ASSET MANAGEMENT SUPERVISION DIVISION

Industry Letter 10 March 2020

Thematic Inspection of Cybersecurity Risk Management in Asset Management Firms

The Central Bank of Ireland (Central Bank) recently undertook a Thematic Inspection of Cybersecurity Risk Management (Thematic Inspection) in Investment Firms and Fund Service Providers (Asset Management Firms). The purpose of the inspection was to determine the adequacy of cybersecurity controls and cybersecurity risk management practices of the inspected firms and to identify good practices.

The Thematic Inspection examined (i) cybersecurity risk governance, (ii) cybersecurity risk management frameworks and (iii) certain technical controls for mitigating cybersecurity risk. The on-site inspections included a point-in-time maturity assessment of key cybersecurity risk management practices in place across the selected firms.

The risks associated with IT and cybersecurity are key concerns for the Central Bank. The Central Bank's 'Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks 2016' (2016 Cross Industry Guidance) highlights that "*firms are expected to have adequate processes in place to effectively address cyber risk. While it is recognised that there is no one size fits all solution to addressing this risk, all firms should understand the strategic implications of cyber risk. The cyber risk management elements of the IT risk management framework, including associated policies and procedures, should not be viewed as static. Firms should review and update the framework regularly to reflect threat intelligence and changes in the internal and external operational environment*".

Purpose of this Letter

This letter details the key findings identified during the Thematic Inspection. The Central Bank expects Asset Management Firms to fully consider these findings and evaluate their own cybersecurity risk management practices to establish if any improvements are required. The Key Findings, with associated Central Bank expectations, are outlined in Appendix 1.

The details / findings set out in this letter are not exhaustive and firms should, at all times be evaluating their own risks related to cybersecurity. This letter is required to be brought to the attention of all Board members and Senior Management before 30 April 2020. Please note that a review of cybersecurity risk management and the issues raised in this letter may form part of any future risk assessments, including inspections, carried out by the Central Bank. In this respect, supervisors will have regard to the consideration given by a firm to the matters raised in this letter. Supervisors will discuss with the firm matters raised in this letter during future supervisory engagement meetings.

Summary of Key Findings

It is noted that whilst some firms have made good progress in certain areas, many of the weaknesses highlighted in the Central Bank's 2016 Cross Industry Guidance are still prevalent three years later. Consequently, concerns still exist for the Central Bank regarding the arrangements that are in place to adequately oversee all cybersecurity risks.

It is the responsibility of the Board and Senior Management to ensure that cybersecurity is embedded in their firm; this should be achieved through a combination of raising awareness, building resilience and enhancing capabilities. The Board has responsibility for overseeing a clearly defined strategy for cybersecurity to enable the firm to achieve a desired state of resilience and protection. There should be a sufficient skill set on the Board to challenge and oversee the strategy. This skill set and knowledge should be built upon and refreshed regularly to enable the Board to understand the evolving nature of the threat and the implications for the business. The Board and Senior Management should prioritise the development of a strong organisational culture of cybersecurity. This is key in supporting effective identification, monitoring, reporting and mitigation of cyber risks. However, many firms failed to demonstrate sufficient focus on the development of a culture of cybersecurity during the Inspection.

Preparedness for a cybersecurity incident is crucial to enhancing resilience to an attack or event. However, weaknesses were identified in firms' vulnerability identification and management processes. Furthermore, cybersecurity incident response and recovery plans did not meet the Central Bank's expectations, with many being in draft form, incomplete or not tested with an appropriate frequency. Deficiencies in IT asset inventories were identified, where the inventories did not capture the complete IT estate and / or classify assets by their business criticality. While all firms reported on cybersecurity risks, the quality and frequency of the reporting was variable. In general, risk indicators used were overly focused on qualitative indicators with insufficient utilisation of quantitative indicators. Robust risk reporting, including to the Board, is a critical tool to support effective assessment of a firm's cybersecurity risk exposure.

The Inspection identified that some firms have made good progress in strengthening their cyber risk resilience through enhancements in areas such as security incident management and IT asset inventories. It was also found that many firms have aligned their risk management approach with that of internationally adopted frameworks for IT and cybersecurity Risk Management. Furthermore, it is noted that the proliferation of dedicated IT and cyber risk personnel in firms is a positive indication that cyber risk is increasingly a consideration in business-as-usual operations.

However, cybersecurity is a practice that remains underdeveloped in the Asset Management industry. Firms must give more consideration and support to identifying and managing the different threats they are exposed to, whilst recognising that the inherent risks of IT are continuously increasing. Firms must focus on increasing the maturity of their cybersecurity model by driving a process of continuous improvement.

APPENDIX 1: KEY FINDINGS

1. Cybersecurity Risk Governance

Boards and Senior Management are not prioritising to a sufficient extent the need to have a robust cybersecurity culture. A strong cybersecurity culture will support effective identification, monitoring, reporting and mitigation of cybersecurity risks. Cybersecurity risks, in particular the risk of business disruption and reputational damage in the event of an incident / breach, are not given adequate, or in some cases any, consideration when developing the business strategy. It is the responsibility of the Board and Senior Management to determine, oversee and implement a clear strategy for cybersecurity to enable the firm to achieve a desired state of resilience and protection. Cybersecurity strategies require improvement to ensure they are sufficiently comprehensive, contain adequate detail and communicate a clear intent.

Deficiencies were identified in the governance of cybersecurity policies. Specific findings included a lack of tailoring of Group policies to the firm's business operations as well as a failure to review policies in accordance with the frequency mandated in firms' own policy management criteria. Deficiencies were also identified in firms' oversight of Group or third party cybersecurity service providers.

Central Bank Expectations

Firms should have a comprehensive, documented and Board-approved IT and cybersecurity strategy, supported by sufficient resources and aligned with the overall business strategy. Firms' Senior Management should ensure that there is a well-defined and comprehensive IT and cybersecurity risk management framework in place that provides effective oversight of IT related risks and gives assurance to the Board regarding the management of these risks within the firm.

2. Cybersecurity Risk Management

Firms were found to make limited, and in some cases no use of defined quantitative metrics in Management Information for monitoring, reporting on and measuring cybersecurity risk exposures against the approved risk appetite statement (RAS). Inadequate risk indicators impede the ability of the Board and Senior Management to effectively assess the firm's cybersecurity risk exposure and whether the firm's risk appetite or thresholds are being breached. Boards, in general, do not receive sufficient reporting on cybersecurity and other technology risks, for example, regarding trends in a firm's level of security risk incidents / near misses. Conflicting reporting lines were also observed in some instances regarding cybersecurity risk personnel, where they reported to senior first line of defence (1LOD) positions, resulting in a lack of independent challenge on cybersecurity risk.

Central Bank Expectations

Firms should implement, maintain and communicate an appropriate cybersecurity risk management framework that includes risk identification, assessment and monitoring, the design and implementation of risk mitigation and recovery strategies, and testing for effectiveness. Cybersecurity risk assessments should be conducted at regular intervals, at least annually, and should be comprehensive, considering internal and

external sources of risk. Assessments should have appropriate parameters for evaluating and prioritising risk, such as risk likelihood and potential impact on the business operations of the firm.

3. IT Asset Inventories

Firms were unable to demonstrate that there was a single, complete IT asset inventory solution in place. IT assets are not being managed, from a security perspective, in accordance with their business criticality. The lack of a comprehensive asset inventory impedes a firm's ability to effectively manage cybersecurity risks, as a clear understanding of the complete IT asset estate is required to both secure the environment and respond to a cybersecurity threat. As a result, firms are not fully aware of all the hardware, software, and data assets on their networks and therefore cannot assess the associated risks in a holistic manner.

Central Bank Expectations

A thorough inventory of IT assets, classified by business criticality, should be established and maintained to support an effective IT Risk Management framework. A process (for example, a business impact analysis) should also be in place to regularly assess the business criticality of IT assets and assess the associated risks in a holistic manner. Configuration baselines for IT assets should be established, with divergence from the baselines identified and managed appropriately.

4. Vulnerability Management

The following deficiencies were identified in firms' vulnerability management processes:

- Inadequate vulnerability management planning and mitigation activities;
- Frequently, either incomplete or unknown coverage of vulnerability scans;
- In some cases, failure to use vulnerability scanning tools to identify devices that deviate from the security baseline.

Devices that are exposed to a high number of known vulnerabilities for a lengthy period of time are more vulnerable to malicious actors who may gain unauthorised access to IT assets and compromise the confidentiality, integrity and availability of stored business critical data.

Central Bank Expectations

Exposure to vulnerabilities should be assessed on a continuous basis, on the entirety of the IT estate, and include identification of external and internal vulnerabilities. Robust safeguards should be in place, including a proactive patch management process and a comprehensive configuration hardening activity, to protect against cybersecurity threats.

5. Security Event Monitoring

Firms were unable to demonstrate that security events from all pertinent systems and devices are collected by and analysed in the Security Information and Event Management system (SIEM). Firms did not evidence sufficient oversight for outsourced Security Operations Center (SOC) services. For example, in some cases, there was an absence of formal agreements for SOC services, no performance reporting, no documented guidance for security analysts or no consideration for chain outsourcing.

Inadequate coverage of monitored devices, used for hosting or accessing critical data, will impede firms' ability to effectively identify security events and handle confirmed incidents in a consistent and timely manner. Furthermore, inadequate oversight of SOC services renders the firm unable to determine whether the service being provided is appropriate and aligned with the firm's business needs.

Central Bank Expectations

Cybersecurity management activities should address the timely detection of security events and incidents, ensure comprehensive monitoring of all assets containing or processing critical data, and assess the potential impact to the business. Additionally, regular reviews should take place to assess the effectiveness of detection processes and procedures.

6. Security Incident Management

Cybersecurity incident response and recovery plans were observed as incomplete and / or not actionable. Issues identified included plans that were in draft, were not complete, had not considered key scenarios or were not part of a formal incident management framework. Furthermore, in some cases, it was identified that cybersecurity incident response and recovery plans were not tested. The lack of an effective cybersecurity incident management framework will impair a firm's ability to respond, contain and recover from cybersecurity attacks in a timely and organised manner. The absence of a regular suitability assessment of the framework, performance of response plan tests, and reporting of such to Senior Management could result in uncertainty on whether additional resources or skill sets are required to prepare for and respond to a cybersecurity incident.

Central Bank Expectations

Firms should have documented cybersecurity incident response and recovery plans in place that provide a roadmap for the actions the firm will take during and after a security incident. Incident response plans should address, inter-alia, roles and responsibilities of staff, incident detection and assessment, reporting and escalation, as well as response and recovery strategies to be deployed. Communication with relevant external stakeholders, including customers and the Central Bank, should also form a part of the response plan.

***