Chapter 1

Security Challenges for the Critical Infrastructures of the Financial Sector

By Ernesto Troiano, Maurizio Ferraris and John Soldatos

DOI: 10.1561/9781680836875.ch1

Published in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures* by John Soldatos, James Philpot and Gabriele Giunta (eds.). 2020. ISBN 978-1-68083-686-8. E-ISBN 978-1-68083-687-5.

Suggested citation: Ernesto Troiano *et al.* 2020. "Security Challenges for the Critical Infrastructures of the Financial Sector" in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*. Edited by John Soldatos, James Philpot and Gabriele Giunta. pp. 2–12. Now Publishers. DOI: 10.1561/9781680836875.ch1.

now
the essence of knowledge

This chapter is an introduction to the first part of the book, which deals with security technologies for the infrastructures of the financial sector. It motivates the need for strong security based on recent security incidents that affected financial institutions. Accordingly, it presents some of the main security challenges for the financial sector, where is also highlights the need for cyber-physical threat intelligence. Furthermore, the chapter presents state-of-the-art technologies that can help confronting the presented challenges. Some of the presented technologies are elaborated in subsequent chapters of the first part of the book.

1.1 Introduction

In the era of globalization, the financial sector comprises some of the most critical infrastructures that underpin our societies and the global economy. In recent years, the critical infrastructures of the financial sector have become more digitalized and interconnected than ever before. Advances in leading edge ICT technologies like Big Data, Internet of Things (IoT), Artificial Intelligence (AI), and blockchains, coupled with a wave of Financial Technology (FinTech) innovations, has resulted in an explosion of the number of financial transactions. Furthermore, the critical assets of financial institutions are no longer only physical (e.g., bank branches, buildings, ATM machines, computer rooms), but rather comprise many different types of cyber assets (e.g., computers, networks, IoT devices) as well.

The increased digitization and sophistication of the critical infrastructures of the financial sector has also raised the importance of cybersecurity in the financial sector. Nevertheless, despite significant investments in cybersecurity, recent large-scale incidents demonstrate that financial organizations remain vulnerable against cyberattacks. As a prominent example, the fraudulent SWIFT (Society for Worldwide Interbank Financial Telecommunication) transactions cyberattack back in February 2016 resulted in $81 million being stolen from the Bangladesh Central Bank. Likewise, the famous "WannaCry" ransomware attacked financial institutions and had a significant adverse impact on Russian and Ukrainian banks. Another major attack took place in 2017, when a data breach at Equifax created a turmoil in the global markets and affected more than 140 million consumers.

In addition to these major incidents, smaller scale attacks against financial institutions happen daily. While most of them are confronted, there are still many cases where these attacks affect the operations of banks and financial institutions, as well as their customers. For instance, back in February 2019, Metro bank was named as a victim of a cyberattack that targeted the codes sent via text messages to customers, as part of the transactions' verification process. A small number of customers of the bank were potentially affected, while the bank reported the issue to relevant security authorities [1]. During the same month, the Bank of Valletta had to shut down all its operations after hackers broke into its systems and moved €13 million into foreign accounts. Specially, the bank shut down all the bank's functions, including branches, ATMs, mobile banking, as well as email services and the website of the bank [2].

In general, the financial sector suffers from security attacks (notably cybersecurity attacks) more than other sectors. During 2016, financial services customers suffered over 60% more cyberattacks than customers in any other sector, while cyberattacks against financial services firms increased by over 70% in 2017. Moreover, a 2018 analysis from the IMF (International Monetary Fund) estimated that emerging cyberattacks could put at risk a significant percentage of the financial institutions' profits, which ranges from 9% to even 50% in worst-case scenarios [3].

In response to the rising number of attacks against financial institutions and their cyber assets, financial sector organizations are allocating more money and effort in increasing their cyber resilience. According to Netscribes, the global cybersecurity market for in financial services is expected to expand at a CAGR (Compound Annual Growth Rate) of 9.81%, leading to a global revenue of USD 42.66 billion by 2023. Other studies reflect a similar estimation, e.g., a Compound Annual

Growth Rate (CAGR) of 10.2% during 2018–2023 and a cybersecurity market growth from USD 152.71 billion in 2018 to USD 248.26 billion by 2023 [4].

1.2 Financial Sector Security Challenges

Through their security investments, financial organizations are striving to confront the challenges described in the following paragraphs. The importance of these challenges has been demonstrated during some of the above-listed security incidents.

1.2.1 Limited Integration Between Physical Security and Cybersecurity

Even though the critical infrastructures of the financial sector comprise both physical and cyber assets, physical security and cybersecurity are still handled in isolation from one another. Specifically, cybersecurity and physical security processes in financial organizations remain "siloed" and fragmented. The latter fragmentation concerns both the technical and the organizational levels, i.e., physical and cybersecurity are handled by different security technologies and different security teams. For instance, physical security systems such as CCTV (Closed Circuit Television) systems, intelligent visual surveillance, security lighting, alarms, access control systems, and biometric authentication are not integrated with cybersecurity platforms like SIEM (Security Information and Event Management) and IDS (Intrusion Detection Systems). Likewise, processes like vulnerability assessment, threat analysis, risk mitigation, and response activities are carried out separately by physical security officers and cybersecurity teams.

This "siloed" nature of systems and process leads to several inefficiencies, including:

- Inefficient security measures that consider the state of the cyber or the physical assets alone, instead of considering the global security context. There are specific types of security attacks (e.g., ATM Network attacks), where security processes like risk assessment and mitigation should consider the status of both types of assets.
- Inability to cope with combined cyber/physical attacks, which are set to proliferate in the years to come. For example, a physical security attack (e.g., unauthorized access to a device or data center) is nowadays one of the best ways to gain access to internal resources and launch a cybersecurity attack as an insider. Indeed, the recent cyberattack against the Bangladesh Central Bank exploited access to physical assets of the bank like SWIFT computing devices.

- Increased costs as several processes are duplicated and overlapping. In this context, an integrated approach to security could help financial organizations streamline their cyber and physical security resources and processes, towards achieving greater efficiencies at a lower cost.

1.2.2 Poor Stakeholders' Collaboration in Securing Financial Services

In an era where financial infrastructures are more connected than ever before, their vulnerabilities are likely to impact other infrastructures and systems in the financial chain, having cascading effects. In this context, stakeholders' collaboration can be a key towards identifying and alleviating issues in a timely manner. However, collaboration is currently limited to exchanging data as required by relevant security regulations and do not extend to join security processes like (collaborative) risk assessment and mitigation.

Information sharing between stakeholders of the financial supply chain is a first and prerequisite step to their collaboration in security issues. In the financial sector, the Financial Services Information Sharing and Analysis Center (FS-ISAC) has been established, as an industry forum for sharing data about critical cybersecurity threats in the financial services industry. FS-ISAC provides its members with access to threat reports with tactical, operational, and strategic levels of analysis for a greater understanding of the tools, methods, and actors targeting the sector. This allows them to better mitigate risk.

Information sharing (e.g., as implemented by FS-ISAC) is a foundation for collaboration in security processes like joint risk scoring for assets and services that are part of the financial services supply chain. Such IT-supported collaborative workflows have been demonstrated in many sectors, including the financial sector. Nevertheless, there are still trust barriers to information sharing and collaboration, especially when data must be shared across private enterprises. Recent advances in IT technologies like blockchain and cloud computing could facilitate the sharing of information and the implementation of collaborative security functionalities.

1.2.3 Compliance to Stringent Regulatory Requirements and Directives

Financial institutions are nowadays faced with a need of complying with a host of regulations, which has a severe impact on their security strategies. For example:

- The Second Payment Services Directive (PSD2): Compliance to the 2nd Payment Services Directive (PSD) demands for banks to be able to interact with multiple Payments Services Providers (PSPs) in the scope of an API-based

Open Banking approach. This raises more cybersecurity concerns and asks for strong security measures like pentesting and vulnerability assessment on the APIs.

- The General Data Privacy Regulation (GDPR): As of May 2018, financial organizations have to comply with the General Data Privacy Regulation (GDPR), which asks for stricter and effective security measures for all assets where personal data are managed and exchanged. Note that GDPR foresees significant penalties for cases of non-compliance, which is one of the reasons why financial organizations are heavily investing in security systems and measures that boost their compliance.
- The Network Information Systems (NIS) Directive [i.e., Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016] [5]: The NIS Directive prescribes security measures for the resilience of the IT systems and networks that support Europe's critical infrastructures, including infrastructures in the financial sector. The prescribed measures include the establishment of risk-driven security polices, as well as the collaboration between security teams (including CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams) at national and international level. The directive defines entities in the Financial services as 2 of the 7 critical sectors and called the member states upon actions to protect and guarantee the availability of their services. Financial organizations are therefore investing in the implementation of the NIS Directive's mandates.
- The EU legislative framework for electronic communications (EU Directive 2009/140/EC) was reformed in 2009 and Article 13a introduced into the Framework directive (Directive 2002/21/EC as amended by Directive 2009/140/EC). Article 13a concerns security and integrity of electronic communications networks and services. The first part of Article 13a requires that providers of networks and services manage security risks and take appropriate security measures to guarantee the security (paragraph 1) and integrity (paragraph 2) of these networks and services. The second part of Article 13a (paragraph 3) requires providers to report significant security breaches and losses of integrity to competent national authorities, who should report about these security incidents to ENISA and the European Commission annually.

1.2.4 The Need for Continuous Monitoring of Transaction and Limited Automation

Financial organizations are nowadays required to secure their infrastructures in a fast moving and volatile environment, which is characterized by a proliferating number of threats and vulnerabilities that are likely to emerge and affect critical infrastructures. Hackers and adversaries are continually taking advantage of leading-edge technologies in order to exploit the rising number of vulnerabilities of the physical and cyber assets of the critical infrastructures. Therefore, it is not practical, and in several cases not possible, to manually carry out all security and protection tasks such as detection, monitoring, patching, reporting, and security policy enforcement activities.

In this context, one of the main challenges faced by the security officers of financial organizations is the poor automation of security functions. To confront this challenge, there is a need for solutions that offer immediate mitigation actions, as well as (semi)automated enforcement of security policies. To this end, financial organizations can take advantage of recent advances in technologies like Artificial Intelligence, Machine Learning and automated orchestration of security functions.

The lack of significant automation is also a setback to fulfilling one of the main security requirements of the financial institutions, which is the ability to monitor transactions without interruptions, i.e. on a 24×7 basis. This is challenging as it requires significant amounts of human resources, including cybersecurity experts and members of security teams. However, it is an essential requirement given that adversarial attacks can happen at any time during the day. Some of the recent attacks against the SWIFT system might have been avoided should a close 24×7 monitoring of transactions and security events was in place.

1.2.5 Lack of Flexibility in Coping with a Proliferating and Dynamic Number of Threats

In addition to automation, security officers of financial organizations are very keen on being flexible when dealing with the proliferating number of threats, including the emergence of several new cyber threats every year. Hence, security departments must be able to deploy new security functions (such as patches or protection policies) very frequently, e.g., daily or even several times per day. In this direction, financial organizations could benefit from latest developments in software engineering practices and methodologies such as the DevOps (Development and Operations) paradigm. Recent research initiatives are exploring the use of DevOps in security systems engineering, which is sometimes called DevSecOps.

1.2.6 Digital Culture and Education

The human factor plays a significant role in alleviating cybersecurity attacks. Proper digital culture and education can provide a sound basis for complying with the mandates of security policies, while avoiding mistakes that could open backdoors to malicious parties. Nevertheless, there is currently a proclaimed gap in digital knowledge in general and specifically in cybersecurity. This holds true for physical security teams as well. Hence, the cybersecurity knowledge gap hinders the implementation of integrated security strategies, while being a setback to the cyber resilience of modern financial institutions.

1.3 Solution Guidelines

With these challenges in mind, the following paragraphs provide solution guidelines and recommendations about securing modern financial organizations. The presented solutions are empowered by advanced security technologies and include the technologies presented in subsequent chapters of this first part of the book.

1.3.1 Structuring and Developing Integrated Security Systems

For over a decade, financial organizations have been deploying and using systems that process and analyze digital information towards implementing cyber defense strategies. Prominent examples include network monitoring and analysis probes, SIEM systems, vulnerability scanners, and more. However, these systems cannot adequately support the definition and implementation of integrated security policies, i.e., policies addressing cyber and physical aspects at the same time. Therefore, there is a need for designing and implementing more integrated systems that will be able to combine cybersecurity aspects with information about physical security, such as information derived from CCTV (Closed Circuit Television) cameras, access control systems, biometric systems, and more.

The design and implementation of integrated security policies requires rethinking of the architecture of the various security platforms, to a direction that considers physical information and devices. Thus, there is a need for new security architectures. The latter can take advantage of the recent advances in Industry 4.0 and the Industrial IoT, including relevant reference architectures such as the Industrial Internet Security Framework (IISF) of the Industrial Internet Consortium [6]. In this context, Chapter 2 introduces the Reference Architecture (RA) of the FINSEC project, which is destined to facilitate the development of data-driven security systems for the financial sector, including systems that address the cyber-physical nature of modern cyber physical infrastructures. As outlined in Chapter 2, the FINSEC RA is implemented based on modern microservices-based approach and can be used to support DevSecOps methodologies in building software systems for security.

1.3.2 Integrated Security Knowledge Modeling

Integrated (i.e., cyber and physical) security systems must deal with data for both cyber and physical threats. Likewise, they should capture and maintain knowledge about both cyberattacks and physical attacks, including combined cyber/physical attacks. Thus, there is need for extending existing security models and format, with constructs that enable them to represent integrated security knowledge. State-of-the-art knowledge bases for cybersecurity consolidate several sources of knowledge for Cyber Threat Intelligence (CTI), such as:

- CPE (Common Platform Enumeration), which is a structured naming scheme for IT software, systems, and packages.
- CWE (Common Weakness Enumeration), which lists common software's vulnerabilities.
- CAPEC (Common Attack Pattern Enumeration and Classification), which lists common attack patterns on software and their taxonomy.
- CVE (Common Vulnerabilities and Exposures), which lists all publicly known cybersecurity vulnerabilities and exposures.

Furthermore, they can also collect and store external CTI data sources through available documents in various formats like JSON (JavaScript Object Notation) and XML (eXtensible Markup Language). There are several knowledge bases available, including commercial SKBs (Security Knowledge Bases) from major security vendors and SKBs from standards development bodies [e.g., the OWASP (Open Web Application Security Project) Security Knowledge Framework]. Nevertheless, these knowledge bases do not include security knowledge for physical assets, which limits their ability to support integrated (i.e., cyber/physical) security.

Hence, there is a need for enhancing knowledge bases and formats for representing cyber-threat intelligence, with information about physical assets and security, towards Cyber-physical Threat Intelligence (CPTI). In-line with this requirement, Chapter 3 introduces FINSTIX, a STIX (Structured Threat Information Expression) based format, for supporting integrated security modeling for critical infrastructures in the financial sector.

1.3.3 Automation and Flexibility

To increase the automation of security processes, financial organizations are nowadays offered with the opportunity of leveraging Machine Learning (ML) and Artificial Intelligence (AI) on large volumes of security data. Specifically, financial institutions are currently collecting large amounts of cybersecurity and physical security related information through many different sensors and probes. This information, if analyzed properly, could provide insights about possible security incidents. Moreover, it can also facilitate the extraction of hidden attack patterns, beyond the ones already known and registered within security knowledge bases. Also, it is possible to employ predictive analytics towards identifying and anticipating security threats before their materialize. This can greatly boost the preparedness of security teams like CERTs.

AI and ML algorithms can boost not only the intelligence and proactiveness of the security processes, but also their automation as well. Specifically, they can automate security and surveillance processes through obviating manual surveillance and tracking of security information streams (e.g., from CCTV systems). Furthermore, they can boost the continuous, 24×7, monitoring of financial systems and transactions, through lowering the human resources needed for the surveillance tasks.

Two of the following chapters introduce data-driven, AI-based solutions for security and surveillance. Chapter 4 presents an AI-based gateway that can combine cyber and physical surveillance in financial environments. The gateway offers a range of intelligence and performance features, which are detailed in the chapter. Also, Chapter 7 presents a novel system for collecting security data from different probes, which incorporates security intelligence (e.g., awareness about security events) towards adapting the rate, the scope, and the context of the data collection.

1.3.4 Information Sharing and Collaboration Across the Financial Services Supply Chain

As already outlined, financial institutions are nowadays digital interconnected as part of different value chains and purposes. SWIFT and SEPA (Single Euro Payments Area) transactions are, for example, carried out across interconnected institutions. As another example, various financial enterprises are interconnected in the scope of trading and stock exchange transactions. Interconnected enterprises are vulnerable to attacks that originate from attacks against other stakeholders in the value chains where they participate. Specifically, financial organizations should not only consider the status of their assets and infrastructures. Rather, they should keep an eye on the status of interconnected infrastructures as well. A potential vulnerability in a connected infrastructure can influence other stakeholders in the supply chain.

Moreover, to address supply chains security, stakeholders had better collaborate in their security processes. As a prominent example, enterprises could engage in collaborative assessments of the risk factors that are associated with their assets. Such processes can be empowered by the automated and seamless sharing of information across stakeholders of the supply chain. Currently, financial organizations share such information as part of regulatory mandates and in the scope of their participation in initiatives like the Financial Services Information Sharing and Analysis Center (FS-ISAC). Nevertheless, the level of security information sharing is still quite low. Lack of trust is one of the reasons that make organizations reluctant to share security information. In recent years, distributed ledger technologies (i.e., blockchain technologies) are explored as a means of sharing information across financial organizations in a decentralized and trustworthy way. Chapter 5 presents a relevant approach, where data shared through a blockchain is used to facilitate collaborative risk assessment.

1.3.5 Regulatory Compliance Technologies

To confront the challenges of regulatory compliance, financial organizations need technologies that facilitate the implementation of relevant technical measures. As a prominent example, data anonymization and data encryption can be used to facilitate adherence to GDPR principles. Likewise, SIEM systems can be used to collect and analyze information about access, transfer, and use of data in an organization, towards identifying potential data breaches. In this context, Chapter 6 presents a suite of security tools for PSD2 compliance. These include, for example, pentesting tools for Open Banking APIs (Application Programming Interfaces), which are destined to identify vulnerabilities of these APIs prior to their use in PSD2 compliant applications.

1.3.6 Security-by-Design and Privacy-by-Design

Beyond regulatory compliance, financial organizations need to adopt new principles regarding the design and implementation of their applications. Specifically, they are expected to adhere to the security-by-design and privacy-by-design principles. The latter should become the preferred path of the software design and development cycle for financial organizations like banks. Likewise, traditional serialized development approaches should be updated towards more flexible and responsive approaches that involve the design and implementation of security controls early in the application development life cycle. Note that privacy-by-design is referenced in the text of the GDPR regulation, and hence, it can serve as a basis for achieving GDPR compliance as well.

1.3.7 Security Education and Training

Financial organizations should heavily invest in security education and training with a twofold objective: First to close the knowledge gap about cybersecurity issues, and second towards engaging the organization's personnel in IT security, regardless of their background and security knowledge. Such measures will help ensuring that employees are no longer one of the weakest links in the security value chain. Along with investments in training and education, financial organizations should be investing in IT security awareness campaigns. In this direction, the FINSEC project is contributing to training and awareness raising based on various trainings and presentations that are available through the market platform of the project, i.e., finsecurity.eu.

1.4 Conclusions

The critical infrastructures of the financial sector are increasing in size, complexity, and sophistication, while at the same time comprising both cyber and physical elements. At the same time, financial organizations are obliged to comply with many and complex regulations and directives about security, privacy, and data protection. As a result, financial enterprises must deal with increased security vulnerabilities and threats in a rapidly evolving regulatory environment. To this end, they are increasing their investments in cybersecurity and its intersection with physical security. Despite the rising investments, they remain vulnerable to security and privacy threats, as evident in several notorious incidents that have occurred during the last couple of years.

In order to properly secure the critical infrastructures for the financial sector, there is a need for new integrated approaches that addresses physical and cybersecurity together rather than dealing with them in a "siloed" fashion. To this end, financial organizations should benefit from the capabilities of emerging technologies like Big Data and AI analytics for security monitoring and automation, while at the same time leveraging the flexibility of the DevOps paradigm that provides opportunity for frequent changes to security measures and policies (e.g., patching on a daily basis). Likewise, integrated approaches to security knowledge modeling and information sharing can be employed. Following chapters of the first part of the book will illustrate novel technologies for cyber-physical threat intelligence, which address several of the security challenges that are currently faced by financial organizations.

Acknowledgments

Part of this work has been carried out in the scope of the FINSEC project (contract number 786727), which is co-funded by the European Commission in the scope of its H2020 program. The authors acknowledge valuable help and contributions from all partners of the project.

References

[1] Natasha Bernal, "Metro Bank hit by cyber-attack used to empty customer accounts," The Telegraph, February, 2019, available at: https://www.telegraph.co.uk/technology/2019/02/01/metro-bank-hit-cyber-attack-used-empty-customer-accounts/

[2] "BOV goes dark after hackers go after €13 m," Time of Valletta, February 2019, available at: https://timesofmalta.com/articles/view/bank-of-valletta-goes-dark-after-detecting-cyber-attack.701896

[3] Antoine Bouveret, "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment," International Monetary Fund (IMF) Paper, July 2018.

[4] "Cyber security in Financial Services Market: Market players, Market Research, Growth During, to 2018–2023," Marketwatch Press Release, September 2019, available at: https://www.marketwatch.com/press-release/cyber-security-in-financial-services-market-market-players-market-research-growth-during-to-2018-2023-2019-09-17

[5] European Parliament and Council. Directive (EU) 2016/1148, measures for a high common level of security of network and information systems across the Union. 2016.

[6] The Industrial Internet Security Framework Technical Report, available at: https://www.iiconsortium.org/IISF.htm (Accessed February 2020).