DILLON EUSTACE

Cyber Supervision – where is IT at?

The Central Bank said last year that it considered cybersecurity to be one of its key supervisory risks. That was before the COVID-19 pandemic arrived testing firms' IT systems with large numbers of staff working remotely and which has seen an increase in phishing and malware campaigns. MUIREANN REEDY looks at the Central Bank's expectations in the area.

Background

In 2016 the Central Bank of Ireland ("CBI") published its "Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks" (the "Guidance") stating that the risks associated with information technology ("IT") and cybersecurity are a key concern to the CBI, given their potential to have serious implications for prudential soundness, consumer protection, financial stability and the reputation of the Irish financial system. In 2018 the CBI evidenced the importance it placed on this area, by establishing a dedicated Central IT Risk Team with responsibility for conducting on-site inspections and supporting ongoing supervision in the areas of IT and cyber risk across all regulated firms.

"the risks associated with information technology and cybersecurity are a key concern to the CBI, given their potential to have serious implications for prudential soundness, consumer protection, financial stability and the reputation of the Irish financial system."

There has been further supervisory focus on IT and cybersecurity this year. In March, the CBI issued a "Dear CEO" letter to the asset management industry following a thematic assessment which the Central IT Risk Team carried out on cybersecurity risk management in asset management firms. This was followed in October by the creation of the new pre-approval controlled function of Chief Information Officer. The CBI said the creation of the Chief Information Officer role was necessary to reflect the reliance placed by regulated financial service providers on technology, as well as the risks posed by IT. So how does the CBI expect IT and cyber risk to be managed?

Muireann Reedy

CBI's expectations

The Guidance sets out in detail the CBI's expectations in relation to IT and cyber risk management and is split into four key areas of governance, risk management, cybersecurity and outsourcing. The "Dear CEO" letter is also useful – although it is addressed to the asset management industry its findings are of relevance to all firms. Some key themes have come up in both documents.

Firstly, the CBI expects boards to engage with IT related issues – they should have a sufficient understanding of the IT risks facing the firm and ensure that these are properly managed, as well as setting the right tone from the top by promoting an IT security conscious culture at the firm. Boards are also expected to approve the IT and cybersecurity strategy and to check that this is aligned with the firm's overall business strategy. Boards should be briefed on key IT matters including major IT projects, IT priorities and significant IT incidents. In both documents the CBI highlighted the importance of IT policies being tailored to a firm's business and Irish regulatory requirements, being critical of this not being done in some cases where firms were part of an international group.

The CBI considers regular assessments to be a vital component of an IT and cybersecurity risk management framework (in its "Dear CEO" letter the CBI stated that cybersecurity testing should be done at least annually), emphasising the importance of new and emerging risks being considered, rather than the review being backwards-looking/event driven. It said that IT risk registers should also be kept up-to-date and include sufficient detail to enable the risks described in them to be proactively managed. Disaster recovery and business continuity plans should also be documented and tested periodically.

"they should have a sufficient understanding of the IT risks facing the firm and ensure that these are properly managed, as well as setting the right tone from the top by promoting an IT security conscious culture at the firm."

In terms of cybersecurity, the CBI has recommended that security awareness training programmes should be provided to staff and that firms should classify data so that appropriate safeguards can be put in place to protect any sensitive, valuable or critical data which is stored or processed by them. In its "Dear CEO" letter, the CBI highlighted the importance of firms having a documented cybersecurity and incident response plan in place which provides a roadmap for the actions that will be taken during and after a security incident, including responsibilities of staff, escalation, and communication with stakeholders, such as customers and the CBI.

The CBI noted that regulated firms often rely on outsourced service providers ("OSPs") to provide IT services and reminded firms that the responsibility for managing those risks lies with the regulated firm which engages the OSP.

"in its "Dear CEO" letter the CBI stated that cybersecurity testing should be done at least annually, emphasising the importance of new and emerging risks being considered, rather than the review being backwards-looking/event driven."

The CBI said it expects thorough due diligence to be conducted on prospective OSPs, for a detailed Service Level Agreement to be in place, and that firms will monitor the development of potential concentration risks.

Comment

IT and cybersecurity should be a recurring agenda item at all board meetings. When key IT issues are raised, they should be probed, considered and discussed by the board, and this should be evidenced in the meeting minutes. It is more important than ever for firms to ensure that staff are being provided with adequate cybersecurity training, with the state's National Cyber Security Centre reporting a rise in phishing and malware campaigns by fraudsters trying to exploit the pandemic.

It is worth noting that the CBI has imposed three enforcement fines on firms arising from IT-related incidents, the most recent fine being imposed in July of this year. In two of the cases the CBI found that regulatory failings left the firm open to cyber-fraud, and in the other case the firm was fined several million euro for IT governance failings. The CBI's focus on IT and cybersecurity is set to continue, with the CBI mentioning in a speech in October that firms' resilience to IT and cyber risk would be one of the areas which inspection teams would be reviewing, particularly in light of the disruption caused by COVID-19.

"It is more important than ever for firms to ensure that staff are being provided with adequate cybersecurity training, with the state's National Cyber Security Centre reporting a rise in phishing and malware campaigns by fraudsters trying to exploit the pandemic."

The CBI also stated in its 2019 Annual Report and Performance Statement that it intended to update the Guidance this year.

Muireann Reedy is a senior associate in Dillon Eustace's Regulatory Investigations Unit.