Capital Markets Information Security Monitor

Continue reading

AFM

Table of contents

Summary

Business processes of capital market institutions are strongly (and increasingly) dependent on more and more complex IT environments. This dependence makes capital market institutions vulnerable to both internal and external cyber risks, which affect the availability, integrity and confidentiality of information and systems. Capital market institutions are required by national and European legislation to take information security measures to safeguard the continuity and reliability of their IT and information systems and to prevent or limit the consequences of possible IT incidents and cyberattacks.

The AFM considers information security and related cyber risks to be one of the important operational risks for capital market institutions. Not only is the number of cyberattacks increasing, the disruptive impact of attacks is also growing. Cyberattacks have the potential to seriously disrupt the continuity of business operations. For this reason, the AFM conducts market-wide and individual investigations at capital market institutions and cooperates with the financial sector to further strengthen the resilience of capital market institutions.

This information security monitor 2022 contains the most recent observations on IT and cyber risks, based on a self-assessment survey completed by fourteen capital market institutions (trading venues, proprietary traders, and clearing & settlement institutions). This survey confirmed that capital market institutions face high inherent information security and cyber risks, with 80% of participants indicating that their inherent IT risks are high.

Our supervisory interviews and surveys show that the observations mentioned in this information security monitor are also relevant for Dutch capital market institutions in general. These observations are summarised below:

1. IT is crucial to business operations and is a key driver of innovating business practices. A high degree of digitalisation and key dependencies on IT increase the need for robust IT risk and information security management. The AFM recommends that capital market institutions take appropriate measures and implement procedures and processes to ensure the continuity and reliability of their information systems.
2. Agile, DevOps and a hybrid approach to software development are the most popular. Security can be a significant challenge in DevOps. The AFM recommends embedding information security in the development process and testing software for security vulnerabilities.
3. Management of IT outsourcing and supply chain risks is critical. Outsourcing increases the dependency on third parties. The AFM recommends incorporating adequate information security management into cyber supply chain risk management practices. Furthermore, institutions face high inherent IT availability and continuity risks. Adequate business continuity measures are important to recover from cyberattacks. The AFM recommends that capital institutions develop and maintain a plan to respond to cyber incidents and quickly adapt to disruptions.
4. Security Operations Centres (SOCs) are an important tool in dealing with increasing cyber threats. The establishment and effective operation of SOC teams, or similar security teams, contributes to controlled business operations. The AFM recommends that capital market institutions cooperate proactively in detecting and responding to IT and information security incidents in the chain of outsourced services and IT infrastructure.
5. The IT architecture of capital market institutions is complex. Effective change and configuration management processes are more important in organisations with a complex IT architecture. The AFM recommends that capital market institutions implement information security control measures in line with the complexity of their IT architecture.

6. Implementing patches is fundamental to ensuring the security of systems. Moreover, patch management is an important strategy in minimising cyber security incidents. The AFM recommends that capital market institutions put in place a patch management policy in line with their IT and business strategy and implement critical security patches in line with their risk appetite.
7. Clearly defined Recovery Time Objectives (RTOs) are set for critical business processes. Setting RTOs and Recovery Point Objectives (RPOs) is an important step in business continuity management. The AFM recommends setting clearly defined RTOs for the most critical business processes in line with the organisation's risk appetite.

Observations

Observation 1: IT is crucial to business operations and is a key driver of innovating business practices

Capital market institutions have a high dependence on IT both for running the organisation's business processes and services and for innovating business practices. All institutions in scope indicate that IT is of strategic value for the organisation, meaning that it is critical for both running and innovating the organisation's business processes and services.

A high degree of digitalisation and key dependencies on IT increase the need for robust IT risk and information security management. In view of the applicable laws and regulations, and in line with our principles[1] for information security, the AFM recommends that capital market institutions take appropriate measures and implement procedures and processes to ensure the continuity and reliability of their IT, information and the provision of information, and to limit the impact of any security incidents to an acceptable level as determined by the organisation. Internationally accepted risk management frameworks for IT, such as ISO 27001 and ISO 27002, COBIT, NIST Frameworks, and guidelines from CPMI-IOSCO, can provide guidance in this regard.

Observation 2: Agile, DevOps and a hybrid approach to software development are the most popular

All capital market firms in scope indicated that they develop software in-house. Only 14% of capital market institutions indicate that they use a classic (waterfall) approach to software development, separating software development and operations. In most cases, an Agile, DevOps or hybrid approach is used.
For each development methodology it is important that information security is part of the development process and that the software is tested for security vulnerabilities. DevOps has replaced siloed development and operations and has the advantage that integration and deployment of new software is automated (CI/CD pipelines), which reduces the time to market. However, security is not always included in DevOps. Security is therefore one of the significant challenges in DevOps. Unless the security team operates in collaboration with the development and operations teams, the rapidly developed software changes might be deployed without adequate security reviews, which can lead to software vulnerabilities.

Integrating security principles within the DevOps process may assist the organisation in achieving better quality software and stability.[2] Important security practices in DevOps are using effective automated security testing tools, security championship within the institution, and sufficient application security skills/proficiency in DevOps teams.[3] The AFM recommends that capital market institutions implement effective DevOps security procedures and processes.

1 AFM Principles for information security, https://www.afm.nl/en/professionals/nieuws/2019/dec/principes-informatiebeveiliging

2 Rahman, A. A. U. & Williams L. (2016), Software Security in DevOps: Synthesizing Practitioners Toolchain. *International Workshop on Continuous Software Evolution and Delivery*

3 Bird, J. (2018), Secure DevOps: Fact or Fiction?. *Research Paper of SANS*.

Observation 3: Management of IT outsourcing and supply chain risks is critical. IT availability and continuity risks remain widespread in capital market institutions.

89% of institutions in scope indicate that they use third party service providers for the provision of IT services. 36% of institutions in scope indicate that they use the cloud for important and/or critical services. 29% of institutions in scope indicate that they face a high exposure to IT outsourcing risks. Furthermore, half of institutions indicate that they face high inherent IT availability and continuity risks.

Outsourcing increases the dependency on third parties. Therefore, it is important to perform risk analyses before and during outsourcing, and to ensure that the maturity of outsourcing controls is adequate. ESMA has published Guidelines for outsourcing of critical and important functions to cloud service providers,[4] which investment firms and regulated markets should comply with. Furthermore, as discussed by the Dutch central bank (*De Nederlandsche Bank*, DNB) in its most recent information security monitor, published in December 2021, the creation of partnerships, unbundling of the value chain and outsourcing means that institutions' management of information security transcends the boundaries of their own organisation.[5] The AFM recommends incorporating information security management into cyber supply chain risk management practices (C-SCRM).[6] C-SCRM is a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. The importance of C-SCRM has been highlighted by the recent vulnerabilities in Log4J, VMware, Citrix and SolarWinds products. All recent incidents in relation to these vulnerabilities received a lot of media coverage.[7]

Adequate business continuity measures have proven to be important to recover from ransomware attacks.[8] Capital market institutions should react rapidly to ensure business operations can resume in a timely manner and to maintain availability of resources and information at a level acceptable for their institution in the event of a significant disruption. The AFM recommends that capital institutions develop and maintain a plan to respond to cyber incidents and quickly adapt to disruptions. In addition, business continuity measures based on Recovery Time Objectives (RTOs) and frequent testing of the business continuity measures are an important prerequisite to reduce the impact of IT incidents and to minimise business interruptions.

4 https://www.esma.europa.eu/press-news/esma-news/esma-publishes-cloud-outsourcing-guidelines
5 https://www.dnb.nl/media/xudmbbi2/web_135695_information-security-monitor-december-2021_eng.pdf
6 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (nist.gov)
7 Cybersecuritybeeld Nederland 2022, https://www.nctv.nl/binaries/nctv/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022/Cybersecuritybeeld+Nederland+2022.pdf
8 NCSC Ransomware incident response plan, https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2022/augustus/2/incident-response-plan-ransomware/Opmaak+Incident+response+plan_WEB2.pdf

Observation 4: Security Operations Centres (SOCs) or similar security teams are an important tool in dealing with increasing cyber threats.

79% of institutions in scope indicate that they have a Security Operations Centre. A successful cyberattack could have a material impact on the continuity of business operations and confidentiality, integrity or availability of data, information, and systems. Therefore, it is important to have processes and controls in place to prevent cyberattacks or to minimise their impact. In short, the establishment and effective operation of SOC teams contributes to controlled business operations.

A Security Operations Centre (SOC) is defined as the practice of defence against unauthorised activity within compute networks, including monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities. SOCs monitor computers and networks by collecting log information. Threat intelligence is used as input to analyse this log information. These activities enable organisations to identify activities of threat actors and take prompt action to mitigate potential threats. The AFM recommends that capital market institutions cooperate proactively in detecting and responding to IT and information security incidents in the chain of outsourced services and IT infrastructure. The institution can set up a SOC, or a similar security team, for this purpose. SOCs are an important tool in dealing with increasing cyber threats. Capital market institutions should consider best practices for conducting security operations, such as following the NIST cybersecurity framework

and MITRE[9] strategies for SOCs, quickly acknowledging an alert, reducing the time to remediate a detected adversary, and prioritising security investments in critical systems.

Observation 5: The IT architecture of capital market institutions is complex.

64% of institutions in scope indicate that their IT architecture is highly complex, with 29% indicating that their infrastructure has a medium degree of complexity. A high level of complexity could increase IT risks of an institution. The larger the institutions, the more complex it will be, requiring more people and technologies to operate. The risks of a cyberattack increase as information systems' interdependencies grow more and more complex.[10] High IT architecture complexity within the capital market institutions may result in inadequate level of operational resilience and inability to recover from a cyberattack or technology failure. Furthermore, adequate change and configuration management may be more challenging in organisations with a complex IT architecture. The AFM recommends that capital market institutions implement information security control measures in line with the complexity of their IT architecture.

Observation 6: Patch management and implementing critical security patches is fundamental.

Implementing patches is fundamental to ensuring the security of systems. Moreover, patch management is an important strategy in minimising cyber security incidents.

Once a patch is released by a vendor, the patch should be applied in a timeframe commensurate with an organisation's exposure to the security vulnerability and the level of cyber threat the organisation is aiming to protect themselves against. For example, once a security vulnerability in an internet-facing service is made public, it can be expected that malicious code will be developed by adversaries within 48 hours. In fact, there have been cases where adversaries developed malicious code within hours of the discovery of new security vulnerabilities.[11] For most systems, it is therefore important to install the patches as soon as possible.[12] Accordingly, the AFM recommends that capital market institutions put in place a patch management policy in line with their IT and business strategy and implement critical security patches in line with their risk appetite.

Observation 7: Clearly defined Recovery Time Objectives should be set for critical business processes.

Recovery Time Objectives (RTOs) refer to the time within which a system should be available again after its failure. Nearly all institutions in scope indicate that they have defined RTOs for their most critical business processes. The AFM recommends that the RTOs for the most critical business processes be clearly defined and in line with the organisation's risk appetite.

Pursuant to Article 15 of Commission Delegated Regulation (EU) 2017/584, trading venues must ensure that trading can resume within or close to two hours of a disruptive incident. In addition to regulatory requirements, RTOs and Recovery Point Objectives (RPOs) should be set on the basis of an assessment of the impact of an incident on business operations and the organisation's risk appetite. Defining RTOs and RPOs is an important step in business continuity management. Therefore, a lack of RTOs and RPOs may indicate blind spots in an organisation's risk management.

9 MITRE (2022), 11 Strategies of a World-class Cybersecurity Operations Center, https://www.mitre.org/sites/default/files/publications/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf
10 PwC 2022 Global Digital Trust Insights, https://www.pwc.com/us/en/assets/cyber-global-digital-trust-insights.pdf
11 PROTECT - Assessing Security Vulnerabilities and Applying Patches (October 2021).pdf (cyber.gov.au)
12 NCSC Guide to Cyber Security Measures, https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2021/august/4/guide-to-cyber-security-measures/210729+NCSC+Cyber+Security+Measures+EN+A4+RGB.pdf

Financial sector threat analysis

This section provides an overview of cyber threats faced by capital market institutions and the financial sector. This information is based on supervisory investigations, incident reports and dialogues with our national and international partners.

Social engineering

In cybersecurity, social engineering tricks users into opening files or emails, visiting websites or granting unauthorised persons access to systems or services. It always relies on a human element to be successful. This threat type mainly consists of vectors such as phishing and business email compromise. The AFM has observed that phishing is the most common vector for initial access.

Ransomware

In recent years, the AFM has seen an increase in the number of ransomware attacks on financial institutions. Ransomware has been one of the prime threats in 2022. These attacks sometimes brought the production of these organisations to a standstill, resulting in significant damage and losses. Threat actors are becoming more sophisticated and increasingly target medium-sized institutions, using public information to research potential victims before proceeding. What has changed in recent years is that ransomware is now a huge underground economy with many actors that specialise in specific parts of the ransomware chain, from developing malware to breaking into a network and compromising it, to laundering the illegally earned proceeds. This phenomenon is known as 'cybercrime-as-a-service'.

Supply chain threats

A supply chain attack targets the relationship between financial institutions and their suppliers. This threat comprises two types of attacks:[13] attacks through suppliers and attacks on third parties. An attack through a supplier specifically targets a supplier of a financial institution in order to ultimately target the institution itself. Attacks on third parties are attacks on financial institutions' suppliers but are not specifically targeted at the institutions themselves. Examples where a third-party supplier was used as an intermediary include the REvil attack on Kaseya, Apache Log4J, and Spring4shell incidents. The AFM has observed an increase in the number of supply chain threats.

DDoS

DDoS attacks are performed by exhausting the service and its resources or by overloading the components of the network infrastructure. While DDoS attacks are not a new threat, they are becoming more intensive, requiring vigilance and investments in the cyber resilience of capital market institutions and the financial sector. Furthermore, the increase in the intensity of DDoS attacks also increases the need to collaborate by sharing knowledge and combining technical capabilities. Consequently, public private partnerships and other information sharing associations play an important role in DDoS mitigation and cyber security in general. The AFM observes that DDoS attacks have had limited impact on the targeted financial institutions.

13 FI ISAC – One Financial Threat Landscape #NL2022

Outlook for supervision of cyber risks

Digitalisation and ongoing developments in information security and cybersecurity mean that capital market institutions need to consider their cyber resilience.

Preparations for supervision on the Digital Operational Resilience Act (DORA)

The DORA regulation is a new piece of European legislation that sets uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector, as well as critical third parties that provide them ICT (information and communications technology)-related services, such as cloud platforms and data analytics services. DORA provides a regulatory framework on digital operational resilience that requires all firms to ensure that they can withstand, respond to, and recover from all types of ICT-related disruptions and threats. These requirements are uniform across all EU member states. The core aim is to prevent and mitigate cyber threats.

The entry into force of DORA will broaden the AFM's mandate for supervision on business operations and IT. Together with our national and international partners, the AFM will spend the next two years preparing for DORA supervision by strengthening our information position regarding the information security and operational risk management of financial institutions under our remit, develop new supervisory methodologies, and actively reach out to institutions to exchange information on cyber threats, risks and best practices.

Sources

Capital market institutions information security foundation self-assessment 2022

The AFM has been investigating the control of information security and cyber security within the Dutch financial sector for several years. We do this based on, among other things, periodic self-assessments of the institutions under our supervision. The AFM's information security foundation self-assessment is based on the information security foundation self-assessment drawn up by the Dutch central bank (DNB) for the institutions under its supervision as part of DNB's Good Practice for information security[14] and the related Information Security QA updated in 2019. As part of supervisory convergence and the increased importance of information security, the AFM has, in close cooperation with DNB, included the information security foundation self-assessment in its supervisory toolkit for the first time this year.

14 DNB's Good Practice for information security: https://www.dnb.nl/media/yffn1wji/good-practice-ib-2019-2020.pdf

Disclaimer

The observations and trends found in this information security monitor are mainly based on a self-assessment pilot for fourteen capital market institutions. Therefore, when reading this report, it is important to consider the nature of a self-assessment, the fact that no comparisons can be made with previous years, and that the institutions in scope may not be representative of the capital market sector.

This information security monitor contains various examples and observations. Observations give rise to recommendations for the application of the legislation in the area of controlled and sound business operations. A recommendation highlighted in an observation provides insight into the behaviour we have observed or expect to see in institutions' policy practice, is indicative and does not preclude institutions from applying the underlying rules in a different way, or stricter, where necessary. It is up to the institutions to make these considerations concerning the application of our recommendations.

Any questions or comments about this publication?

Send an email to: redactie@afm.nl

The Dutch Authority for the Financial Markets
PO Box 11723 | 1001 GS Amsterdam

Telephone
+31 20 797 2000

www.afm.nl

Data classification
AFM - Publiek

Follow us:

The AFM is committed to promoting fair and transparent financial markets.

As an independent market conduct authority, we contribute to a sustainable financial system and prosperity in the Netherlands.