Cyber risk response strategies for financial market infrastructures : towards active cyber defence

Filip Caron

Introduction

Technology is fundamentally transforming the financial industry and its underlying financial market infrastructures (FMIs). Innovation is being embraced by FMIs to streamline their processes for clearing, settling and recording financial transactions between market players. While technological advances enable FMIs to develop competitive advantages in an increasingly complex world, these advances also expose them to a variety of new types of threat, such as cyber threats. Indeed, it appears that a variety of actors might in fact be interested in unlawfully gaining access to transactional information or in compromising the confidentiality, integrity and/or availability of an FMI's information systems.

Recent cyber incidents in diverse industries have indicated that it can be notoriously hard to adequately protect and defend an information system. The complexity of information systems and interaction between them makes it nearly impossible to identify all entry points to an information system. Moreover, developing a control environment that effectively protects all entry points would most probably not be (economically) feasible[1].

The main premise in cyber security increasingly becomes: a *security breach will be inevitable.* In this context it is important to complement the protective security measures with capabilities to rapidly detect, analyse and mitigate malicious activities in the information systems. Cyber security strategies developed according to the principles of active cyber defence aim at (near) real-time detection, analysis and mitigation of cyber threats, preferably before damage occurs.

This article will discuss the components of a comprehensive cyber defence strategy permitting this real-time detection, analysis and mitigation. The next section starts by positioning active cyber defence in a layered cyber security strategy. Active cyber defence requires the effective implementation of supporting techniques, and these will be described in sections 3 and 4. Section 5 elaborates on the actual active cyber defence techniques and section 6 concludes the article. The techniques described in this article are applicable for all financial services organisations.

[1] The thematic article in the 2015 Financial Stability Report describes the process of building a risk-based cyber security strategy (Caron, 2015).

1. Towards active cyber defence

Cyber risk mitigation strategies have been continuously evolving. FMIs have constructed highly sophisticated defensive perimeters around their critical information systems, but the new security-breach-inevitability assumption has generated a strong momentum for the development of resilient[1] and active cyber defence strategies (Dewar, 2014).

While active defence strategies are often associated with retaliatory action, these strategies cover a broader set of interdependent activities, and might even explicitly exclude retaliation. *Active cyber defence aims at the fast identification, detection, analysis and mitigation of immanent cyber threats.*

Implementing active cyber defence strategies requires robust processes and practices, which could be organised in a layered architecture as depicted in Chart 1. Developing effective cyber defence practices attributed to a specific layer requires the presence of robust practices appertaining to lower layers. For example, retaliatory actions require strong attribution of a cyber attack, which in turn requires that the information systems continuously capture relevant information on their status.

Planning forms the basis of an effective active cyber defence strategy. It should enable the FMI to determine how it will defend its critical assets against looming threats. The focus should be on determining both the risk appetite and the threats in the organisation's environment. Exercises which define risk appetite also need to take into account the additional business and legal risks that could be created by particular active defence practices.

Based on the findings of the planning layer, the organisation should *adapt* its infrastructure in order to limit the possible attack paths. After establishing an initial foothold, the attackers typically focus their efforts on lateral movements through the information systems in order to identify the assets of value. Typically, the practices in the second layer are oriented towards restricting entry points, reducing the direct interdependence between information systems and shielding critical information assets.

The third layer focusses on the implementation and positioning of *detection* mechanisms in the adapted infrastructure, as well as on external collaboration. Decisions on information capturing within the information systems will have an impact on the available analysis options. For example, data flows can only be analysed when network devices register the packages that pass by them. Proactive, anomaly and forensic *analysis* capabilities are located in the fourth layer.

Practices in the top layer deal with *responding in real time* to a cyber attack. This layer includes activities to contain the infection, to trace the cyber attacker who has gained unauthorised access to the infrastructure, and retaliatory hacking.

[1] Resilient cyber defence strategies emphasise the continuity of service provision under extreme circumstances, e.g. cyber attacks or natural disasters. Guidance papers such as (CPMI-IOSCO, 2015), encourage FMIs to develop disaster recovery functions, to elaborate cyber business continuity plans, and to adopt technological diversity.

CHART 1 ACTIVE CYBER SECURITY STRATEGY

Supporting actions *(FSR 2015)*	Active cyber defence strategy layers	Active cyber defence actions *(FSR 2016)*
• Incident communication • Recovery planning	Real-time react	• Cyber incident response team • Trace back • Retaliation
• Events collection	Analyse	• Security incident and event management • Incident analysis
• Cyber threat environment analysis	Identify and detect	• Cyber threat intelligence sharing and coordination • Honeypots
• Cyber risk assessment • Preventive cyber defence controls	Plan	• Active cyber defence planning • Adapt to defend

All cyber defence processes and practices are to some degree associated with one or more of the following cyber security objectives: intelligence gathering, annoyance, containment, attribution and attack. The intelligence gathering, attribution and attack objectives are straightforward to interpret. Annoyance involves deceiving the attacker, e.g. by establishing decoy environments, which could significantly increase the amount of resources needed by the attacker to obtain control over the critical information assets. Containment refers to techniques that isolate the infected information system components in order to protect the other components from contamination.

The next four sections will highlight some of the major techniques in the different layers.

2. Enabling active cyber defence

Each active cyber defence strategy comes with its own prerequisites. The information systems' architecture needs to comprise some basic defence components, e.g. for containing system infections. These defence components might not be present in the current portfolio of information system resources, which tends to include multiple legacy systems. This section will discuss the planning activities and some of the most effective measures for improving the cyber defence readiness of the existing portfolio. Other relevant practices are adequate patching and a continuous vulnerability assessment.

2.1 Active defence planning

Planning is the logical first step in the development of an active defence strategy and will enable the FMI to concisely define how it will defend its critical information assets against relevant threats. Table 1 provides an overview of common practices in active defence planning.

Cyber defenders must acquire a clear understanding of the mission-critical business processes and the information assets most coveted by potential attackers. Regular meetings with the business operations could foster a better understanding of the business risks and concerns. These basic business insights will become valuable when a defence decision needs to be made. A recent survey suggested that only 23 % of organisations with a dedicated active defence team explicitly invest in developing these business insights (Ernst & Young, 2015). These are organisations that are commonly considered to have obtained a high level of cyber security maturity.

TABLE 1 ACTIVE DEFENSE PLANNING

Organization	• Facilitate direct interaction between cyber defenders and business experts; • Document the business assets and resources that need to be protected, e.g. financial, intellectual property and customer data. Classify these assets and resources in terms of sensitivity and priority; • Document and update how the information systems are designed (including the sources of security operations data such as alert logs) and what is considered to be normal behavior in the information system. Identify critical information that is lacking; • Determine the defense capabilities you will establish in house and what you require from external experts. Establish working relationships with external cyber incident response teams.
Environment	• Identify and describe the relevant threat actors. Threat actor classification schemes can support this analysis, e.g. (Casey, 2007); • Detect strong dependencies on third party service providers and technologies. Research the vulnerabilities related to these services and technologies.
Risk appetite, assessment and mitigation planning	• Define the residual risk tolerance levels, taking into account regulatory and contractual requirements; • Identify the potential legal and business risks of different active defense strategies; • Select the active cyber defense practices that will be implemented and develop an implementation roadmap.

Acquiring advanced technical expertise in defending every aspect of the information systems might not be (economically) feasible. FMIs are encouraged to determine which cyber defence activities will be outsourced. Developing working relationships with capable and trustworthy experts forms an integral part of the planning layer. Guidance on selecting these experts can be found in (Creasey, 2013).

The assessment of the organisational environment and the risks posed by this environment were discussed in last year's article (Caron, 2015). Planning an active defence strategy requires the selection of practices in higher layers. Certain active defence strategies will introduce additional risks. These risks will be considered during the discussion of the related active cyber defence strategies.

2.2 Adapt to defend

Network segmentation and data flow restrictions are considered as important first lines of defence against a cyber security breach.

Segmentation could constrain lateral movements between the information system components, as well as enabling faster isolation of compromised segments. The cyber attack against Target, where card details were stolen after the security of the heating-ventilation-and-air-conditioning system was breached, is an often-cited example of a lack of network segmentation.

Furthermore, segmented networks enable FMIs to differentiate the levels of cyber security in the various segments. For example, the segments containing the infrastructure to host the official webpage might be considered less critical than the segments containing services of systemic importance for our financial system.

Restricting inbound data flows will reduce the risk of receiving malicious code. Controlling outbound data flows helps prevent data leaks and could stop malware connecting back to the intruder's servers. Table 2 discusses the implementation of these defence components.

TABLE 2 ADAPT TO DEFEND

Network segmentation	• Segment the network in logical enclaves of information resources, e.g. based on the user (anyone, customers, employees, developers, etc.) or product lines; • Consider implementing demilitarized zones (DMZs) between systems with strongly different security requirements; • Limit the exposure of legacy systems by encapsulating them in well-managed segments; • Develop and impose access policies for the different network segments taking into account the principles of least privilege and need-to-know; • Enforce data encryption in highly confidential segments.
Restrict data flows	• Impose stringent policies on the data that can be transferred between network segments; • Limit data flows into network segments (i.e. ingress filtering); • Restrict the outbound data flows of network segments (e.g. egress filtering and sinkholing); • Consider the use of proxy servers for data flows.

Several standards are actively promoting network segmentation to segregate critical services and sensitive data (e.g. customer data or source code) from less secure network components, e.g. (CPMI-IOSCO, 2015). Similarly, the National Bank of Belgium stressed the importance of network segmentation in its guidance on the expectations for business continuity and information security for systemically important financial institutions (National Bank of Belgium, 2015). Furthermore, the scope of mandated security assessments might be significantly reduced if organisations can demonstrate effective network segregation for their critical services (PCI, 2015).

While physically disconnecting network segments would prevent lateral movement, it would also disable intersegment data flows. This might obstruct legitimate business behaviour, e.g. a customer trying to connect over the internet to a critical service. A multitude of other approaches have been suggested. For example, VLAN technologies enable the logical grouping of information system components regardless of the underlying physical connections. Cyber criminals with access rights to a specific VLAN could attack an underlying component in an attempt to gain privileges to other VLANs supported by that component (i.e. VLAN hopping) (Altunbasak, *et al.*, 2005).

Recently, software-defined networking (SDN) has been suggested as a set of technologies to manage networks, enabling the implementation of granular and flexible policy management for network segments. In a software-defined network, the controller orchestrating the network and its flows could become the weakest link (ONF, 2013).

In addition to segmentation, the FMI should consider restricting the data flows to the different segments. Where possible the FMI should consider whitelisting for ingress and egress filtering (e.g. identified customers or trusted self-managed servers), instead of using a blacklist. Furthermore, FMIs could opt for indirect flows between segments with significantly different levels of trust, e.g. between customers on the Internet and the internal network. This could be achieved by directing the flows to proxy servers located in between the firewalls of a demilitarised zone (DMZ). Data flow analysis tools could be added to the DMZ in order to detect attempts at data exfiltration and malicious code delivery. However, legitimate encryption tunnels – for example to the hijacked computers of a customer – could still be used for data exfiltration.

3. Identification and detection techniques

FMIs that have adapted their infrastructure, network and information systems to improve their cyber defence readiness need to ensure that effective mechanisms for the identification of threats and detection of cyber attacks are put in place. A comprehensive overview of detection systems can be found in (Scarfone & Mell, 2007).

Cyber threat intelligence sharing & collaboration and honeypots are two detection mechanisms that are often mentioned in the context of active defence. These techniques will be further developed in this section. An overview of the related considerations can be found in Table 3.

TABLE 3 THREAT IDENTIFICATION AND DETECTION

Cyber threat intelligence sharing and collaboration	• Develop a sharing framework that describes the objectives and scope of the sharing initiative, as well as its conditions under which sharing would be permitted; • Define data storage, sharing and protection standards for threat intelligence, consider encryption and sanitization of sensitive information; • Establish formal and informal sharing relationships. Consider appointing a liaison officer (fostering long term trust relationships) and signing memoranda of understanding (for formal multilateral sharing initiatives); • Participate in the sharing relationship: distribute the results of your cyber threat analyzes and incident investigations; • Contribute to knowledge maturation, i.e. bringing together seemingly unrelated observations to distil robust sets of indicators of compromise; • Improve the internal control system of the FMI based on the intelligence received through the sharing initiatives.
Honeypots	• Determine the type (low versus high interaction) and location of the honeypots; • Implement adequate protective measures that isolate the honeypot form the legitimate systems in the network; • Consider restricting outbound flows to protect legitimate systems of innocent third parties (for high interaction honeypots); • Ensure that the honeypot provides a "realistic" decoy environment, i.e. that it contains technologies and data elements that are expected to be found in the real information systems; • Reserve sufficient resources to analyze honeypot activity, to communicate the findings and to formulate actionable recommendations for improving the internal control system.

Two important general considerations should be mentioned. Firstly, detection mechanisms do not provide any value without the skilled experts to evaluate the situation. These systems may generate a multitude of false positive alerts, e.g. for exceptional but legitimate network flows. Further analysis may be required (analysis layer) and mitigating actions might need to be taken (active defence layer). Secondly, failure to detect anything does not necessarily mean that a cyber attack is not imminent or even taking place. If there are no effective detection mechanisms, it might be almost impossible to identify, analyse and stop subtle attacks (e.g. espionage-driven attacks).

3.1 Cyber threat intelligence sharing and collaboration

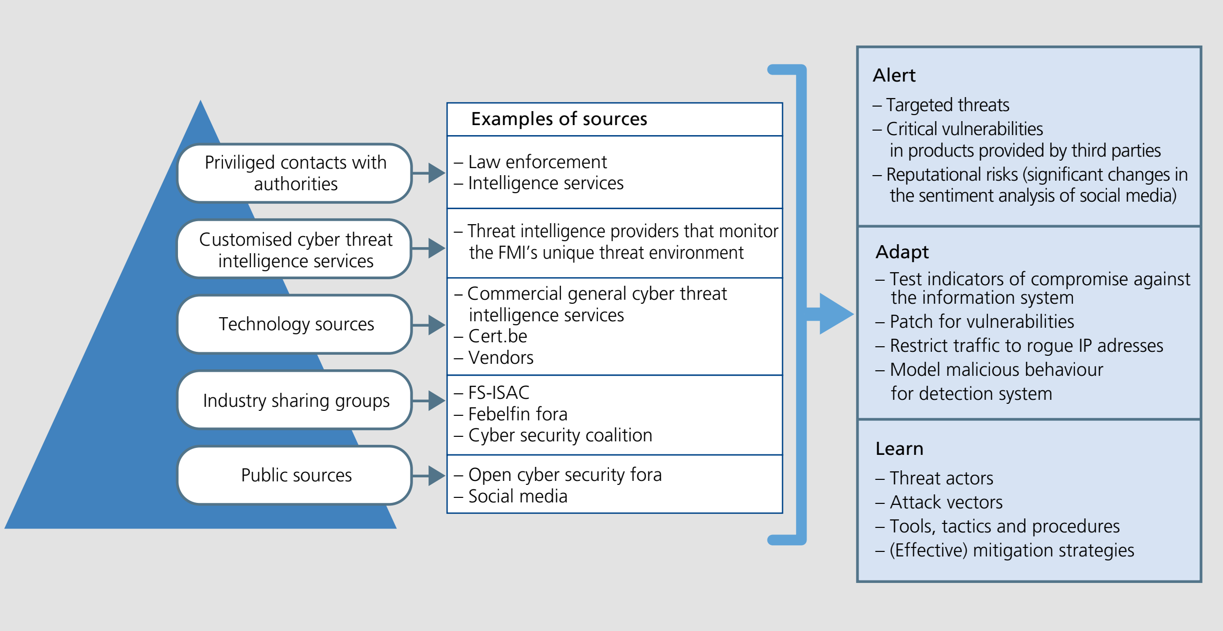
Significant *commoditisation* of successful cyber attacks has been observed (Sood & Enbody, 2013). Cyber intrusion tactics that appear to be successful in breaching the security of an organisation are often quickly directed against (similar) organisations. For example, investigations revealed that the Carbenak attack vectors have been directed at up to a hundred banks, e-payment systems and other financial institutions (Kaspersky Lab, 2015).

FMIs are encouraged to set up cyber threat intelligence-sharing relationships with their peers, commercial threat intelligence services and law enforcement agencies. Individual organisations that limit their threat analyses to their own information systems and networks may be left blissfully unaware of targeted attacks against their industry sector, acquired technology or business processes.

Various information-sharing and analysis centres (ISACs) and computer emergency response teams (CERTs) have been established. FS-ISAC is a global non-profit organisation that focuses on providing a platform for cyber and physical threat intelligence analysis and sharing. For Belgium, Febelfin has signed a Memorandum of Understanding on intelligence sharing with FS-ISAC. Additionally, the federal cyber emergency team CERT.be and the cross-sector Cyber Security Coalition provide platforms for cyber intelligence exchange.

FMIs could further enrich the cyber threat intelligence obtained from their peers with information acquired from open source fora, commercial cyber threat intelligence services, or law enforcement agencies. Commercial threat intelligence services gather information from a variety of sources, which is filtered and further analysed. They provide their clients with detailed cyber threat reports customised for their industry or even their organisation. Figure 2 provides an overview of the different cyber threat intelligence sources.

CHART 2 CYBER THREAT INTELLIGENCE SOURCES (ORDERED ACCORDING TO THE INCREASING RELEVANCE FOR THE FMI)


Priviliged contacts with authorities
Customised cyber threat intelligence services
Technology sources
Industry sharing groups
Public sources
Examples of sources
– Law enforcement
– Intelligence services
– Threat intelligence providers that monitor the FMI's unique threat environment
– Commercial general cyber threat intelligence services
– Cert.be
– Vendors
– FS-ISAC
– Febelfin fora
– Cyber security coalition
– Open cyber security fora
– Social media
Alert
– Targeted threats
– Critical vulnerabilities in products provided by third parties
– Reputational risks (significant changes in the sentiment analysis of social media)
Adapt
– Test indicators of compromise against the information system
– Patch for vulnerabilities
– Restrict traffic to rogue IP adresses
– Model malicious behaviour for detection system
Learn
– Threat actors
– Attack vectors
– Tools, tactics and procedures
– (Effective) mitigation strategies

Standardisation in the structuring of actionable threat intelligence promises to further foster sharing initiatives. The Organization for the Advancement of Structured Information Standards focuses on the continued development of three open cyber threat sharing standards: STIX, TAXII and CybOX (OASIS, 2015). These standards respectively focus on the structuring of threat information, the definition of a message exchange protocol, and the specification of observable events in information systems and networks.

There are currently two major obstructions to fruitful threat intelligence sharing: privacy concerns and the lack of an adequate sharing framework. Firstly, precise descriptions of threats could contain data elements that are considered to be personally identifiable information (PII), e.g. the IP addresses that were used to launch the attack (Gorzelak, *et al.*, 2011). Secondly, the lack of an adequate sharing framework hampers active participation in sharing initiatives. A recent survey indicated that only 24 % of the organisations were 'very likely' to share information with the community, and more than half of the respondents stated that this was due to inadequate policies (Dinkar, *et al.*, 2016).

A potential pitfall of successful cyber threat intelligence sharing is that the security analysts could become overwhelmed by notifications. External triage might be a useful service in that context. Due to economies of scale, cloud providers trying to protect their customers' virtual resources might develop an advantage under such circumstances.

3.2 Honeypots

During cyber attacks there are often extended periods in which the victim organisation is unaware of the ongoing attack. By remaining under the radar, the intruder can identify and locate the most valuable pieces of information. Decoy cyber resources or honeypots could be deployed to detect malicious behaviour and characterise adversaries.

Honeypot are commonly divided into two types: low interaction and high-interaction (Grudziecki, Jacewicz, Juszczyk, Kijewski, & Pawlinski, 2012). Low-interaction honeypots provide the cyber attacker with emulations of some potentially vulnerable services which are expected to be found in the FMI's information systems. They do not provide all the functionality that is commonly found in an operational information system, but will be able to respond to (basic) malicious activities such as port scanning. In contrast, high-interaction honeypots offer a more complex environment with full operating system and application functionality. They may therefore provide far richer insights into the attacker's behaviour.

Honeypots give an FMI the facility to rapidly collect a limited amount of highly valuable information, i.e. all recorded connection to and behaviour in a decoy environment must be considered suspicious. This potential can only be achieved if the FMI allocates sufficient resources and places the honeypots in strategic positions. Firstly, the FMI will have to devote significant resources both to develop realistic decoy environments, in order not to tip off the intruders, and to analyse all suspicious behaviour. Secondly, the location of the honeypots will affect the security and the potential findings. By implementing a honeypot in a well-managed DMZ environment, the FMI protects its legitimate systems from lateral movement originating from the honeypot. Alternatively, honeypots could be placed in the internal operations environment to act as sensors for infected systems. Network segmentation will limit the scope of the sensor capabilities to the segment in which the honeypot is located.

Moreover, attackers are increasingly able to spot (commercial low-interaction) honeypots. As a result, the attacker who is able to identify a honeypot may decide to either avoid it or perform irrelevant actions on it. Both will significantly impair the value of the honeypots as detection mechanisms.

However, downstream liability is probably the most important risk related to the implementation of a high-interaction honeypot (Grant, 2004). Research has indicated that under certain circumstances the extensive functionality of these honeypots could be exploited to launch an attack on other systems (McGrew & Vaughn, 2006). In order to limit the downstream liability risk, the honeypot operator might consider prohibiting or limiting outbound connections to third parties.

Other legal risks which could be broadly categorised as negligence liabilities have been cited. If you identify important weaknesses through your honeypot, you should remedy them promptly and effectively. Honeypot analyses could indicate that the organisation has been aware of an important weakness but neglected to correct it (promptly) (Harrington, 2014).

Honeypots are not the only deception mechanisms available to an FMI. Detection mechanisms can be configured to intercept the transmission of honeytokens, i.e. decoy data such as fake user credentials and program code. Careful selection is crucial to the use of honeytokens.

4. Analysis techniques

Security events are significant occurrences, i.e. something that happens at a certain point in time and is triggered by someone or by a system component. For example, a router passes a packet between two other network components, or a cyber attacker changes the content of a certain file. Typically, information systems and applications tend to record a wide variety of events occurring within their perimeter. Other sources of these security events include detection systems, data/intrusion prevention systems and mitigation techniques (e.g. antiviruses). Together, these events contain a wealth of information on what happens in the FMI's information systems and infrastructure. Security incident and event management tools provide a means to collectively analyse the relevant events.

While these security events are a valuable input for the analysis of an incident's impact, these analyses tend to require the investigation of additional data. Incident analyses may also examine malware samples or verify whether critical files have been corrupted. An overview of the analysis-related activities can be found in Table 4.

TABLE 4 ANALYSIS TECHNIQUES

Security incident and event management	• Identify the relevant sources of security events (hardware/software logging, detection and prevention controls …) and establish centralization of these events; • Define, refine and update the rule-set based on both expected and abnormal behavior; • Adapt the rule-set whenever new threat intelligence is obtained; • Establish processes to respond to events and alerts generated by the SIEM.
Incident analysis	• Set up multi-disciplinary incident handling teams that consist of forensic, legal, business and communication experts with a deep insight in the information systems and business operations; • Define data extraction, collection, reduction and custody policies; • Consider the development of a software reference library for in-house developed and customised applications; • Decide on the priority between forensic analysis and incident containment for different lines of business. Take relevant directives and business risks into account; • Develop a scientifically accepted methodology and build relationships with firms specialised in cyber forensics.

4.1 Security incident and event management

Security incident and event management (SIEM) tools enable the collection and correlation of security relevant data from a wide variety of information system components. Complex attack vectors might not be intercepted by individual detection mechanisms, but automated rule-based analyses on integrated data could flag these vectors. Some tools will take historical information and risk correlations into account. An example of a correlation rule might be triggering an alert when an unusually large number of emails are bounced in combination with antivirus notifications, as this might be the result of a poorly designed phishing attack.

The integration of security data and the analysis possibilities that this integration creates are considered to be the major advantage of SIEM tools. These tools do not replace other detection measures, such as network intrusion detection systems, firewalls or malware detection systems.

Implementing an SIEM tool is not considered straightforward due to the increasing complexity and the excessive requirement for professional services (Schultz, 2009). Three considerations will have a significant impact on the effectiveness of the SIEM implementation: the quality of the correlation and detection rules, the coverage of security events, and the response processes.

Developing the correlation and detection rule-set is an iterative process, which starts with modelling expected and/or abnormal behaviour. Results from organisational and environmental analysis in the planning layer will support the definition of expected behaviour. Threat analyses and intelligence could provide actionable inputs for abnormal behaviour. Depending on the flexibility and predictability of the business processes, providing alerts for all deviating behaviour might not be desirable as it could overwhelm the incident response team with false positives.

The rules in the SIEM rule-set will need to be continuously refined. Penetration tests could provide valuable insights into the detection capabilities of the developed rule-set and highlight blind spots. Additional detection mechanisms and log-generating components will be introduced over time, which may require their incorporation in existing rules and/or demand new rules. Similarly, new threats will continue to appear and influence the rule-set.

Optimising the coverage of the SIEM tool will be crucial in order to reduce the risk of non detection and inaccurate reporting of incidents. Consequently, the FMI will need to ensure that sufficient detection and event registration mechanisms are precisely positioned in its infrastructure. Moreover, all critical detection and registration mechanisms must be connected to the SIEM in order to avoid critical gaps in the collected information.

Well-designed SIEM tools will not provide additional value for cyber security programs unless they are combined with effective processes to respond to the generated alerts. As previously mentioned these processes require highly skilled experts. The active defence section will discuss this in more detail.

4.2 Incident analysis

FMIs operate diverse interlinked information system components which generate huge amounts of data. As intruders often move laterally between these components, data relevant to a cyber attack is likely to be scattered over multiple files and storage devices.

The objective of incident analysis is to identify, collect, preserve and analyse data in order to reveal the details of a cyber attack and its impact, without damaging the integrity of the evidence. A wide variety of incident analysis techniques can be applied, including memory analysis, data recovery techniques, data analytics and malware reengineering. While it remains difficult to predict exactly which techniques will be needed to investigate a specific attack, having some incident policies in place can ensure that evidence cannot get lost or corrupted.

FMIs are encouraged to proactively analyse the context in which incident analyses would take place. This involves identifying experts with both technical and business knowledge who could direct and conduct the analyses, setting up priorities for collecting (volatile) evidence, analysing related regulatory requirements, selecting incident analysis toolkits, and contacting specialised external experts. SIEM tools which provide centralisation of security event logs could assist in the rapid reconstruction of the intruder's activity sequence. By maintaining a software reference library, which contains digital signatures of the in-house or customised applications, the FMI rapidly eliminates known-to-be-good files during an incident analysis. The National Software Reference Library (NSRL) holds an extensive collection of digital signatures of known software applications (NIST, 2016). A similar approach can be taken for other data files.

The rapid adoption of cloud technologies has sparked discussion on the validity and reliability of forensic sciences in this new context. Investigators have less insight into and control over the information system resources in the cloud. There are considerable differences between the cloud models. Infrastructure-as-a-service (IaaS) clouds offer a set of virtualized computer resources and the greatest scope for evidence collection, as it enables the user to configure the systems and install advanced detection and monitoring software. In contrast, software-as-a-service (SaaS) cloud solutions provide on-demand software without insight in or access to the underlying components, which results in the narrowest scope for evidence collection. The 65 principal challenges are enumerated in (Dykstra, *et al.*, 2014).

There may be other impediments to incident analysis. Firstly, it is almost impossible to analyse files that have been encrypted by the cyber attacker. Similarly, steganography that relies on embedding data within other data can be notoriously hard to trace, e.g. digital watermarks or hiding information in images. Secondly, incident analysts must take into account the incident containment strategies of the FMI. While incident analysts would opt for isolation of the information systems affected in order to preserve the evidence, the FMI may prioritise the rapid restoration of (part of) its services.

5. Active defence techniques

The techniques of the previous layers provide the base capabilities required to adequately react in case of a cyber incident. Table 5 lists three important technique sets that deal with containing the infection, with tracing back the cyber attacker who gained unauthorized access to the infrastructure and with retaliatory hacking.

TABLE 5 ACTIVE DEFENSE TECHNIQUES

Cyber incident response team	• Develop a cyber incident response plan that focuses on incident detection; notification & escalation; communication; and coordination with forensics and vendors teams. • Define an incident categorization scheme. • Acquire containment and remediation capabilities. • Establish contingency plans. • Outline processes for post-incident evaluations and follow-up on recommendations.
Trace back	*FMIs could consider the deployment of trace back techniques under specific circumstances:* • Apply trace back techniques in internal networks, while respecting all privacy and other legal restrictions. • Inform and collaborate with law enforcement agencies and internet service providers before starting the trace back exercise outside their own network.
Retaliation	*FMIs are strongly advised not to engage in retaliatory actions.*

5.1 Cyber incident response team

As a cyber security breach may become inevitable, FMIs should consider the establishment of a cyber incident response team or blue team. The cyber incident response team could be proactive by conducting incident prevention campaigns and developing incident response plans and capabilities. However, the focus should be on the detection, containment and remediation of the incident. The team should play an important role in the recovery of the operations.

Cyber incident response teams should be able to review the FMI's cyber security programme and challenge the security designs for applications and changes to the existing infrastructure. Through recommendations on these designs, a cyber incident response team will aim at ensuring that adequate defence mechanisms are available to limit the impact of a cyber attack. It should be noted that optimal defence mechanisms in real-world business settings might deviate from technologically optimal defence mechanisms. For example, two internet-facing servers with the same security policies but supporting different business services could be placed in the same DMZ zone from a technological cost-effective perspective. However, the business might opt for separate segments to protect the business services from cyber incidents impacting on the other service.

The second proactive activity deals with specifying operation and incident response procedures. It is important to consider the staffing roles. While the cyber incident response team should contain highly skilled ICT experts familiar with the information systems and the infrastructure, it could greatly benefit from the input of legal, public relations, business and human resources experts. Legal experts will have to ensure that the actions remain compliant with regulations (including privacy laws), assess third party exposure and protect the admissibility of the collected evidence. Public communications might play a critical role when the incident affects service delivery or a third party, e.g. customers who are not able to perform financial transactions. Business experts could assist in prioritising the services that need to be protected. Human resources experts could advise the team when the organisation faces a malicious insider.

Previous sections have provided an overview of incident detection mechanisms. Established and effectively configured SIEM tools will provide the cyber incident response team with valuable initial assessments. These assessments will enable the team to categorise the incident and notify the right level of decision makers.

Containment strategies focus on isolating the affected components. By restricting the network connectivity to those components, the cyber incident response team prevents the malware from receiving further commands from the attacker and from moving laterally between components of the organisation's information system.

After isolating the affected components, the cyber incident response team will focus on removing the threat and restoring the business services. Recent proposals for cyber security guidance have suggested that an FMI should design and test its systems and processes to enable the safe resumption of critical operations within two hours of a disruption, and to enable complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios (CPMI-IOSCO, 2015).

5.2 Trace back

Organisations confronted with a cyber attack often aim at tracing the origin of the attack, i.e. determining who launched and assisted in the attack. Obtaining this information would be useful in legal action and for some immediate threat mitigation activities, e.g. blocking malicious traffic and hacking back. Moreover, cyber security experts indicate that a strong attribution might be a critical component in cyber attack deterrence (Geers, 2010).

There are two main types of technique : tracing back the origin of a message flow and forced self-identification of the attacker.

Firstly, message flows can be reconstructed by means of marking, logging and input debugging techniques. Marking requires the routers to add flow information to the individual IP packets. Deterministic marking is often used for critical applications that require advanced security services such as non-repudiation. As this requires the marking of all packages, it entails a significant processing overhead. Alternatively, probabilistic marking reduces the processing overhead but complicates the reconstruction of the message flow. Logging requires network devices that are configured to log unique identifiers of packets (e.g. hashes) which they have handled. These logs could be queried afterwards. In contrast to marking and logging, input debugging is based on a continuous message flow in the future. Input debugging is based on the iterative processes of requiring adjacent network devices to report the occurrence of a behavioural pattern.

Resourceful cyber attackers can make attribution extremely difficult. Techniques include – but are certainly not limited to – spoofing, laundering hosts, and varying the timeframes in which events take place.

Secondly, forced self-identification or beaconing is based on enhancing files containing sensitive information with code that phones home, i.e. sends a message back to the servers of the legitimate owner. Depending on the circumstances, the message that is sent back may contain valuable information for identifying the intruder. Web bugs in a file are considered a benign version of beaconing. These bugs are basically links to a surreptitious object, which will be retrieved from a server at the site of the legitimate owner. Web bugs are commonly used in email messages to link to externally stored images. Upon opening the email, the email management software sends a message including the user's IP address and other information in order to obtain the image.

5.3 Retaliation

The ability to initiate legal action, holding cyber attackers accountable for the damage caused by them, can be considered a significant deterrent. Yet effective legal action seems difficult to achieve in the current context. This is partly due to the cross-border nature of contemporary cyber attacks, i.e. the attacks are often launched from jurisdictions with less developed criminal justice systems (Messerschmidt, 2013). Cross-border cyber crime could create thorny jurisdictional issues, but a lack of legislation adapted to the current cyber space is also a commonly cited weakness (Kuchler, 2015).

Additionally, legal action against cyber attackers may result in public disclosure of the cyber security weaknesses. Such public disclosures could pose significant business risks, e.g. by having a major negative impact on the reputation of the organisation under cyber attack.

Hence, victims of a cyber attack may be tempted to respond in kind, i.e. by means of hacking back or retaliatory hacking. In general, cyber attack victims can deploy the same tools and techniques as the cyber attackers. Retaliatory attacks generally focus on achieving at least one of the following objectives: destroy, disrupt, degrade, deny and exploit.

Destruction involves responses that cause complete and permanent damage to the attacker's computer systems, i.e. the systems can no longer perform any function and need to be entirely rebuilt. Exploitation is a related objective in which the victim organisation conducts vengeful activities that involve accessing the attacker's computer systems in order to collect and/or modify data in its systems.

Disruption aims at interrupting the flow of information to the attacker's computer systems. For example, last year the FBI, Europol and several security vendors succeeded in poisoning the botnet of the Dridex banking Trojan's and redirecting infected systems to a sinkhole (Leyden, 2015). Hence, the infected computers in the botnet were no longer sending information back to the cyber attackers.

Degradation is meant to reduce the effectiveness and/or efficiency of the attacker's computer systems. The activation of a fork bomb could be considered as a degradation-based retaliatory action. These bombs are often disguised as important-looking information, and organisations can place them in strategic positions; once the bomb leaves its original position or is copied, it starts continually replicating itself. At a certain point the system's resources will be depleted, resulting in a system crash (Nong, 2008).

Denial-based strategies focus on preventing the attacker from accessing and using critical information and/or services. The use of ransomware-like software on your own data which is triggered when the data is accessed by an unauthorised party could block access to the data without rendering other systems unusable (Laperruque, 2015).

As organisations involved in retaliatory hacking are using techniques similar to those of the cyber attackers, they are exposed to the same legal risks as cyber attackers. Through retaliatory hacking, an organisation is at the very least knowingly (or even intentionally) accessing an information system without authorisation. This is in itself a criminal offence (Wong Yang & Hoffstadt, 2006). But the organisation also faces non-legal risks.

Retaliatory hacking raises the risk of collateral damage to innocent parties (Lewis, 2013). By routing their communication and commands through the information systems of innocent parties, trace back analyses may result in misattribution. Retaliatory hacking on the systems of innocent bystanders will result in financial losses and have an impact on the brand and goodwill of the organisation.

Playing cat and mouse with serious cyber attackers may result in them raising their game, e.g. launching even more sophisticated and destructive attacks. Retaliatory hacking may have two outcomes: the attacker either decides to move on to an easier target, or perceives the attack as an invitation to return fire. Security analysts have warned that organisations are not ready to compete with large criminal organisations or nation states (Fisher, 2013). Furthermore, in (Harrington, 2014), the author indicates that customers might wonder whether their data has been placed at risk because of escalation.

Finally, an organisation's code of corporate ethics and business conduct should reflect its corporate values, including uncompromising integrity, responsibility and good citizenship. Organisations that empower or direct security experts to conduct retaliatory hacking may violate their own code of corporate ethics and compromise their ethical standing in the community.

Conclusion

In a world where FMIs increasingly assume that they will inevitably face a security breach, the development of an operative real-time incident response capability becomes crucial. The effectiveness of these active defence capabilities is very dependent on the existence and quality of the supporting techniques and access to internal and external experts.

Active cyber defence requires a carefully designed multi-layer cyber security strategy. Careful planning and an infrastructure that comprises a basic defence mechanism are fundamental. Detection and analysis techniques should provide the necessary information to conduct effective cyber incident responses.

Effective cyber incident response programmes complement advanced technologies with professionals from diverse backgrounds to mitigate the various risks related to an incident. Additionally, these experts should carefully evaluate the legal, reputational and business risks related to the mitigating actions.

Bibliography

Altunbasak, H., Krasser, S., Owen, H. L., Grimminger, J., Huth, H.-P., & Sokol, J. (2005). Securing layer 2 in local area networks. *Lecture Notes on Computer Sciences 3421*, 699-706.

Arnold, M., & Brathwaite, T. (2015, January 22). Davos 2015 : Banks call for free rein to fight cyber crime. *Financial Times*.

Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic Cyber Intelligence. *Information and Computer Security*, 317-332.

Caron, F. (2015). Cyber risk management in financial market infrastructures : elements for a holistic and risk-based approach to cyber security. *Financial Stability Review (National Bank of Belgium)*, 169-184.

Casey, T. (2007). *Threat agent library helps identifiy information security risks*. Santa Clara : Intel Corporation.

CPMI-IOSCO. (2015). G*uidance on cyber resilience for financial market infrastructures*. Basel : CPMI-IOSCO.

Creasey, J. (2013). *Cyber Security Incident Response Supplier Selection Guide*. CREST.

Dewar, R. S. (2014). The « triptyck of cyber security » : A classification of active cyber defence. *6th International Conference on Cyber Conflict* (pp. 7-21). Tallinn : NATO CCD COE Publications.

Dinkar, D., Greve, P., Landfield, K., Paget, F., Peterson, E., Schmugar, C., . . . Sun, B. (2016). *McAfee Labs Threat Report*. Santa Clara : Intel Security.

Dykstra, J., Gowen, L., Jackson, R., Reemelin, O. S., Rojas, E., Ruan, K., . . . Zatyko, K. (2014). *NIST Cloud computing forensic science challenges*. Gaithersburg, Maryland : National Institute of Standards and Technology.

Ernst & Young. (2015). C*reating trust in the digital world : EY's Global Information Security Survey 2015*. London : EY Risk Advisory.

Fisher, M. (2013, May 23). Should the U.S. allow companies to 'hack back' against foreign cyber spies ? *The Washington Post.*

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law and Security Review*, 298-303.

Gorzelak, K., Grudziecki, T., Jacewicz, P., Jaroszewski, P., Juszczyk, L., & Kijewski, P. (2011). *Proactive detection of network security incidents* I. Heraklion, Greece : European Network and Information Security Agency.

Grant, E. P. (2004). System Security Liability. In *GIAC Security Essentials*. SANS Press.

Grudziecki, T., Jacewicz, P., Juszczyk, L., Kijewski, P., & Pawlinski, P. (2012). *Proactive detection of security incidents II : Honeypots*. Heraklion : European Network and Information Security Agency.

Harrington, S. L. (2014). Cyber security active defense : Playing with fire or sound risk management ? *Richmond Journal of Law & Technology*, 12.

Johnson, C., Badger, L., & Waltermine, D. (2014). *Guide to cyber threat information sharing*. Gaithersburg : National Institute of Standards and Technology.

Kaspersky Lab. (2015, February 16). *The great bank robbery ; Carbanak cybergang steals $ 1bn from 100 financial institutions worldwide*. Retrieved from Virus News : http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response*. Gaithersburg : National Institute of Standards and Technology.

Kuchler, H. (2015, July 27). Cyber insecurity : Hacking back. *Financial Times.*

Laperruque, J. (2015, July 28). *How CISA's countermeasures authorizatin threatens security.* Retrieved from CDT : https : / / cdt.org / blog / how-cisas-countermeasures-authorization-threatens-security /

Lewis, J. A. (2013, May 22). *Private retaliation in cyberspace*. Retrieved from Center for Strategic and International Studies : http : / / csis.org / publication / private-retaliation-cyberspace

Leyden, J. (2015, October 14). FBI takes down Dridex botnet, seizes servers, arrests suspect. *The Register*.

Marinos, L., Belmonte, A., & Rekleitis, E. (2016). *ENISA Threat Landscape 2015*. Heraklion : European Union Agency for Network and Information security.

McGrew, R., & Vaughn, R. B. (2006). Experiences with honeypot systems : Development, deployment and analysis. *39th Hawaii International Conference on System Sciences* (pp. 1-9). IEEE.

Messerschmidt, J. E. (2013). Hackback : Permitting retaliatory hacking by non-state actors as proportionate countermeasures to transboundary cyberharm. *Columbia Journal of Transnational Law*, 275-324.

National Bank of Belgium. (2015). *Circulaire : Aanvullende prudentiële verwachtingen op het vlak van de operationele bedrijfscontinuïteit en beveiliging van systeemrelevante financiële instellingen*. Brussels : NBB.

NIST. (2016, March 4). *National software reference library*. Retrieved from Information technology library : http : / / www.nsrl.nist.gov /

Nong, Y. (2008). *Secure computer and network systems : Modeling, analysis and design.* Wiley.

OASIS. (2015, July 16). *OASIS Advances automated cyber threat intelligence sharing with STIX, TAXII, CybOX.* Retrieved from Standards : https : / / www.oasis-open. org / news / pr / oasis-advances-automated-cyber-threat-intelligence-sharing-with-stix-taxii-cybox

ONF. (2013). *SDN security consideration in the data center.* Palo Alto : Open Network Foundation.

PCI. (2015). *Data Security Standard v3.1.* Payment Card Industry.

Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)*. Gaithersburg : National Institute of Standards and Technology.

Schultz, E. (2009). Security information and event management (SIEM). In H. Tipton, & M. Krause, *Information security management handbook, 6 Edition*. New York : ISC2 Press.

Sood, A. K., & Enbody, R. J. (2013). Crimeware-as-a-service : A survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, 28-38.

Strand, J., Asadoorian, P., Robish, E., & Donnelly, B. (2013). *Offensive countermeasures : The art of active defense*. CreateSpace.

Willis, B. (2012). *Sharing cyber-threat information : An outcomes-based approach*. Santa Clara, US : Intel Corporation.

Wong Yang, D., & Hoffstadt, B. M. (2006). Countering the cyber crime threat. *American Criminal Law Review*, 201.