September 2016

Central Bank publishes Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks

Introduction

Following several inspections, thematic reviews and ongoing supervisory engagements throughout the course of 2015 and 2016, the Central Bank of Ireland (the "**Central Bank**") has on September 13, 2016 published Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks (the "**Guidance**").

The Guidance applies to all regulated firms in Ireland and follows a September 23, 2015 Central Bank letter to industry communicating the results of its thematic inspection in relation to cybersecurity and the related operational risks across investment firms, fund service providers and stockbrokers.

The Guidance highlights that, based on the Central Bank's supervisory experience to date, firms are not implementing sufficiently robust IT systems and controls and must increase their capability to deal with IT failures and cybersecurity incidents in order to minimise any potential impact on their business and reputation.

For most firms in the financial services sector, IT is a core aspect of the functioning of the business, with most (if not all) key functions supported or run by IT. The Central Bank highlights a number of inadequate practices, namely a lack of prioritisation, a lack of awareness and a lack of understanding of IT and cybersecurity related risks and point out that more attention is required at both senior management and Board level to ensure that these risks are

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

Breeda Cunningham
DD:+ 353 (0)1 673 1846
breeda.cunningham@dilloneustace.ie

Michele Barker
DD: +353 (0)1 673 1886
michele.barker@dilloneustace.ie

managed effectively. The Central Bank also identifies a number of recommended practices as set out below:

(i) Board of Directors and Senior Management Oversight of IT and Cybersecurity Risk

The Central Bank expects firms to develop and document a comprehensive Board approved IT strategy which is aligned with the overall business strategy with sufficient staff and financial resources allocated to the strategy to ensure it can be executed efficiently. The Central Bank also recommends that a well-defined, comprehensive and functioning IT risk management framework is implemented.

The Guidance emphasises the need for the Board to receive updates on key IT issues, including major IT projects, IT priorities and significant IT incidents as well as regular reports on key IT risks. Board members and senior management are also expected to possess sufficient knowledge and understanding of the IT risks facing firms and take steps to ensure that these risks are well understood throughout the firm.

(ii) IT Specific Governance

The Central Bank recommends that firms should ensure that documented policies, standards and procedures which address the identification, monitoring, mitigation and reporting of firms' IT related risks are in place and that the roles and responsibilities in managing IT risks are clearly defined, documented and communicated to relevant staff. In addition, a sufficiently senior person in the firm should be appointed with responsibility for IT and cybersecurity matters. The Central Bank recommends that these policies and procedures are reviewed and updated on a regular basis.

(iii) IT Risk Management Framework

The Central Bank expects that firms develop, implement, maintain and communicate an IT risk management framework, which should facilitate a comprehensive review of IT risks, encompassing risk identification, assessment, monitoring and testing of its effectiveness and set out staff and senior management responsibilities and accountability.

The Guidance provides that risk assessments should be carried out on a regular basis, considering both internal and external sources of risk and firms should maintain an inventory of all IT assets within the firm. Particular consideration should be given to the risks associated with the continued use of older IT equipment/infrastructures. An up-to-date list of identified IT risks should be developed and maintained by firms and the Central Bank should be notified in circumstances where an IT incident has a significant adverse effect on the firm's ability to provide adequate services to its customers, its reputation or its financial condition. The effectiveness of IT controls should be subject to a periodic and independent review and, where warranted, given the nature and scale of the firm, penetration testing should be carried out.

(iv) Disaster Recovery and Business Continuity Planning

One of the issues raised by the Guidance is that a high reliance on IT for critical business operations exposes firms to the risk of severe disruption. Firms should ensure that documented disaster recovery and business continuity plans are in place and that sufficient resources are provided to support effective planning, testing and execution of same.

The Central Bank expects firms to consider a range of plausible event and disaster scenarios, including cybersecurity events and must have in place a documented back-up strategy for critical data and conduct regular back-up and restore tests to verify the restore capabilities for critical systems.

The Central Bank expects that the Board is provided with updates on the various scenarios considered and the development and testing of the disaster recovery and business continuity plans.

(v) IT Change Management

The Guidance outlines that firms are expected to have in place adequate systems to manage the change/upgrade/replacement of IT systems, including having approval requirements in place.

It is also recommended that IT project plans are clearly documented and periodic updates should be provided to the Board detailing the progress of any significant IT projects.

(vi) Cybersecurity

The Guidance states that cyber-attacks are becoming more sophisticated and difficult to detect. Current technological trends (such as cloud computing and mobile devices) further increase exposure to cyber risk. Firms are required to have in place a documented strategy to address cyber risk, which is reviewed and approved at Board level.

The Central Bank recommends that training programmes are implemented to enable staff to identify good IT security practices, common threat types and familiarise themselves with the firm's policies and procedures regarding the appropriate use of applications, systems and networks.

The Central Bank provides that, at a minimum, cyber risk management should address the identification, prevention and detection of security events, threats and incidents, security incident handling and recovery planning after an incident. Firms should also have in place a documented cybersecurity incident response plan which provides a roadmap for the actions the firm will take during and after a security incident.

The Central Bank should be notified in circumstances where a cybersecurity incident has a significant adverse effect on the firm's ability to provide adequate services to its customers, its reputation or its financial condition.

(vii) Outsourcing of IT Systems and Services

The Guidance states that regulated firms are becoming increasingly reliant on outsourcing IT services to external service providers. Outsourcing does not reduce the risks associated with IT and the Central Bank points out that the responsibility for the effective management of these risks remains with the regulated firm. Therefore firms are required to ensure that a framework is in place with clear lines of responsibility for ongoing management, operational oversight, risk management and review of the firm's external service providers.

The Central Bank expects to conduct thorough due diligence on any potential service providers, to include consideration of their technical capabilities, performance track record, financial strength and viability, service quality and reliability. In circumstances where any IT services are outsourced, the contract between the firm and the service provider should include a Service Level Agreement detailing sufficiently robust provisions in relation to security, service availability, performance metrics and penalties.

The Guidance also outlines the requirement to have in place an exit management strategy to reduce the risk of disruption in the event that key outsourced IT services are unexpectedly withdrawn by the service provider or terminated by the firm.

For further information on any of the issues discussed in this briefing note please contact Breeda Cunningham, Michele Barker or your usual contact in Dillon Eustace.

Dillon Eustace
September 2016

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.