A&L Goodbody

Cybersecurity: *CBI expectations for funds and fund service providers*

The Central Bank of Ireland (**CBI**) issued a letter to industry on 10 March 2020 following a thematic inspection of cybersecurity risk management.

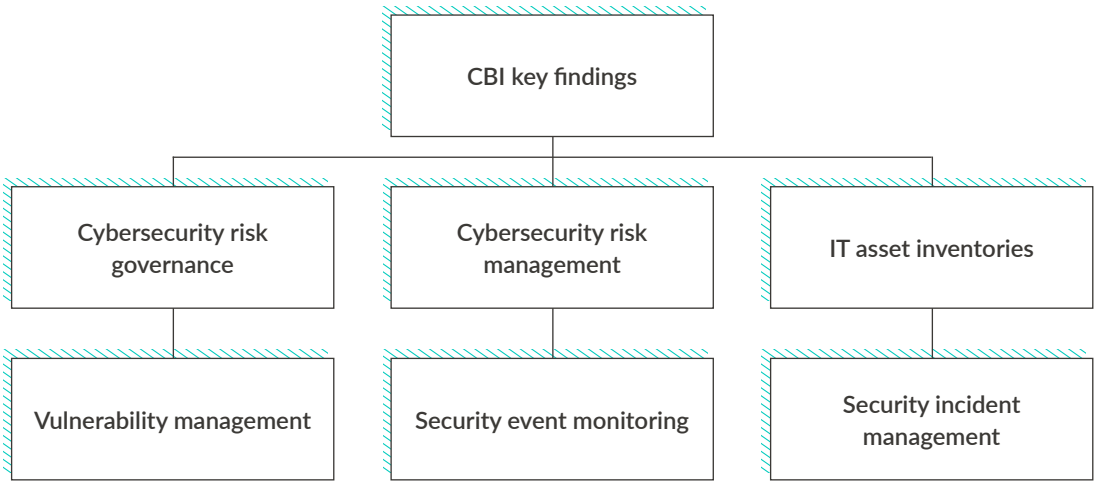
The letter is addressed to investment firms and fund service providers. Self-managed or internally-managed funds are in scope and should review the letter proportionally, taking account of nature, scale and complexity and of their delegated business model.

Fund service providers have been expected to apply the findings of the CBI's industry letter in an environment which changed quickly and significantly from when the themed inspection was carried out.

At the height of the business disruption caused by COVID-19, most funds industry workers switched to a remote working environment and many continue to work from home. The nature and scale of cybersecurity risks changed. The initial focus was on business continuity. Having come through that initial phase, arguably now is a good time to take stock and take a renewed look at the CBI findings and expectations.

Summary

- Boards and senior management are ultimately responsible for ensuring that cybersecurity is embedded in the firm
- CBI required the letter to be brought to the attention of all board members by 30 April 2020
- Six key findings
- Heightened prospect of cybersecurity threat with increased remote working during pandemic
- Sufficient skill set on the Board to challenge and oversee the cybersecurity strategy



CBI expectations

The CBI set out its key findings under each of the six headings in the industry letter together with CBI expectations for each. These are takeaways from the CBI expectations.

Cybersecurity risk governance

Firms' IT and cybersecurity strategy should be Board approved. Senior management should ensure that the IT and cybersecurity risk management framework enables effective oversight of IT risks and gives assurance to the Board of the management of these risks.

Cybersecurity risk management

The cybersecurity risk management framework should include 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.

IT asset inventories

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 should also be in place to regularly assess the business criticality of IT assets and assess the associated risks. Configuration baselines for IT assets should be established.

Vulnerability management

Exposure to vulnerabilities should be assessed on a continuous basis and include identification of external and internal vulnerabilities. Robust safeguards should be in place to protect against cybersecurity threats.

Security event monitoring

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. Regular reviews should take place to assess the effectiveness of detection processes and procedures.

Security incident management

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. The content of incident response plans should include roles and responsibilities of staff, incident detection and assessment, reporting and escalation, response and recovery strategies to be deployed. Communication with relevant external stakeholders, such as customers and the CBI should be addressed.

Recent CBI commentary

In a CBI enforcement action notice published on 28 July 2020 concerning regulatory breaches which involved a cyber-fraud incident, the CBI's Director of Enforcement said *"This case should serve to highlight to all firms the importance of ongoing vigilance in the area of cyber security. The Central Bank expects all firms to consider, identify and manage operational and cyber risks and ensure that their staff receive appropriate training tailored to the risks associated with their duties and responsibilities."* The CBI also commented on its expectations around communication and reporting of security incidents.

Proposed Chief Information Officer role

The CBI is of the view that due to the advancement of information technology and its impact on the way business is conducted in the financial services industry, it is appropriate to introduce a new PCF-49 role of Chief Information Officer for regulated financial service providers (**RFSP**). This underlines the general CBI focus on the impact of information technology in the sector, but the PCF-49 role will not apply to funds as they are ranked as low impact by the CBI under PRISM. It is unlikely to apply either to fund management companies. The CBI expects that a Chief Information Officer role will apply to the most senior individual with responsibility for IT matters at firms that have a PRISM impact rating of high or medium high and/or where information technology is a key enabler or core element of the RFSP's business model.

Practical considerations for funds

Funds' and fund management companies' cybersecurity controls and risk management practices should ensure security of information throughout a fund's organisational and operational structure. The approach should take into account the structure of the fund, for example whether it is internally managed or externally managed. It should address the cybersecurity processes of

its service providers and delegates, directors and professional advisers. Where a service provider or delegate is a CBI authorised RSFP, it can reasonably be expected to demonstrate that it is conforming to the CBI standards.

The industry letter states that 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.

Directors of funds and fund management companies will need to ensure that the board can satisfy this expectation and demonstrate how it is continually satisfied.

Key takeaways

- Boards should be familiar with the content of the industry letter.
- A gap analysis against current policies and procedures may be advisable. Cybersecurity strategies of service providers will be relevant.
- An assessment should take place as to whether the board composition has the required skillset to oversee and challenge the cybersecurity strategy.
- The CBI will be following up with individual firms to ensure that they are taking steps to enhance their cybersecurity resilience and to minimise the risk to themselves and to the wider industry from a cyber-attack.
- Firms should be prepared to engage with CBI supervisors on the industry letter during future supervisory engagement meetings.

The Commercial & Technology team at A&L Goodbody has an international cross-disciplinary data security team which provides practical and creative advice to organisations tackling cybersecurity, and other data security, issues.

You can contact any member of the ALG Asset Management & Investment Funds team for further information.

Our team

Brian McDermott
Partner and Head of Asset Management & Investment Funds
+353 1 649 2307
bmcdermott@algoodbody.com

Michael Barr
Partner
+353 1 649 2327
mbarr@algoodbody.com

Stephen Carson
Partner
+44 20 7382 0820
scarson@algoodbody.com

Mary McKenna
Partner
+353 1 649 2344
mmckenna@algoodbody.com

Kerill O'Shaughnessy
Partner
+353 1 649 2422
koshaughnessy@algoodbody.com

Laura Butler
Partner
+353 1 649 2209
lbutler@algoodbody.com

Nollaig Greene
Associate & Knowledge Lawyer
+353 1 649 2359
ngreene@algoodbody.com

Ann Shiels
Associate & Knowledge Lawyer
+353 1 649 2396
ashiels@algoodbody.com