Cyber security in financial market infrastructures

Thomas Provoost

Cyber crime has seen an exponential rise over the last decade and a significant part targeted the financial sector in particular. During the course of 2016 alone, the vulnerability of information assets and the importance of safeguarding the confidentiality, integrity and availability of these assets have been made clear to all parties in the financial ecosystem (see box 1 on the most prominent cyber events revealed in 2016). These threats to information flows and the infrastructure that stores and processes them are central in the confrontation between cyber attackers and the institutions that find themselves defending their systems. This article takes a look at the attributes and channels the offensive side is targeting, and, at the defensive side, how strategies such as testing and information-sharing can be leveraged in creating a sustainable long-term approach by and for financial institutions and the ecosystem in which they work. While all participants in the financial community are facing roughly similar challenges stemming from cyber threats, some particularities for financial market infrastructures (FMIs) will be covered, since these are often at the heart of today's hyperconnected ecosystem.

Cyber criminals[1] seek out targets that yield them the highest expected pay-off : those that show low resistance to intrusion and extraction of value (high chance of success), or where high values can be extracted (big pay-out). In contrast to 'traditional', physical-world crime, the risk of being caught plays a much smaller role in this, not least since cyber space offers many opportunities to act across jurisdictional borders. Furthermore, the anonymity and jurisdiction-transcending nature of cyberspace has given rise to digital marketplaces where an economy of illicit information, tools and services is flourishing (often referred to as the "dark web"). The challenging nature of regulating and enforcing these types of criminal activity confounds the construction of adequate defence measures, since dissuasion by threat of incrimination is an implicit component of any institution's physical defences. But properly-functioning national law enforcement can not easily be transposed into the virtual world, and broad, actionable international cooperation as a necessity for a suitable crime deterrent is only to be encouraged.

The fact that more valuable channels are being targeted could be observed from a growing focus on the high-value transaction chain (bank back offices and interbank payments) as opposed to targeting retail customers (bank accounts). The Bank of Bangladesh case in February 2016 is the most notable instance. But next to being a force in choosing targets, the NBB (the Bank) has noticed that this optimisation of expected pay-off by criminals is also influencing what attribute of information[2] is sought to be compromised. There has been more pressure on the integrity element of data, as cyber criminals are finding ways to fraudulently create or alter rogue payments. This is happening in both the retail and the large-value domain, as evidenced by the recent Tesco Bank (UK) and Bank of Bangladesh heists respectively.

(1) For the purposes of this article, the generic term 'criminals' is used to designate the parties that are on the offensive side. This includes criminal activities such as theft of information or funds, but also refers to more advanced persistent threats such as cyber terrorism and nation-state attacks. These do not seek financial gain *per* se, but their objective lies in obtaining or disrupting information flows. This does not impact the further analyses of this text.

(2) To remind the reader, information has three critical characteristics (or attributes) that need to be maintained in any system : **confidentiality** (no disclosure of information to unauthorised individuals, entities, or processes), **integrity** (assurance of accuracy and completeness of data over its entire life cycle), and **availability** (accessibility of information when needed).

Nevertheless, the characteristics of availability and confidentiality remain under heavy fire, as seen by respectively the 21 October 2016 Internet of Things-powered DDoS attack ("Mirai") and the data theft at Yahoo widely covered in 2016 (see box 1).

Box 1 – The most prominent cyber events of 2016 (1)

Bank of Bangladesh (Bangladesh): In February, cyber criminals hacked into the systems of the Bangladesh central bank and, by compromising the local IT environment, attempted to make several fraudulent transfers. These added up to a total value of $ 951 million. While many of the payments were blocked, $ 81 million was still funnelled out to accounts in the Philippines and diverted to casinos there. Most of those funds are still missing.

Democratic National Committee (USA): In June, reports were made public of two separate breaches in the computer network of this American political organisation. Hacker groups gained access to the entire system, including research databases and emails (which were leaked to the public in July).

Yahoo ! (USA and global impact): In September, this internet company reported the compromise of more than 500 million of its users' names, e-mail addresses, birthdates, phone numbers, and passwords in a breach in 2014. An investigation was triggered by the discovery of a significant chunk of this information being offered for sale on the dark web.

Dyn (also known as the "Mirai" botnet attack) (USA): In October, a widespread distributed denial of service (DDoS) attack on this domain name service (an essential part in guiding internet browsers to the intended domain, which typically serves a website) saw their servers taken offline a number of times. This attack was broadly staged by making use of the plethora of internet-facing devices (through the "Internet of Things" connecting smart devices such as cameras, thermostats, etc.) that were infected with the Dyn malware. This outage affected access to many popular sites such as Twitter, Netflix, Airbnb and The New York Times.

Tesco Bank (UK): In November, the retail banking subsidiary of this UK supermarket fell victim to a hack which occurred most probably through its online banking system. Around 40 000 accounts were affected, almost half of which saw hundreds or thousands of pounds in unauthorised transactions. The company repaid £ 2.5 million of effective losses to 9 000 of its customers. Security experts and regulators have described this heist as an unprecedented attack on the UK's banking sector.

(1) References:
- Bank of Bangladesh: https://www.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8.
- Democratic National Committee: https://www.ft.com/content/d8ddee0e-5168-11e6-9664-e0bdc13c3bef.
- Yahoo !: https://www.ft.com/content/0ebde3b4-80fb-11e6-8e50-8ec15fb462f4.
- Dyn/Mirai: https://www.ft.com/content/d9b8445a-98d0-11e6-8f9b-70e3cabccfae.
- Tesco Bank: https://www.ft.com/content/a0300790-a4ba-11e6-8b69-02899e8bd9d1.

Any potential target that wishes to defend itself comprehensively against cyber attacks must evidently cover all aspects of its information flow, where both *confidentiality* and *availability* are essential to maintain. However, while compromising the *integrity* of its information is often more complex than any impact on *confidentiality or availability* (as access privileges generally need to be escalated further), safeguarding this aspect is often new terrain, where an institution is faced with a plethora of novel and often creative attack patterns. This is partly due to the increased sophistication of cyber criminals, taking their time to become accustomed to the procedures and technical intricacies of the institution under attack, allowing them eventually to tailor their approach into a highly effective attack. This requires targets to be equally flexible and nimble in their cyber stance, in order to improve the chances of being hardened against this.

Furthermore, a holistic stance towards their protection is advised, including not only the organisation itself, but also the counterparties with which it interacts, and the community as a whole. In this tightly interconnected financial ecosystem, most if not all transactions (and/or relating information) go through multiple parties before reaching their destination, many of them being FMIs, but also infrastructure operators and payment service providers. For criminals, this offers a multitude of attack vectors to focus on during the lifetime of a business interaction, and from the point of view of a transaction, one can only be hardened against fraudulent attempts if all steps in the chain are adequately secure.

In the following sections three best practices are discussed, as well as the related policy measures and regulatory initiatives. Section 1 elaborates on penetration testing and red team exercises as techniques to acquire reasonable assurance on the effectiveness of an organisation's protection, detection, response and recovery capacities. Section 2 discusses the need to share information to cooperate with partners in the ecosystem. Section 3 deals with endpoint security for FMIs. The article concludes with an overview of international coordination in the context of cyber security.

1. Penetration testing

Penetration tests are performed to identify vulnerabilities and attack vectors that can be used to exploit business systems successfully. This practice can vary widely in depth and with it, the resulting findings it can uncover. In its simplest form, automated tests are run on parts of the system to uncover some of the more conspicuous security issues. A more robust and encompassing form of assurance can be found in red team exercises. These put a team of outside specialists (the "red team") to assess the all-round security of an organisation by attempting to compromise it, often applying tactics and techniques closely resembling those of a criminal staging a similar attempt (that then has less noble goals). If well executed, the latter type of exercise provides a more realistic picture of an organisation's security stance than exercises that are automated, prepared, and/or announced. Furthermore, the red team may trigger active controls and responses during its campaign, not just limiting the assessment to the effectiveness of protection measures, but also putting an enterprise's detection, response, and recovery capabilities to the test. Of course, the assurance obtained is doubly effective if these exercises are not taken as a snapshot in isolation, but are well-prepared and well-followed-up, long before and after the actual tests take place. This requires sufficient maturity of the information security governance within the organisation, but equally of the security specialists that are performing the tests and guiding the organisation through preparation and debriefing.

Many regulators are working with the industry to encourage adoption of this practice, and to assist the organisations within their jurisdictions with its implementation and execution. One prime example of this is the Bank of England's CBEST[(1)] initiative. The initiative offers a testing framework designed to give major financial institutions and their regulators better insight into their vulnerability to cyber attacks, and the effectiveness of the measures in place. The main innovation of this framework has been in defining a scope much closer to what is essentially at stake, thus reflecting the ongoing strategic battle between cyber attackers and financial institutions. This tends to shift focus away from attempting a definite protection against attacks, a contingency which is, for all practical purposes, impossible to accomplish and might actually lead to complacency and a false sense of security. Rather, the framework seeks to improve an institution's resilience encompassing prevention, detection, response, and recovery as essential capabilities to cope with the full lifecycle of a cyber attack (i.e. including its potential materialisation and aftermath). In this vein, the red team exercises are an essential component put forward by CBEST. Furthermore, the framework ensures that the security experts are competent to perform these tests by subjecting them to accreditation by the Council for Registered Ethical Security Testers (CREST)[(2)].

2. Information sharing

A further cornerstone of the CBEST initiative is the promotion of broad information-sharing in the financial services sector. As mentioned earlier, this is a necessary venture that encourages an institution to recognise the ecosystem it is a

(1) CBEST is an intelligence-led vulnerability testing framework that has been devised by the UK financial authorities (the Bank of England and the Financial Conduct Authority) in conjunction with CREST (the Council for Registered Ethical Security Testers). For more information, see http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx.
(2) http://www.crest-approved.org/.

part of, and with which it shares the general challenges of cyber security. Two broad purposes this information can serve are being distinguished, as characterised by the urgency behind its content. Firstly, there is the information coming from a (potential) breach. Through their business relationships, an institution's direct counterparts may be directly exposed to the effects of such a breach. This requires an institution not only to be prepared for fraudulent incoming traffic, but also – as a sender – to clearly and promptly inform its correspondents of any compromises on its side should they occur. Whereas details of such events will also be reported to local law enforcement agencies and relevant regulators, this does not rule out the need to further reach out to the community by informing the market infrastructures that interconnect it. Furthermore, relevant Information Sharing and Analysis Centres (ISACs) and Malware Information Sharing Platforms (MISPs) offer an opportunity to contribute to common knowledge and insight across the ecosystem, much like on the attacking side: criminals often pool their tools and resources to raise the sophistication of their attacks. Participation in ISACs is therefore a practice that is a crucial element of an industry's resilience, and one which is strongly encouraged.

These ISACs/MISPs also play a fundamental role in divulging this information for its second purpose, one which satisfies more of a long-term, preventive necessity. While indeed the knowledge discussed before served in assisting the immediate reaction to current breaches, its value does not disappear afterwards. These early warnings can still be further analysed and assembled for the community to strengthen its preparations, a function often fulfilled by ISACs. This can result in a positive feedback loop to the benefit of the whole ecosystem: all players in the community contribute information to ISACs, which can then provide informed cyber intelligence such as indicators of compromise and best practices back to the community. This allows all parties access to expertise, allowing them with time to raise the sophistication of their resilience to threats. In this interaction, authorities are certainly not relegated to the sidelines: as well as being a part of this ecosystem, often with their own information and know-how to contribute, this interaction between players can only be optimally constructive given a fitting framework for information exchange. This requires a coordinated and balanced approach between different fields of regulation, such as financial stability, conduct, and privacy[1]. There can also be tremendous value in interacting with other sectors such as the energy and telecoms sector, as financial institutions are certainly not alone in their challenge against these threats.

3. Endpoint security for FMIs

FMIs play a central and systemic role in the efficient functioning of the global financial system. They often aggregate transactions both in volume and in value, and could therefore make them an interesting target for cyber criminals. Strengthening FMIs against any disruption that fraud or criminal attacks on their services can cause is therefore of the utmost importance.

Besides this direct aspect of securing these infrastructures, there is another important role for FMIs: it is through them that the best part of the financial system is interconnected, and this offers an almost natural channel through which fraud can be directed. This interconnectivity lays bare the exposure of any participant in the financial system not only to the security of the FMIs through which it connects, but also to the counterparties that the participant is connected with.

Core to this is a need for any interconnected system to be hardened as a whole, which is a more stringent condition than a sufficient hardening (however advanced) of the central nodes. In essence, any party in a transaction needs sufficient trust that the information encoding a transaction has been kept secure at every step along its way towards its destination: end-to-end security of transactions.

Recent developments such as the Bank of Bangladesh incident have exposed the limits of individual authorities to fully protect these end-to-end flows of the institutions in their jurisdiction. While the regulatory community is moving quickly to coordinate efforts, the centrality of FMIs extends to a responsibility that it has towards its community. That is to say, on top of the immediate responsibility for securing its own infrastructure, and preventing it from being directly compromised, it should also require a level of hardening to be taken up by the FMIs' participants. This unique central position that an FMI has between its participants is what allows it to hold them to high standards, in joint accountability towards keeping the FMI itself secure, and ultimately the entire counterparty community. Since essentially all parties are

(1) See also Caron, F. (2016), *Cyber risk response strategies for financial market infrastructures: towards active cyber defence*, NBB Financial Stability Report, 171-185 (https://www.nbb.be/doc/ts/publications/fsr/fsr_2016.pdf). and Caron, F. (2015), *Cyber risk management in financial market infrastructures: elements for a holistic and risk-based approach to cyber security*, NBB Financial Stability Report, 169-184 (https://www.nbb.be/doc/ts/publications/fsr/fsr_2015.pdf).

at risk of cyber attacks through these channels, this mission to harden the information flows end-to-end can only benefit the community at large.

Currently, this responsibility of FMIs and their participants is highly implicit. The final section will cover some recent efforts that are being undertaken to determine and harmonise the different roles. A key question here is on which party it will fall to set the requirements, enforce them, provide assurance and verify compliance, since these are still necessary elements for maintaining a level of trust that is essential in obtaining financial stability.

4. International coordination

As cyber criminals operate across and from remote jurisdictions, complicating criminal prosecution, and as financial markets themselves are more and more interconnected across borders, an open dialogue and cooperation between all regulatory authorities is necessary to avoid an asymmetry in their respective speed of action. In this cooperation, the ultimate goal is the advancement of the entire ecosystem's resilience in this continuing battle. In this respect, significant efforts have already been made as the regulatory community is actively promoting further hardening of defences.

As a notable example of this, in June 2016 the BIS Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) published their "Guidance on cyber resilience for financial market infrastructures". Inspired by the industry's ongoing endeavours in this area, this guidance aims to offer a coordinated approach, and to foster international consistency in these efforts. This document offers comprehensive guidance in pre-empting cyber attacks, responding rapidly and effectively to them, and achieving faster and safer recovery objectives if they succeed. Alongside the elements of identification, protection, detection, response and recovery, a key concept in this guidance is also the governance aspect, where board and senior management attention is critical to a successful cyber resilience strategy. This guidance is to be applied to the FMIs under the Bank's oversight.

Building further on this guidance on cyber resilience, and sparked by the heightened impact on FMIs and wholesale payments, a new initiative has emerged within the CPMI. It has recently established a task force looking into the end-to-end security of wholesale payments that involve banks, FMIs and other financial institutions (i.e. cyber security in endpoints of payment system networks), thus recognising the increasing attention of cyber criminals towards the high-value transaction chain.