WILLIAM FRY

Asset Management & Investment Funds

April 2020

Central Bank publishes findings from thematic on cybersecurity risk management

On 10 March 2020, the Central Bank published findings, along with associated expectations, from its thematic inspection into the cybersecurity risk management practices of Irish authorised investment firms and fund service providers. The thematic involved on-site inspections of a selection of firms' (i) cybersecurity risk governance, (ii) cybersecurity risk management frameworks and (iii) certain technical controls for mitigating cybersecurity risk.

Thematic Inspection Findings

While acknowledging the progress made by certain firms in *"strengthening their cyber risk resilience through enhancements in areas such as security incident management and IT asset inventories"*, the Central Bank highlighted several concerns in the practices and controls used by firms for the identification, oversight, governance and management of cybersecurity risk. Referencing the publication of its 2016 Cross Industry Guidance on IT and cybersecurity risks, the Central Bank noted that many of the weaknesses identified at that time continue to exist, which it considers as evidence of an *"underdeveloped"* practice of cybersecurity in the asset management industry.

In its thematic inspection findings, the Central Bank sets down its expectations for firms' management of cybersecurity risk, along with the poor practices it identified during its on-site inspections:

Regulatory Expectations	Poor Firm Practices Identified by Central Bank
Cybersecurity Risk Governance Boards should document and adopt an IT & Cybersecurity Strategy that: • is comprehensive, detailed and communicates clear intent; • is supported by sufficient resources; • is aligned with overall business strategy; • provides for effective oversight of IT related risks applicable to the business of the firm; and • gives assurance to the Board regarding the management of IT related risks.	Insufficient prioritisation by Boards and Senior Management of robust cybersecurity culture that supports effective identification, monitoring, reporting and mitigation of cybersecurity risks. — Inadequate focus on cybersecurity risks in business strategy development, in particular the risk of business disruption and reputational damage in the event of an incident / breach. —

Regulatory Expectations	Poor Firm Practices Identified by Central Bank
Boards should have a sufficient skill set to challenge and oversee the IT & Cybersecurity Strategy: • a Board's skill set & knowledge should be built upon and refreshed regularly to enable it to understand the evolving nature of the threat and the implications for the firm's business.	Deficient governance of cybersecurity policies e.g. lack of tailoring of Group policies to the firm's business operations and a failure to review policies in accordance with the frequency mandated in firms' own policy management criteria. — Lack of oversight of Group or third-party cybersecurity providers.
Cybersecurity Risk Management Firms should implement, maintain and communicate an appropriate risk management framework that: • includes vulnerability & risk identification, assessment and monitoring; • includes the design and implementation of risk mitigation and recovery strategies; and • provides for effectiveness testing; • provides for regular (at least annual) assessment of internal external risk sources; • provides for appropriate parameters for evaluating and prioritising risk such as likelihood and potential impact on the business operations of the firm.	Overreliance on qualitative, with limited/no use of quantitative risk indicators, in management information for monitoring, reporting on and measuring cybersecurity risk exposures against the approved risk appetite statement (RAS). — Insufficient Board reporting on cybersecurity and other technology risks e.g. regarding trends in a firm's level of security risk incidents / near misses. — Conflicting reporting lines for cybersecurity risk personnel e.g. reports issuing to senior first line of defence (1LOD) positions, resulting in a lack of independent challenge on cybersecurity risk. — Incident response & recovery plans in draft form, incomplete or not tested with appropriate frequency.
IT Asset Inventories Firms should establish and maintain a thorough inventory of IT assets which: • supports effective IT risk management framework; • is classified by business criticality; • incorporates a process e.g. business impact analysis, to regularly assess the business criticality of IT assets and assess the associated risks in a holistic manner; and • establishes configuration baselines for IT assets, divergence from which should be managed appropriately.	No single, complete IT asset inventory solutions in place. — IT assets not being managed, from a security perspective, in line with business criticality. — Risk assessments impeded by lack of awareness of all hardware, software, and data assets on networks.

Regulatory Expectations	Poor Firm Practices Identified by Central Bank
Vulnerability Management Firms should have in place processes for: • continuously assessing, on the entirety of the IT estate, exposure to vulnerabilities, both internal and external; • ensuring robust safeguards, including proactive patch management process and a comprehensive configuration hardening activity, to protect against cybersecurity threats; • monitoring devices to protect against malicious actors who may gain unauthorised access to IT assets and compromise the confidentiality, integrity and availability of stored business critical data.	Inadequate vulnerability management planning and mitigation activities. — Incomplete or unknown coverage of vulnerability scans. — Failure to use vulnerability scanning tools to identify devices that deviate from security baseline.
Security Event Monitoring Firms' cybersecurity management activities should: • address the timely detection of security events and incidents; • ensure comprehensive monitoring of all assets containing or processing critical data; • assess the potential impact to the firm's business; and • incorporate regular reviews to assess the effectiveness of detection processes and procedures.	Failure by Security Information and Event Management system (SIEM) to collect and analyse security events from all pertinent systems and devices. — Insufficient oversight for outsourced Security Operations Centre (SOC) services. — Absence of formal SOC service agreements resulting in 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 impeding firms' ability to effectively identify security events and confirmed incidents.
Security Incident Management Firms should have in place a documented cybersecurity incident response & recovery plan that: • provides an actions roadmap during and after a security incident; • addresses staff roles and responsibilities; • provides for incident detection and assessment; • provides for reporting and escalation; and • provides for deployment of response and recovery strategies including communication with relevant external stakeholders e.g. customers and Central Bank.	Incomplete/unactionable/untested cybersecurity incident response & recovery plans. — No formal incident management framework. — Absence of regular framework suitability assessments.

Next Steps

The Central Bank requires the above findings to be brought to the attention of Board Members and Senior Management by 30 April 2020 and confirms that "a review of cybersecurity risk management and the issues raised [ ] may form part of any future risk assessments, including inspections, carried out by the Central Bank", during which "supervisors will have regard to the consideration given by a firm to the matters raised".

For more information, please contact the below or your usual William Fry contact.

Patricia Taylor
PARTNER
+353 1 639 5222
patricia.taylor@williamfry.com

James Phelan
PARTNER
+353 1 489 6590
james.phelan@williamfry.com