March 2020

Central Bank of Ireland issues Industry Letter on the Thematic Inspection of Cybersecurity Risk Management in Asset Management Firms

The Central Bank of Ireland (the "**CBI**") published on the 10 March, 2020 a letter to industry on the key findings of their recent thematic inspection (the "**Thematic Inspection**") of cybersecurity risk management in Asset Management Firms (the "**Industry Letter**").

The CBI expects Asset Management Firms to fully consider the findings and evaluate their own cybersecurity risk management practices to establish if any improvements are required.

As per other "Dear CEO letters", the CBI notes that it will have regard to the contents of the Industry Letter when conducting any future risk assessments and will discuss the matters raised in the Industry Letter during any future supervisory engagement meetings.

The Asset Management Firms

The Thematic Inspection carried out by the CBI was in respect of Investment Firms and Fund Service Providers (the "**Asset Management Firms**").

As a result, these firms should consider the Industry Letter as recommended by the CBI.

Key findings and CBI expectations

In the Industry Letter, the CBI highlighted the key findings on the Thematic Inspection as well as their expectations going forward for Asset Management Firms. The CBI has acknowledged in the Industry Letter and subsequently in Michael Hodson's speech on 10 March, 2020, that some Asset Management Firms have made good

For further information on any of the issues discussed in this article please contact:

Emmet Quish
DD:+ 353 (0)1 673 1724
emmet.quish@dilloneustace.ie

Hannah Fenlon
DD: + 353 (0)1 674 1005
hannah.fenlon@dilloneustace.ie

progress in certain areas. However, many of the weaknesses highlighted in the CBI's 2016 Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks are still prevalent three years later.

The Industry Letter reminds Asset Management Firms that the responsibility to ensure that cybersecurity is embedded in their firms lies with the Board and Senior Management.

A summary of the CBI's non-exhaustive key findings and expectations are as follows:

Cybersecurity Risk Governance

Findings: Boards and Senior Management are not prioritising to a sufficient extent the need to have a robust cybersecurity culture. Cybersecurity risks are not given adequate or in some cases any consideration when developing the business strategy. There was also a lack of tailoring of group policies to the relevant firm's business operations and a failure to review policies in accordance with the frequency mandated in the firm's own policy.

Expectations: Asset Management Firms should have a "comprehensive, documented and Board-approved IT and cybersecurity strategy". There should also be a well-defined and comprehensive IT and cybersecurity risk management framework in place that is appropriate to the business.

Cybersecurity Risk Management

Findings: Asset Management Firms had 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 statements. Boards are not receiving sufficient reporting on cybersecurity and other technology risks and there are conflicting reporting lines regarding cybersecurity risk personnel resulting in a lack of independent challenge on cybersecurity risk.

Expectations: The cybersecurity risk management framework should ensure related risks are identified, assessed and monitored. Risk mitigation and recovery strategies should be designed and implemented and tested for effectiveness. Risk assessments should be conducted at "regular intervals" (at least annually).

Information Technology ("IT") Asset Inventories

Findings: Asset Management Firms were unable to demonstrate that there was a single, complete IT asset inventory solution in place and IT assets were found not to be managed, from a security perspective, in accordance with their business criticality.

Expectations: Asset Management Firms must conduct and maintain a thorough inventory of IT assets. The business criticality of IT assets should be assessed regularly.

Vulnerability Management

Findings: Asset Management Firms had inadequate vulnerability management planning and mitigation activities. There was either incomplete or unknown coverage of vulnerability scans and in

some cases, failures to use vulnerability scanning tools to identify devices that deviate from the security base line.

Expectations: Vulnerabilities should be assessed on a continued basis and Asset Management Firms should identify both external and internal vulnerabilities and appropriate robust safeguards should be put in place.

Security Event Monitoring

Findings: Asset Management Firms were unable to demonstrate that security events from all pertinent systems and devices are collected by and analysed in the relevant security information and event management system. There was no evidence of sufficient oversight of outsourced security operations center ("**SOC**") services. 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.

Expectations: Security events and incidents should be detected on a timely basis and Asset Management Firms should ensure that all assets containing or processing critical data are monitored. The potential impact on the business of security events and incidents should be assessed. The processes and procedures in place for detecting security events should be regularly reviewed.

Security Incident Management

Findings: Cybersecurity incident response and recovery plans were in some cases incomplete and/or not actionable. Cybersecurity incident response and recovery plans that were in draft were not complete, had not considered key scenarios or were not part of a formal incident management framework and in some cases cybersecurity incident response and recovery plans were not tested.

Expectations: Asset Management Firms should have a documented cybersecurity incident response and recovery plan in place outlining what actions will be taken during and after a security incident, including roles and responsibilities of key staff, reporting and escalation and response and recovery strategies to be deployed and communication with external stakeholders (including the CBI).

Impact of the Industry Letter

The Industry Letter must be brought to the attention of all Board Members and Senior Management by 30 April, 2020 where the findings are to be considered and, if necessary, improvements should be made to cybersecurity risk management practices. In tandem with this, Michael Hodson referenced in his speech that 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.

This is a timely Industry Letter given the CBI's recent Notice to firms in respect of the new Chief Information Officer pre-approval control function (PCF-49). Asset Management Firms should review the Notice in tandem with the Industry Letter and the impact that the Industry Letter may have in

further shaping the new PCF-49 role. Please see out recent article on this Notice for further information.

As mentioned above, the CBI reminded Asset Management Firms that it is the responsibility of the Board and Senior Management to ensure that cybersecurity is embedded within the compliance culture of the Asset Management Firm. As part of this, the CBI set out in the Industry Letter that there should be a sufficient skill set on the Board to challenge and oversee the cybersecurity strategy. This could lead to (i) additional or replacement directors being appointed to Asset Management Firms with a background and expertise in cybersecurity and IT and (ii) regular Board level training on cybersecurity and IT risk management, given that the CBI also expects skill sets and knowledge at Board level to be built upon and refreshed regularly to ensure the Board understands the evolving nature of the threat and the implications for the Asset Management Firm's business.

Asset Management Firms should be prepared to engage with CBI supervisors on the Industry Letter during future supervisory engagement meetings.

If you have any queries in respect of the issues raised in this article, please do not hesitate to contact us.

Dillon Eustace
March 2020

DILLON EUSTACE

Dublin
33 Sir John Rogerson's Quay, Dublin 2, Ireland. Tel: +353 1 667 0022 Fax: +353 1 667 0042.

Cayman Islands
Landmark Square, West Bay Road, PO Box 775, Grand Cayman KY1-9006, Cayman Islands. Tel: +1 345 949 0022 Fax: +1 345 945 0042.

New York
245 Park Avenue, 39th Floor, New York, NY 10167, U.S.A. Tel: +1 212 792 4166 Fax: +1 212 792 4167.

Tokyo
12th Floor, Yurakucho Itocia Building, 2-7-1 Yurakucho, Chiyoda-ku, Tokyo 100-0006, Japan. Tel: +813 6860 4885 Fax: +813 6860 4501.

DISCLAIMER:
This document is for information purposes only and does not purport to represent legal advice. If you have any queries or would like further information relating to any of the above matters, please refer to the contacts above or your usual contact in Dillon Eustace.

Copyright Notice:
© 2020 Dillon Eustace. All rights reserved.