.bofbulletin.fi/en/2015/2/could-a-cyber-attack-lead-to-financial-crisis//).
2. Aleksi Grym's blog post (Finnish only): Kyberriskit huomioitava, jotta rahoitusvakaus säilyy (https://www.eurojatalous.fi/fi/blogit/2017/kyberriskit-huomioitava-jotta-rahoitusvakaus-sailyy/).

the volume of data held by service providers will increase and along with it so will challenges relating to the maintenance, storage, and, in the event of disruptions, restoration of these data. Improving resilience against cyber threats would do much to alleviate these risks.

The Bank for International Settlements' (BIS) Committee on Payments and Market Infrastructures[3] and the International Organization of Securities Commissions[4] have published a strategy for improving the resilience of financial market infrastructures against cyber attacks.[5] This framework covers a broad array of topics related to risk management, including governance, identification, protection, detection, and response and recovery. Key principles include governance clearly committing sufficient resources towards cyber security and collaborative efforts to identify and manage shared risks between market infrastructures. Cyber risks need to be exhaustively addressed on all levels of infrastructure, beginning from end-user-specific risks and working all the way up to system-wide vulnerabilities across multiple infrastructures.

Cyber security should be approached with the different roles of market participants in mind. Individual service providers must ensure that they are able to withstand commonplace security threats such as denial-of-service attacks, computer viruses and other forms of malicious software, and ensure that critical data, such as account balances, are backed up daily. In the event of security breaches, data corruption or system failure, backup data ought to be restored as quickly as possible or secondary systems brought online to minimise service disruption. Measures should also be taken against the risk of backup data corruption, as system restoration may otherwise prove to be extremely challenging.

Together, individual market entities comprise a network of products and services that ultimately constitute the financial system. However, even individual entities may operate in several countries and are often involved in the functioning of multiple payment and settlement systems. As such, the disruption of a single market entity may carry risks across multiple countries and financial infrastructures. For the sake of the financial system as a whole, then, it is critical that all market entities reach a sufficient level of resilience against cyber threats and observe best practices, regardless of size or sovereign. This strategy would provide a form of herd immunity against system-wide disruptions caused by cyber attacks. Similarly, market entities should work together to identify and address vulnerabilities where needed.

In Europe, a number of initiatives have been undertaken to shore up the region's protection against cyber threats. In the Netherlands, the national central bank (DNB) has developed a framework for simulating sophisticated cyber attacks and testing resilience against these attacks (Threat Intelligence Based Ethical Red Teaming – TIBER).[6] The ECB recently announced the new Euro Cyber Resilience Board (ECRB)[7], a non-binding

3. CPMI, Committee on Payments and Market Infrastructures (https://www.bis.org/cpmi/).
4. IOSCO, International Organization of Securities Commissions (https://www.iosco.org/).
5. Report 'Guidance on cyber resilience for financial market infrastructure.' (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf).
6. DNB financial stability report 2017 (https://www.dnb.nl/en/binaries/OFS_Autumn%202017_tcm47-363954.pdf).

forum chaired by the ECB whose purpose is to promote the cyber resilience of financial market infrastructures as well as that of the wider EU financial sector. Furthermore, a cyber resilience survey was conducted across more than 75 payment systems, central securities depositories and central counterparties throughout Europe. Based on the survey, areas that require the most development include governance, training and awareness, and incident response. Finally, the Eurosystem is currently finalising the main elements of the European Threat Intelligence-Based Ethical Red Teaming (TIBER-EU) Framework, which will raise the level of cross-border cyber resilience in Europe.[8]

Security of payment services critical for end-users

Cyber security can also be approached from the specific needs and requirements of the end-user. Applications that provide their users with financial services are likely to become all the more ubiquitous on personal computing devices such as laptops and mobile phones in the coming years. The Revised Payment Services Directive (PSD2)[1] provides Third Party Providers (i.e. payment initiation service providers and account information service providers) with the ability to initiate payments and analyse account transactions on the explicit consent of the customer. This allows for the construction of new interfaces between traditional banks and other service providers. As such, the chain of trust linking banks with their customers will become increasingly shared by other market entities. The digital operating environment may provide end-users with lower costs and improved accessibility, but it is vital to make sure that customers may place their trust in new service providers and their respective cyber security protocols. Users must be educated on the terms and conditions associated with digital financial services. More specifically, users must understand the implications of accepting any given set of terms and conditions and also have a clear picture of who has access to their data.

Authorities responsible for maintaining a secure operating environment

Hybrid threats are another type of risk closely linked to cyber security. These refer to the methods and tools used by individual state or non-state actors to disrupt or weaken competitors, adversaries or, indeed, any perceived threat. In the financial sector, hybrid threats may include spreading false market information or other disinformation through trusted news media or harnessing cyber criminals to leak sensitive market data.

It is the duty of authorities to implement regulation and promote initiatives such that cyber security is addressed on all levels of financial infrastructure, encompassing individual market entities all the way up to the system level. Participants on financial markets must ensure that they all commit to protecting the infrastructures that underlie the financial system. One should never be lulled into a false sense of cyber security, as the threat of cyber crime is real and increasing.

---

7. Member of the ECB's Governing Council, Benoît Cœuré, speech, 9.3.2018 (http://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180309_1.en.html).
8. ECB press release, 2 May 2018 (http://www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr180502.en.html).

Tags

cyber security, digitalisation, financial stability