Cyber risk management in financial market infrastructures : elements for a holistic and risk-based approach to cyber security

Filip Caron

Introduction

Dependence on technology is becoming a defining feature for modern financial institutions. Financial market infrastructures (FMIs) provide the clearance, settlement and recording services for financial transactions between other institutions, creating a strongly interconnected financial system. This heavy dependence on technology and communication networks[1] exposes the FMIs to a variety of cyber threats, which are elements in the cyber ecosystem[2] that could cause harm to an organization, industry or system as a whole.

The cyber threat landscape describing all relevant cyber threats has changed a great deal in recent years. Today, FMIs are confronted with actors specialized in mass-exfiltration and manipulation of sensitive data. Increasingly, the fear is that FMIs might become targets for nation-sponsored espionage and political retaliation. Attacks against the FMIs are expected to become more frequent, sophisticated, targeted and persistent. Cyber risks[3] should be considered as an important operational risk category.

Belgian authorities have identified large FMIs as systemically important organizations in our financial system[4]. In addition to their very heavy dependence on technology, FMIs are characterized by both a high degree of interdependence and complexity. Operational failures due to cyber attacks can result in FMIs that are unable to meet their clearance, payment, settlement or recording obligations (i.e. negative network externalities). Because of the interconnectedness, a cascading failure might threaten the overall financial stability.

Structured and innovative governance approaches are crucial in coping with cyber security. The Committee on Payments and Market Infrastructures (CPMI) indicated that effective cyber resilience is the direct result of comprehensive cyber security strategies, covering cyber incident prevention, detection, response and recovery components. Directors with a high proficiency in cyber security are needed to actively monitor and review cyber governance. Overseers of the FMIs are reviewing which structured approaches will enable FMIs to deal effectively with cyber risk, taking into account the impact on financial stability.

[1] The lack of uniform legal and regulatory regimes and the absence of any international policy further aggravates the situation.

[2] The cyber ecosystem comprises the interactions among persons, processes, data and ICT technologies, and is influenced by a variety of conditions (e.g. regulation, political decisions or available resources).

[3] Cyber risk is the possibility that the actor behind the cyber threat is successful in causing this harm (i.e. successful cyber attack). The potential loss of trust after a successful cyber attack is an important factor to take into consideration.

[4] Additionally, the Belgian Law on the security and protection of critical infrastructure (1 July 2011) categorizes the financial sector as critical infrastructure. (http ://www.nbb.be/doc/cp/nl/bcp/law_01-07-2011.pdf)

This article focuses primarily on the governance of cyber-induced operational risk at FMIs. The remainder of the article is structured as follows: section 1 defines cyber security and provides an overview of the security standards that could form the basis of a comprehensive cyber security strategy. An overview of the general risk management cycle for cyber security will be provided in section 2. The components of holistic cyber security governance are discussed in section 3. Section 4 concludes the paper.

1. Cyber security

Cyber security is the process of defining strategies and implementing measures to protect the organization's assets from occurrences in the cyber ecosystem that have an adverse impact, i.e. cyber attacks. The organization's assets include the information and communications technology, the infrastructure (e.g. buildings and equipment), the personnel, the applications and the totality of information stored and processed by the organization.

In developing cyber security strategies it is crucial to foster the ability to repel cyber attacks, to adapt rapidly, and to recover and/or limit the impact in the event of disruptions caused by such attacks, i.e. cyber resilience. For cyber attacks affecting the FMI's information and communications technology, there is a risk of spreading to other data centres and the fall-back infrastructure of the FMI. While physical damage caused by cyber attacks remains extremely rare, their potential impact could be significant. The most renowned and confirmed cyber attack that intended to cause physical damage is Stuxnet (Falliere, Murchu, & Eric, 2011). This piece of malware was designed to sabotage the centrifuges of a uranium enrichment plant.

A comprehensive cyber security strategy is usually deployed on the basis of security standards. Different standard-setting bodies propose a wide variety of broad security-related concepts for which specific guidance is offered. Typically, these standards cover the following five functional domains:

- Identification: focuses on developing a deep understanding of the cyber ecosystem and the related risks. The former deals with managing the organizational assets (e.g. enterprise architecture, inventory or information system acquisition policy) and analysing the threat landscape (e.g. by actively participating in information sharing and analysis centres). Cyber risk management deals with assessing both the likelihood and the potential impact of the various risks.

- Prevention: covers the activities that deal with developing and implementing safeguards against specific cyber security risks. Firstly, governance-related safeguards that are composed of a broad set of policies and procedures, for example for information security, teleworking or supplier relationships. Secondly, measures concerned with human resources such as personnel vetting, training and awareness. Thirdly, the set of technology-oriented measures that consists of both the implementation of protective technology (e.g. firewalls or network intrusion detection systems) and information system maintenance.

- Event detection: stimulates the adoption of technology and processes to identify cyber security events and incidents[1]. Typically, standards cover the collection of cyber events for forensic purposes and the continuous monitoring of the information systems' behaviour.

- Incident response: focuses on dealing with cyber security events that are taking place. For example, the development of incident response plans (which include escalation procedures), establishing incident communication (including contact with external cyber incident experts), root cause analysis, direct incident mitigation (e.g. information system patching and removal of harmful software), and learning.

- Recovery from incidents: relates the ability to identify and restore the services that have been impaired due to a cyber security incident. Typically, this includes activities related to the development of a recovery plan (e.g. fall-back infrastructure), the introduction of structural improvements and the necessary communication with the various stakeholders.

[1] A **cyber security event** represents an occurrence of importance for the cyber security of an FMI (e.g. rejected access request), whereas a **cyber security incident** describes an event with a negative impact on the organization's assets (e.g. a successful cyber attack).

There are important differences in the type of guidance provided by the various standards : guiding principles, control concepts, implementation guidance and maturity model. For example, in order to preserve the confidentiality and integrity of sensitive information, the cyber security framework of the National Institute of Standards and Technology (NIST, institute affiliated to the U.S. Department of Commerce) includes the following guiding principle : "Data-at-rest is protected" (code PR.DS-1 in the framework). Similarly ISO 27001 prescribes the control of documented information as follows "it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity)" (section 7.5.3 (b) in the ISO 27001 standard). ISO 27002 provides control concepts linked to the principle, e.g. "access control policy" (section 9.1.1 in the ISO 27002 standard). Implementation guidance is provided for example in ISO 13569, which details multiple options for the components of logical access control (section 9.3) : identification, authorization and authentication. The Control Objectives for Information and Related Technology (COBIT) and NIST frameworks provide a maturity model for cyber security strategies. The level of maturity describes the completeness, thoroughness and complexity of the activities and tools used for a specific cyber security component (e.g. access control).

Table 5 in the annex describes the characteristics of a selection of the major security standards that provide relevant guidance for the financial sector. Recently, efforts have been made to develop integrated frameworks that cover all concepts described in the various standards. NIST proposed the cyber security framework for operators and owners of critical infrastructures (NIST, 2014), which includes the financial industry. The CPMI provides guidelines for governance and operational risk in the Principles for Financial Market Infrastructures (PFMIs), which are also relevant for and apply to cyber resilience. Guidance on governance and sound operational risk management are respectively discussed in principles 2 and 17. The CPMI confirmed that cyber risk falls within the scope of both principles. Additionally, both the CPMI and the International Organization of Securities Commissions (IOSCO) have conducted research in order to better understand the FMIs' cyber resilience capabilities and views (CPMI, 2014a) (IOSCO, 2013). The reports indicated that coordinated action and possibly guidance in addition to PFMI principles 2 and 17 may be justified. The adoption of a comprehensive framework might also provide some assurance from a legal perspective, e.g. protecting the FMI against cyber security negligence claims from external parties (Shackelford, Proia, Martell, & Craig, 2014).

2. Stimulating a risk-based cyber security approach

Organizations need to protect themselves against risks originating from cyber threats. The previous section explored the various security guidelines and standards upon which FMIs can structure their cyber risk framework. Cyber security investment decisions should take into account the criticality of the FMI (determinant of proportionality) and the maturity of the existing cyber security infrastructure. This section argues that adopting a risk-based approach can assist an FMI in making cyber security investment decisions and determining priorities.

In the context of FMIs, negative network externalities should be taken into account in the risk-based cyber security approach. The overseer stimulates the development of structured and formal cyber risk management procedures to protect the FMI, and will ensure that the negative network externalities have been appropriately taken into account.

Building a risk-based cyber security approach typically involves an iterative process. The resulting risk management cycles usually consist of four components : risk framing, assessment, response and monitoring. The following paragraphs further detail these components and outline the activities that should be performed at the various organizational levels. Activities at different organizational levels may be interdependent.

2.1 Risk framing

The first component deals with establishing the context and developing a common perspective on how organizations will manage cyber risk. Activities performed in the context of risk framing will result in the specification of a risk management strategy, which details the methodology as well as the assumptions, constraints, risk appetite and (investment) priorities of the organization. This strategy is further defined at three different organizational levels involved in the decision-making process, i.e. the strategic, tactical and operational level. Table 1 provides an overview of the risk framing activities per organizational level.

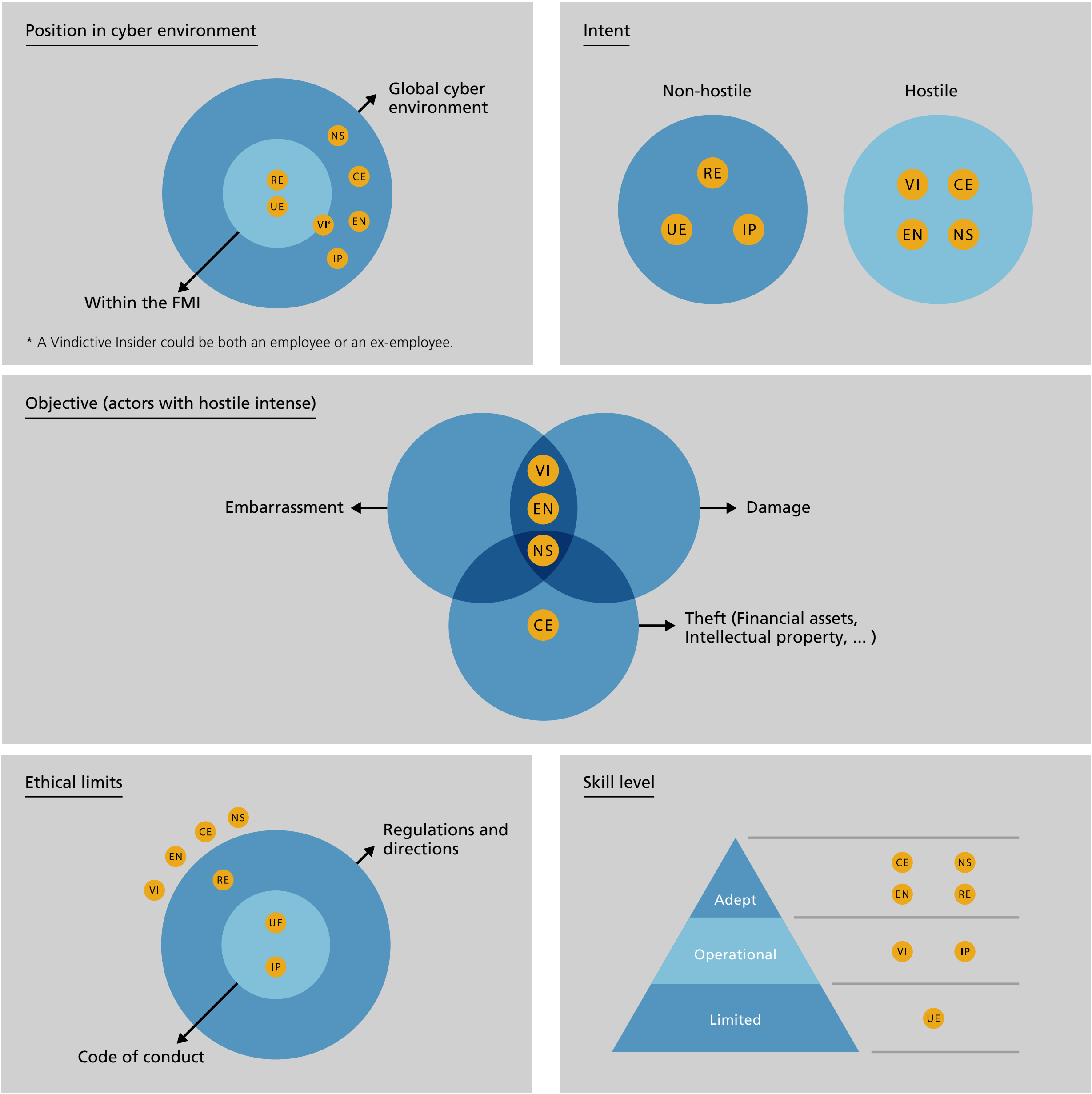
TABLE 1 RISK FRAMING ACTIVITIES

Strategic	• Provide a common perspective by developing the **risk management methodology** (including for example the scope, techniques, risk appetite, priorities, level of detail and communication procedures). • Identify and describe the **broad categories** of threat actors and vulnerabilities. Categorize the types of impacts (i.e. broader than the financial impact). Reviewing trend reports and participating in information sharing and analysis centres (ISAC) will assist in this activity. • Determine the **sources of constraints** for the risk management strategy. A multitude of constraint types can be considered, including financial limitations, regulatory / contractual requirements, organizational policies and limitations originating in the organizational culture.
Tactical	• Identify the **business processes** that support the achievement of the organizational objectives. • Translate the risk appetite into **process-specific risk tolerances**. Differentiation in the risk appetite may be desirable, e.g. extremely low tolerance for processes that could impact on financial stability. • Establish business **process specific context**, analyse which specific threats, vulnerabilities and constraints are relevant for each of the business processes. • Establish the general **risk assessment methodology**, which should ensure consistency in the risk assessments and enable a correct prioritization of the mitigating measures. • Refine the **enterprise architecture** and define the **cyber security components** e.g. including segmentation, creating redundancy and removing single points of failure.
Operational	• Gather **detailed contextual information on the assets**, e.g. asset inventory, owners, network diagrams, data flows, interfaces and existing controls. • Review organizational **responsibilities** for each asset; clarify the accountability for managing the cyber risk.

The specific characteristics of a threat actor determine to a large extent the likelihood and the potential impact of a successful cyber attack initiated by that actor. Therefore, it is crucial to acquire a deeper insight into the threat actors.

Multiple threat actor classifications have been presented in the literature and could be consulted during the risk framing stage, e.g. (Casey, 2007), (Borg, 2014) or (NIST, 2011a). They typically provide information on the specific characteristics of a threat actor type, such as the actor's intent (hostile versus non-hostile), objectives (including theft, business/technical advantage, damage/destruction of assets and embarrassment of the organization), legal and ethical considerations that might constrain the actor, resources (time, money and people) and skill level. Successful cyber attacks require teams with a broad skill set. In addition to expertise in hacking, the team should possess considerable business and process expertise to maximize the outcome (e.g. damage/liabilities or financial gain). Note that these classifications all provide a limited set of archetypes, each with a specific combination of characteristics. Real-life environments may require different combinations of characteristics, e.g. various combinations of resources and skills. Chart 1 provides some examples of threat actor categories.

CHART 1 IMPORTANT THREAT ACTOR CATEGORIES


Position in cyber environment
Global cyber environment
NS
RE
CE
UE
VI*
EN
IP
Within the FMI
* A Vindictive Insider could be both an employee or an ex-employee.
Intent
Non-hostile
Hostile
RE
UE
IP
VI
CE
EN
NS
Objective (actors with hostile intense)
Embarrassment
Damage
VI
EN
NS
CE
Theft (Financial assets, Intellectual property, ...)
Ethical limits
NS
CE
EN
VI
RE
UE
IP
Regulations and directions
Code of conduct
Skill level
Adept
Operational
Limited
CE
NS
EN
RE
VI
IP
UE

Threat actor category

VI **Insider**
An (ex-)employee who feels unfairly treated by the organization.

CE **Criminal enterprise**
Criminal organization that is looking for a maximal financial profit.

EN **Ethno-nationalists**
Experts who share an ethnic identity and feel oppressed or disrespected. Usually a galvanizing incident takes place.

NS **Nation states**
States looking for military, economic or geographical advantage.

RE **Reckless employee**
(Over motivated) employees who take undesired shortcuts or misuse their authorizations.

UE **Untrained employee**
Employee who unknowingly misuses the systems or safeguards.

IP **Information partner**
External contractor with poor data protection with whom the organisation shared sensitive data.

2.2 Risk assessment

Cyber risk assessments are based on the development of cyber threat scenarios. The process of identifying, prioritizing and estimating the risks to which the FMI is exposed, is covered in the risk assessment component.

TABLE 2 RISK ASSESSMENT ACTIVITIES

Strategic	• Identify and describe **threats** to and **vulnerabilities** of an organization. Consulting with cyber threat intelligence companies that are specialized in identifying hostile groups should be an option. • Develop cyber risk **scenarios** and design **potential attack trees**. Sufficient attention should be paid to extreme scenarios.
Tactical	• Identify the **impact of the cyber risk** scenarios on the various business processes. • **Prioritize the business processes** based on impact for both the organization and for financial stability as a whole. The cyber security risk assessment report developed at the operational level should provide the required input.
Operational	• Perform a **cyber security risk assessment** according to the methodology specified by the tactical level in the risk framing component. • Develop a cyber security risk assessment **report** that provides estimates for both the likelihood of a specific scenario and its impact on the assets. The risk assessment estimates should afterwards be aggregated to provide meaningful information for the tactical and strategic level.

Cyber threat scenarios are defined as detailed descriptions of how a threat actor can exploit an organization's dependence on ICT infrastructure to produce an undesirable outcome (e.g. a system take-over or destruction of a service/reputation). For example, scenarios in which a criminal organization acquires access to the FMI's infrastructure and afterwards compromises the integrity of customer transaction data, blackmails the FMI by threatening to destroy critical infrastructure, or extorts money from the FMI by threatening to make sensitive client data public (i.e. confidentiality attack with a significant reputation risk). By refining scenarios like these, an FMI could obtain meaningful risk assessments. Extreme scenarios with combinations of idiosyncratic and sector-wide events that could have a catastrophic impact on the FMI should be taken into account[1].

The FMI should estimate the likelihood of each cyber risk scenario. Is the FMI considered a legitimate object of attack for a specific threat actor? FMIs that would be considered a legitimate object for attack have either (indirectly) offended the actor or symbolically represent an adversary (e.g. a group of nations). In the context of the latter, the threat actor might be more inclined to target systemic infrastructures. Moreover, FMIs should determine whether the information they process or the intellectual property they possess would be of particular value for the threat actor. Acquiring (external) intelligence on the capabilities of the threat actors may also improve the accuracy of the likelihood estimations.

Scenarios should be further refined by producing a set of attack trees, which depict the logical steps and mechanisms involved in a cyber attack. These attack patterns define the challenges that the threat actor might face and how they would be solved. The Common Attack Pattern Enumeration and Classification (CAPEC)[2] provides extensive knowledge on how specific parts of an attack are generally designed and executed. These patterns present the adversary's perspective on the problem and provide guidance on ways to mitigate the attack's effectiveness.

After describing the attack trees, it is possible to determine the business processes and organizational assets that will be impacted in the scenario. The impact will be determined at the operational level based on a dual assessment. The first part of the assessment deals with determining the current level of exposure with regard to the risks identified in

[1] Details on extreme scenarios can be found in the CPMI's recovery for FMIs guidance (CPMI, 2014b).

[2] http://capec.mitre.org/about/index.html (visited on 16/03/2015)

the scenario. Typically, the operational level reviews whether effective controls are currently in place. The effectiveness of the current configuration can be tested by means of penetration testing, vulnerability assessments, code reviews, software reviews or any other appropriate testing procedures. In the second stage, analysts should quantify the costs related to the occurrence of a specific scenario. The value and costs should be defined as broadly as possible, and take account of financial losses, down-time, customers switching to competitors, damage to the FMI's reputation and brand image, indirect costs for other processes and businesses, and other costs. By definition, statistical analyses on historical data (e.g. trend lines, normal distributions, statistical significance or Bayesian corrections), which are traditionally used in operational risk management, will not be adequate in this type of black swan[1] scenario.

2.3 Risk response

Developing risk responses refers to the process of deciding upon and implementing the appropriate courses of action regarding the assessed risks. Traditionally, an FMI has the following risk response options: to accept, avoid, mitigate, share or transfer the risks. Table 3 provides an overview of the risk response activities per organizational level.

TABLE 3 RISK RESPONSE ACTIVITIES

Strategic	• **Decide on the course of action** for the sets of risks related to specific scenarios, taking into account the organization's objectives and the risk appetite. The impact analyses and prioritization exercises of the tactic and operational levels can function as an input. An FMI can opt for one (or a combination of) the following response actions: risk acceptance, avoidance, mitigation, sharing of transfer.
Tactical	• Determine the optimal **risk responses** that translates the generic courses of action into actionable measures (e.g. access control). • Define a **cyber security programme** and propose an implementation **planning** that conforms with the priorities set in the risk assessment component. • Develop a methodology for monitoring the implementation of the cyber security programme, as well as for measuring its effectiveness. • Specifying (design) **requirements, principles and procedures** for the implementation of the actionable measures.
Operational	• Refine each actionable measure into **concrete cyber security controls**. • Determine which cyber security controls need to be added and which existing controls need to be **enhanced**. • **Document the intended application** of each cyber security control. • Draft a **cyber risk mitigating plan**, including the activities for enhancing the cyber defence, the milestones, the required resources and a schedule. • **Enhance the cyber defence** according to the cyber risk mitigation plan.

The international standards on information, ICT and cyber security, discussed in section 1, can provide inspiration for suitable cyber security controls. FMIs should however remain cautious; simply keeping up with compliance requirements as stipulated in standards, directives and regulation will not automatically result in a secure environment. Conversely, non-compliance with these standards, directives and regulation should be considered a significant cyber-related risk in the risk management processes.

Traditionally, cyber defence focuses strongly on developing control structures for mitigating cyber security risks. Alternatively, the FMI could work towards removing some of the motives of potential attackers.

[1] The concept of black swans was developed by Nassim Nicholas Taleb in his books 'Fooled by Randomness' and 'The Black Swan'. Black swans refer to extremely rare events of large magnitude and consequence.

2.4 Risk monitoring and incident response

Typically, the risk monitoring component is composed of the activities related to continuously assessing the appropriateness of the risk responses (i.e. assessing their effectiveness and determining whether emerging changes in cyber risk will be covered) and verifying compliance with a wide set of internal and external directives. Table 4 provides an overview of the risk monitoring activities per organizational level.

TABLE 4 RISK MONITORING ACTIVITIES

Strategic	• Develop a **risk monitoring strategy**, which defines the purpose, type and frequency of the monitoring activities. • Monitor the implementation and **effectiveness of the risk responses** at an organizational level (independent opinions and assurance could be obtained from external consultants or an internal audit function).
Tactical	• Evaluate the **validity of the framework** provided in the cyber security components of the enterprise architecture. If necessary fine-tune or adapt the architecture. • Assess the **tactical effectiveness of the controls implemented** against the framework provided in the cyber security components of the enterprise architecture. • Monitor **changes in the (cyber) environment**, e.g. emerging new threats, cyber incidents and new vulnerabilities such as zero-days.
Operational	• Implement strict **configuration and change management** processes for cyber security controls. • **Assess the effectiveness of the cyber security controls** according to the risk monitoring strategy developed at the strategic level. Reassess controls after changes in order to confirm the appropriateness of the corrective actions. • Review and respond to **vendor or industry warnings/alerts**. • Monitor the information systems for deviations from the standard observed behaviour (i.e. baseline), e.g. with security information and event management (SIEM), applications collecting and correlating events from a wide variety of information systems (i.e. firewalls, network behaviour analysis tools, honeypots, intrusion detection software, and any other event generating system). • Report on the **cyber security status** in terms of both effectiveness and efficiency. This reporting can be both event and time driven. • Implement a **decommissioning strategy**, which includes for example media sanitization and an update of the inventory and configuration management systems.

Incident response capabilities form a key component in the organization's cyber resilience (NIST, 2012). Sound cyber risk management processes can significantly reduce the number of incidents, but there will be incidents that can be neither anticipated nor avoided (i.e. black swan events). Effective incident response handling is based on thorough planning and governance. FMIs should prepare for handling incidents, they should design the incident handler communication infrastructure (e.g. contact information of stakeholders and external experts) and acquire incident analysis hardware and software (e.g. digital forensic software and blank removable media), incident analysis resources (e.g. baselines/normal behaviour, lists of critical assets and network diagrams) and incident mitigation software (e.g. access to uninfected versions of applications). The actual incident response handling consists of incident analysis, containment, eradication and recovery activities.

Incident response handling starts with analysing incident indicators (e.g. network behaviour analysis tools that pick up deviating behaviour) and determining whether an incident has taken place. Initial analyses also specify the scope of the incident, including for example the impacted networks, systems and applications.

At an early stage the team has to decide on a containment strategy to prevent an incident from spreading and to limit the amount of damage. While containment strategies are incident-specific, the decision-making process is usually based on the potential damage caused by the incident (e.g. financial, loss of trust, availability of services), the effectiveness of the strategy, and the time/resources needed to implement the strategy.

After containing the incident, the incident response team can start with the eradication. This phase commonly includes the elimination of the remaining elements of the incident (e.g. breached user accounts or malicious software) and mitigation of the vulnerabilities that have been exploited. The recovery phase deals with restoring the systems' normal operation and may consist of restoring from clean back-ups, rebuilding systems, changing passwords, etc.

This section presented the various components of a risk-based approach to cyber security. Each component will provide input for the next component. Furthermore, risk-based approaches are grounded in continuous processes. Shortcomings of the current set of cyber security controls or changes in the environment identified in the monitoring component will trigger a new iteration of the risk management cycle.

3. Encouraging holistic cyber security governance

Technical cyber security controls and adequate architectures can significantly reduce the cyber risk as acknowledged in most cyber security strategies, but they should be part of a more comprehensive solution. The materialization of cyber risks does not always result from ineffective technical mitigation measures, but can often be directly linked to faulty human behaviour or to external factors. This section first explores the human factor in cyber security before proceeding to discuss the impact of the business environment.

3.1 Senior involvement and accountability

The mission of the board of directors is to secure the future of the FMI and protect the (digital) assets of that organization (Westby, 2004). Currently, this future is increasingly jeopardized by sophisticated cyber threats. Hence, both the board of directors and the management need to develop the ability to cope with future cyber events and to anticipate the impact of those events (IIARF, 2014). This sub-section further outlines the specific actions that need to be undertaken.

The board of directors needs to oversee cyber risk at the FMI and thus to assume its role as the fourth line of defence beyond the 'three lines of defence' model (line management, enterprise-wide risk management, audit). The board's role needs to be underscored. The board should treat cyber risk as an integral component of enterprise risk management (ISF, 2013). Consequently, the directors should oversee the identification of the cyber risks and obtain a clear understanding of the potential impact and the legal implications of their materialization. Activities that should be performed by the directors in this context include:

- Gain insight into the critical business services, applications and data.

- Determine which third parties are involved in providing critical services and review their cyber risk profile.

- Analyse management's cyber security programme and oversee the risk identification, mitigation and management processes developed by the FMI's management. The board can conduct this activity through one of its sub-committees, e.g. the Risk Committee.

- Review annually a cyber posture report requested from the internal audit and/or an external security organization. The board can conduct this activity through one of its sub-committees, e.g. the Audit Committee.

- Discuss key cyber security topics directly with the chief information security officer (CISO) and the chief risk officer (CRO), including cyber events and security breaches.

It has been argued that supporters and sponsors with board credibility can significantly accelerate board engagement in effectively overseeing the cyber risk management (ISF, 2013).

FMIs are confronted by the increasing complexity of their information systems, and by the growing importance of their systems within the financial sector overall. This should be reflected in the composition of the board of directors. Boards could benefit significantly from having directors with a sophisticated understanding of cyber security who are willing to maintain sufficient expertise in the matter.

Even if they are reporting to the board and seeking board guidance, senior managers are ultimately responsible for the identification, assessment, mitigation and monitoring of the risks that threaten their organization, including cyber security risks. Research has indicated that a positive correlation exists between explicitly defining and implementing a comprehensive cyber security strategy and the effectiveness of cyber event detection mechanisms (discussed in (Gregory, 2014)). Effective detection mechanisms in turn can improve the ability to limit the average impact per incident.

In order to develop an effective cyber security strategy, senior managers should engage in the following activities:

- Build a thorough understanding of the ecosystem of the organization's IT operations, which should include trusted partners and customers.

- Identify critical business processes, functions, services and assets.

- Establish a chief information security officer position (or equivalent), reporting directly to the CEO or executive management committee and providing extensive guidance on strategic decisions related to information and cyber security.

- Develop an understanding of the types of potential cyber events and security incidents, and actively monitor the cyber security landscape.

- Ensure that sufficient resources are devoted to the mitigation of cyber risks and to the creation of cyber security awareness in the organization.

- Review the effectiveness of the cyber risk mitigations implemented (e.g. by means of external security audits).

- Sponsor and directly oversee the development of cyber incident response plans.

The senior managers are assisted by the risk managers, who are responsible for facilitating the efficient and effective governance of significant risks, including risk consolidation, and for ensuring risk management uniformity throughout the organization. Internal auditors are considered the third line of defence and conduct assurance activities. They are able to provide an independent assessment of the effectiveness of a broad spectrum of risk management and governance activities and techniques.

3.2 Cyber security culture and insider threats

In The Art of Deception, Keven Mitnick and William L. Simon argue that the impact of social engineering is systematically underestimated in cyber security (Mitnick & Simon, 2002). This seminal work on social engineering states that many cyber-related losses are not caused by a lack of effective technical controls, but by people and faulty human behaviour. The development of cyber security awareness and culture is therefore an important cyber security measure and a means to reduce the insider threat.

A cyber security culture can be defined as a set of shared values, goals and behaviour with regard to the cyber environment. Stimulating the internalization of desired behavioural patterns towards security(1) should improve both the cyber security awareness of the employees and their reaction to unforeseen cyber events. This reduces the risk of reputational and financial damage caused by successful cyber attacks. Management should therefore:

- Ensure that the employees perceive cyber security as an important organizational matter, in which they are engaged and should take responsibility. This could be effectively achieved by providing adequate training and information on

(1) For example, the systematic reporting of irregularities in the operation of information systems or reporting activities of concern.

how their own behaviour could contribute to safeguarding the organization's objectives (e.g. training session for new staff or seminars focused on a specific target audience).

- Provide adequate training and education on cyber security. Different target groups exist, including the regular employees, security experts and IT professionals exposed to the cyber environment such as system administrators.

- Inform (key) employees on the emergence of important threats (e.g. through security alerts).

- Explicitly endorse the cyber security policies and consistently apply them in their own function. Tone-at-the-top is often mentioned as an important driver for success.

- Ensure that cyber security policies are adequate and up-to-date (e.g. new trends such as bring-your-own-device should be addressed).

- Regularly test compliance with the cyber security policies (e.g. hire external consultants to advise employees on dealing with social engineering practices.

FMIs should provide a security-enabling environment. There exists a wide variety of elements that can either enable or inhibit compliance with desired behaviour. Measures that make compliance easier, e.g. taking user-friendliness into account when selecting security tools or providing secured hardware free of charge, are perceived as strong signals of support.

The vindictive insider risk is the second significant human factor that a cyber security strategy should take into account. These (former) employees/contractors will have acquired deep insight into the organization and its information systems. As insiders they obtained an overview of valuable information and have operational knowledge of the processes, controls and technologies that have been implemented to protect this information. Due to this advanced knowledge, cyber security breaches triggered by (former) company insiders tend to be more costly and/or cause more (reputational) damage. The insider as a type of threat actor was described in more detail in section 2 (table 3). In order to mitigate insider threats, management should look into the following risk-mitigating actions :

- Conduct extensive vetting of employees and external contractors, use non-invasive background assessment techniques (e.g. determine the employees' level of satisfaction during the yearly performance evaluation).

- Implement strict access management systems with a least privilege option, monitor failed attempts for unauthorized access, and develop strong access privilege management (e.g. remove authorizations after job rotation or dismissal).

- Introduce four-eyes split responsibility for crucial parts in the processes.

- Employ analysis tools to detect unwanted behaviour (e.g. activity monitoring, confirming the application of the four-eyes principle and data loss prevention tools).

3.3 Third party risk

In addition to acquiring hardware from third parties, organizations increasingly rely on commercial-off-the-shelf software, open source software components, and consultants. Lack of insight in the security procedures of partners, lack of enforcement or ownership, and suppliers that bypass IT security policies, are some of the issues commonly observed in third party relationships. Adversaries may take advantage of these issues to infiltrate FMIs through one of their third-party partners and set up mechanisms for long-term exfiltration of confidential data (e.g. business plans, financial documents and trade secrets).

Consequently, effective attention to cyber security risk throughout the value chain becomes a key requirement for a holistic approach to cyber security governance. For instance, an important aspect is to monitor the behaviour of hardware and software components and ensure that it is completely compliant with set specifications and does not contain any vulnerabilities. Typical examples of cyber risk mitigation activities throughout the value chain include:

- Establish security baselines for external partners (i.e. customers, suppliers and vendors) and legally enforce them through security assurance clauses in agreements.

- Require integration with the third party's incident response processes that handle/have access to critical data.

- Conduct compliance audits with third parties and assess vendor risk.

- Require third parties to comply with the FMI's data privacy policies.

Note that the FMI should also be aware that significant issues can arise further down the value chain, e.g. when the FMI's partners in turn rely on third party agreements.

3.4 Integration and alignment of business processes

Cyber security governance must ensure that the various stakeholders, key processes and strategies work in tandem. The integration and alignment of different business processes focuses on developing a shared understanding of the relevant cyber risks and mutual coordination.

Firstly, cyber security should be fully integrated with the risk management strategies for different domains, i.e. it should become an integral component of enterprise risk management strategy (Bodeau, Boyle, Fabius-Greene, & Graubart, 2010). An integrated approach should result in:

- The positioning/prioritization of cyber security investments compared to other types of investments.

- A clear specification on how the cyber security investments fit into the broader concepts of mission assurance and/or business continuity. Additionally, a distinction will be made between investments that support mission assurance and investments that focus primarily on demonstrating compliance.

- Concise, better coordination between cyber security and other (ICT) investment decisions.

Secondly, in order to ensure a timely and coordinated response to cyber security events, it is advisable to align and integrate cyber risk management with other related business processes. Cyber incidents often have distinct characteristics (e.g. malicious, often persistent, sometimes concealed and usually resulting from the external environment), which should be taken into account in the detection, triage and analysis of the incident. Alignment and integration with well-established incident, problem and crisis management processes directly results in the following benefits:

- Capturing non cyber-specific events that might indicate an underlying cyber origin, such as failed login attempts or crashing applications;

- Access to more complete information on the business and service impact in the event of an information system (component) failure;

- Opportunity to leverage the proven procedures, for example procedures related to communication with the various stakeholders, escalation and ownership, and incident reporting.

Furthermore, cyber security effectiveness is to a certain extent determined by the effectiveness of business processes outside the cyberspace; e.g. employee hiring and screening processes and physical security processes (e.g. to avoid tailgating[1]).

[1] Tailgating refers to the act of entering a restricted area by following an authorized person without his/her consent.

3.5 Information sharing

Early warnings and expert advice on cyber events are crucial in ensuring that cyber security objectives are met. Information sharing and analysis centres (ISAC) are institutions that focus on providing this type of cyber intelligence. These institutions build strategic partnerships between companies, governments, universities and non-profit organizations.

FMIs are encouraged to participate in these ISACs. An independent participant, e.g. a governmental institution, ensures that the information is non-attributable and thereby avoids (further) reputation damage. A good example is the American FS-ISAC, which focus on incumbents of the financial sector. In the European Union the Network and Information Security (NIS) Directive aims to foster ISACs and to provide a concrete structure for sharing information between market participants and the various authorities. The implementation of the NIS directive is expected in early 2017.

Conclusion

Cyber threats have emerged as important drivers of risk for FMIs. Furthermore, cyber attacks against systemically important FMIs pose serious threats to financial stability. This is due to a number of reasons, including the heavy dependence on technology, the high levels of interdependence and the complexity of the FMIs. In addition, cyber attacks are becoming more frequent, sophisticated and persistent.

While standards provide a wealth of recommendations to improve the cyber security of an organization, FMIs are encouraged to implement a rigorous risk-based approach to cyber security and extreme scenarios. Risk-based approaches permit better coordination between the various investments in cyber security and improve the allocation of scarce resources. The role of the overseeing authorities is to ensure that the operational risk of the FMIs remains within the acceptable risk appetite, and that the negative network externalities are adequately addressed.

The overseeing authorities encourage a more holistic perspective on cyber security governance. The cyber security strategies of the FMIs should not focus exclusively on improving the technical cyber security controls, but should also include initiatives to develop a security culture and awareness, to stimulate senior involvement, to manage third party risk and to integrate the cyber security efforts in the broader (inter/intra)organizational context.

TABLE 5 INFORMATION (TECHNOLOGY) SECURITY STANDARDS COMMONLY ADOPTED IN THE FINANCIAL SERVICES INDUSTRY

Standard	Reference	Author			*Identify*			*Prevent*						*Detect*		*Respond*					*Recover*			Guidance				Industry	
		Governmental	Industry	Independent	ICT assets management	Threat environment analysis	Cyber risk assessment	Access control & HR	Training and awareness	Information security	Maintenance ICT systems	Protective technology	Policies and procedures	Events collection	Continuous monitoring	Response planning	Incident communication	Incident analysis	Incident mitigation	Learning	Recovery planning	(Structural) improvement	Communications	Principles	Controls	Implementation	Maturity model	All industries	Financial industry
COBIT 5 [1]	(ISACA, 2012)		X		X	X	X	X	X	X	X	X	X	X	X	X		X		X	X	X	X		X		X	X	
CSC (SANS)	(SANS, 2013)			X	X		X	X	X	X		X	X		X	X					X				X [2]			X	
ISO13569:2005	(ISO, 2005)			X			X	X				X	X		X			X	X		X				X	X			X
ISO/IEC27001:2013 ..	(ISO/IEC, 2013)			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X [3]			X	
ISO/IEC27002:2013 ..	(ISO/IEC, 2013)			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				X	X		X	
ISO/IEC27005:2011 ..	(ISO/IEC, 2011)			X		X	X																	X		X		X	
ISO/IEC27015 2012 ..	(ISO/IEC, 2012)			X	X			X	X	X	X	X	X	X	X										X	X			X
NIST SP 800-39	(NIST, 2011)	X				X	X		X						X									X				X	
NIST SP 800-53 v4 ...	(NIST, 2013)	X			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X		X	
NIST Cyber Security ..	(NIST, 2014)	X			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X [4]	X	
PCI DSS	(PCI, 2010)		X					X		X		X	X		X										X	X			X

[1] COBIT 5 organizes IT governance objectives and good practices in controls over information technology in a logical framework of IT related processes. While COBIT is not an information technology security standard as such, it contains risk and security processes that have been often implemented in the financial sector.

[2] The CSC guidelines do not claim to provide a comprehensive control catalogue; they provide a small number of actionable controls which considerably increases the organization's level of protection.

[3] A high-level overview of the control concepts elaborated in ISO/IEC27002:2013 is presented in annex A of ISO/IEC27001:2013.

[4] The NIST cyber security framework includes a tiers-based scheme that strongly resembles a maturity model.

References

Bodeau D., Boyle S., Fabius-Greene J. & Graubart R. (2010). Cyber Security Governance. Mirte.

Borg S. (2014, February 24-28). Implementing a Quantitative Risk-Based Approach to Cyber Security. Retrieved from RSA Conference 2014 : http://www.rsaconference.com/writable/presentations/file_upload/str-w01-implementing-a-quantitative-approach_v2.pdf

Casey T., (2007). Threat Agent Library Helps Identify Information Security Risks. Santa Clara, CA, USA : Intel Corporation.

CPMI. (2014a). Cyber Resilience in Financial Market Infrastructures. Basel : Bank for International Settlements.

CPMI. (2014b). Recovery of Financial Market Infrastructures. Basel : Bank for International Settlements & OICV-IOSCO.

Falliere N., Murchu L. O. & Eric C. (2011). W32.Stuxnet Dossier. Cupertino, CA, USA : Symantec.

Gregory H. J. (2014, March). Board Oversight of Cybersecurity Risks. Thomson Reuters Practical Law, pp. 24-28.

Group IB – Fox IT. (2014). Anunak : APT against Financial Institutions (aka Carbanak). Group IB – Fox IT.

IIARF. (2014). Cybersecurity : What the Board of Directors Needs to Ask. Altamonte Springs, Florida : The Institute of Internal Auditors Research Foundation.

IOSCO. (2013). Cyber-Crime, Securities, Markets and Systemic Risk. Madrid : international Organization of Securities Commissions.

ISACA. (2012). Control Objectives for Information and Related Technology. Information Systems Audit and Control Association.

ISF. (2013). Engaging with the Board : Balancing Cyber Risk and Reward. Information Security Forum.

ISO. (2005). ISO 13569 :2005 – Financial Services Information Security Guidelines. International Organization for Standardization.

ISO/IEC. (2011). ISO 27005 : 2011 – Information Technology – Security Techniques – Information Security Risk Management. International Organization for Standardization – International Electrotechnical Commission.

ISO/IEC. (2012). ISO/IEC 27015 : 2012 – ISMS Guidance for Financial Services. International Organization for Standardization – International Electrotechnical Commission.

ISO/IEC. (2013a). ISO/IEC 27001 : 2013 – Information Technology – Security Techniques – Information Security Management Systems – Requirements. International Organization for Standardization – International Electrotechnical Commission.

ISO/IEC. (2013b). ISO/IEC 27002 : 13 – Information Technology – Security Techniques- Code of Practice for Information Security Controls. International Organization for Standardization – International Electrotechnical Commission.

Mitnick K. & Simon W. (2002). The Art of Deception : Controlling the Human Element of Security. Hoboken, New Jersey, USA : John Wiley & Sons.

NIST. (2011a). Guide to Industrial Control Systems (ICS) Security (SP800-82). Gaithersburg, Maryland, USA : National Institute of Standards and Technology.

NIST. (2011b). NIST SP 800-39 : Managing Information Security Risk – Organization, Mission and Information System View. Gaithersburg, Maryland, USA : National Institute of Standards and Technology.

NIST. (2012). Computer Security Incident Handling Guide (SP 800-61 Rev.2). Gaithersburg, Maryland, USA : National Institute of Standards and Technology.

NIST. (2013). NIST SP 800-53 Rev.4 : Security and Privacy Controls for Federal Information Systems and Organizations. Gaithersburg, Maryland, USA : National Institute of Standards and Technology.

NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg, Maryland, USA : National Institute of Standards and Technology.

PCI. (2010). Data Security Standard. Payment Card Industry.

SANS. (2013). Critical Security Controls – Version 5. SANS Institute.

Shackelford S., Proia, A. A., Martell B. & Craig A. (2014). Toward a global cybersecurity standard of care ? Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity standards. Texas International Law Journal.

Westby J. R. (2004). International Guide to Cyber Security. Privacy & Computer Crime Committee.