ASSET MANAGEMENT AND INVESTMENT FUNDS

Cybersecurity Management: Central Bank Outlines its Expectations for Firms

March 2020

The Central Bank issued an industry letter following its thematic inspection of asset management firms, which included investment firms and fund service providers, to determine the adequacy of cybersecurity risk management, controls and practices.

The letter details the Central Bank's findings and expectations and all firms should review these findings and, where necessary, take steps to remediate any identified issues or weaknesses in their cybersecurity risk management practices. The industry letter must be brought to the attention of boards and senior management before 30 April 2020.

The Central Bank's Findings

The Central Bank's thematic inspection covered: cybersecurity risk governance; cybersecurity risk management frameworks; and certain technical controls for mitigating cybersecurity risk. The Central Bank notes that while some good progress has been made in certain areas, many of the weaknesses highlighted in the Central Bank's 2016 Cross Industry Guidance on IT and cybersecurity risks still prevail. The Central Bank has concerns about whether the arrangements that are in place in firms to oversee all cybersecurity risks are adequate. Some of the key issues and the Central Bank's expectations for firms are set out below:

Cybersecurity Risk Governance

Identified Issues: A robust cybersecurity culture should inform the effective identification, monitoring, reporting and mitigation of cybersecurity risks. The Central Bank found that boards and senior management are not sufficiently prioritising the need to have a strong cybersecurity culture embedded throughout the organisation. The Central Bank noted that in some instances the risk of business disruption and reputational damage arising from a cybersecurity incident were not adequately considered and in other cases had not been considered at all. The Central Bank also identified specific deficiencies in cybersecurity policies, including:

- group policies not being specifically tailored to the firm's own business operations; and
- failure to review policies in line with internally specified frequencies.

Recommendations: Boards and senior management are reminded that it is their responsibility to ensure that cybersecurity risk management is embedded in a firm's culture. This should be achieved through a combination of:

- raising awareness;
- building resilience; and
- enhancing capabilities.

Cybersecurity strategies should be improved to ensure that they are sufficiently clear in their intent, comprehensive and adequately detailed. A board has responsibility for overseeing the cybersecurity strategy and there should be a sufficient skillset on the board to oversee the strategy and to challenge it. Additionally, a well-defined and comprehensive IT and cybersecurity risk management framework should be

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.

Cybersecurity Risk Management

Identified Issues: Inadequate risk indicators impede the ability to adequately assess cybersecurity risk exposures and to consider whether the risk appetite or thresholds are being breached. The Central Bank found that risk indicators used were often overly focused on qualitative indicators and not quantitative indicators. The Central Bank also found deficiencies in the quality and frequency of reporting to the board.

Recommendations: The Central Bank expects firms to implement, maintain and communicate an appropriate risk management framework that includes the identification, assessment and monitoring of cybersecurity risk, and the design and implementation of risk mitigation and recovery strategies and testing for effectiveness. Cybersecurity risk assessments should be conducted regularly and at least annually. These assessments should be comprehensive and take account of both internal and external risks.

Security Incident Management

Identified Issues: Cybersecurity incident response and recovery plans did not meet the Central Bank's expectations, with many being in draft form, incomplete and/or not tested with an appropriate frequency.

Recommendations: Firms should have documented cybersecurity incident response and recovery plans in place detailing the actions the firms will take during and after a security incident. Incident response plans should include, 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.

Security Event Monitoring

Identified Issues: The review found that firms did not evidence sufficient oversight for outsourced security operations centre ("SOC") services, with the Central Bank noting that in some cases, there were no formal agreements for SOC services, no performance reporting, no documented guidance for security analysts or no consideration for chain outsourcing. Firms were unable to demonstrate analysis being done on security events.

Recommendations: The Central Bank expects firms to have in place arrangements that detect cybersecurity security events and incidents. Further, there should be regular reviews to assess the effectiveness of detection processes and procedures.

IT Asset inventories

Identified Issues: The Central Bank identified deficiencies in firms identifying their IT assets, such as hardware, software and data assets, on their networks and / or classifying assets by their business criticality.

Recommendations: Firms should establish and maintain a thorough inventory of their IT assets, classified by business criticality and a process should be put in place to regularly assess the business criticality of IT assets.

Vulnerability Management

Identified Issues: The Central Bank identified weaknesses in firms' vulnerability identification and management processes. These included: inadequate vulnerability management planning and mitigation activities; either incomplete or unknown coverage of vulnerability scans; and in some instances failure to use vulnerability scanning tools to ensure devices are checked for vulnerabilities.

Recommendations: The Central Bank expects exposure to vulnerabilities on devices to be continually assessed and should include the identification of both internal and external vulnerabilities. Robust safeguards should be in place to protect against exposure to vulnerabilities, noting in particular that devices exposed to a higher number of vulnerabilities for a lengthy time are more vulnerable to those wishing to gain unauthorised access.

What do these findings mean for fund management companies?

Fund management companies should consider these findings and evaluate their own cybersecurity risk management practices and in particular should ensure that:

- the Central Bank's letter is sent to the board and senior management by 30 April 2020;
- the Central Bank's letter is considered and discussed at the next board meeting; and
- given the delegated model that Irish funds adopt, seek assurances from their service providers about their management of cybersecurity risks and in particular what actions have been undertaken by the service providers to ensure that their arrangements comply with the Central Bank's expectations as outlined in the letter. Fund management companies should also seek additional reporting from the service providers to address these requirements on an ongoing basis.

If you would like to discuss the foregoing, or require any assistance in assessing your requirements please do not hesitate to contact a member of our team.

KEY CONTACTS

Kevin Murphy
Partner
+353 1 920 1177
kevin.murphy@arthurcox.com

Tara O'Reilly
Partner
+353 1 920 1787
tara.oreilly@arthurcox.com

Sarah Cunniff
Partner
+353 1 920 1171
sarah.cunniff@arthurcox.com

Dara Harrington
Partner
+353 1 920 1206
dara.harrington@arthurcox.com

Cormac Commins
Partner
+353 1 920 1786
cormac.commins@arthurcox.com

Ian Dillon
Partner
+353 1 920 1788
ian.dillon@arthurcox.com

Siobhán McBean
Partner
+353 1 920 1052
siobhan.mcbean@arthurcox.com