McCann FitzGerald

Central Bank Guidance on IT and Cyber Security Risks

BRIEFING

In September 2016 the Central Bank of Ireland ("**Central Bank**") issued Cross-Industry Guidance in respect of IT and Cyber Security Risks ("**Guidance**") which sets out its current thinking as to good practices that regulated firms should use to develop effective IT and cyber security governance and risk management frameworks. Regulated entities will need to take on board this recent guidance and incorporate it into their governance and risk management frameworks as the Central Bank intends to use it to inform its future supervisory decisions.

In particular, regulated entities should take into account the Central Bank's concerns and criticisms regarding many firms' current contractual arrangements with their outsourcing service providers and ensure that these arrangements are adapted to reflect the Guidance.

The Central Bank and IT and Cyber Security Risks

The Central Bank's concerns around cyber security risks have been well signalled. During the course of 2015 it carried out a thematic inspection in relation to cyber security/operational risk. Later, in September 2015, it communicated the results of its inspections, in the form of a "Dear CEO Letter", to the boards and senior management of investment firms, funds, fund service providers and stock-brokers. In that letter, the Central Bank outlined examples of best practice in dealing with cyber security risk as well as a self-assessment questionnaire for firms regarding their cyber security capabilities. In July 2015, the Central Bank also published a "Dear CEO Letter" in which it emphasised to investment fund boards the need for delegate oversight and the importance of specific reporting by delegates at board meetings on the policies and procedures in place to counter cyber attacks. See our related briefings here and here.

The Guidance - Key Takeaways

In its latest Guidance the Central Bank sets out its current thinking as to good practices that regulated firms should use to inform the development of effective IT and cyber security governance and risk management frameworks. It is based on Central Bank inspections, thematic reviews and ongoing supervisory engagement, which have highlighted a number of areas where IT and cyber security governance and risk management have fallen short of the expected standards. According to the Central Bank:

"[t]he nature and number of inadequate practices identified indicate a lack of prioritisation, awareness and understanding of IT and cyber security related risks and that

Central Bank Guidance on IT and Cyber Security Risks
(continued)

more work is required at Board and Senior Management level to ensure that firms are effectively managing these risks."

The Guidance has four sections which deal with Governance, Risk Management, Cyber Security and Outsourcing. The Guidance does not address all aspects of the management of IT and cyber security risk but rather focuses on those areas that the Central Bank deems most pertinent at this time. The Guidance also acknowledges that the relevance and importance of the issues that it raises will vary according to the business model, size and technological complexity of the institution and the sensitivity and value of its information and data assets.

Governance

The Board of Directors and Senior Management are responsible for setting and overseeing the firm's business strategy and risk appetite and must ensure that IT risk is considered in this context. The Board and Senior Management must possess sufficient knowledge and understanding of the IT related risks facing the firm and take steps to ensure that these risks are well understood and properly managed throughout the firm. The Board must receive updates on key IT issues as well as regular reports on key IT risks.

The Board approved IT strategy must be aligned with the overall business strategy and there must be sufficient resources to execute that strategy, including an adequate IT budget, staff levels and relevant expertise. Firms must have a sufficiently robust IT governance structure in place to facilitate effective oversight of the management of IT risks. They must also have documented IT policies and procedures addressing the identification, mitigation and reporting of the firm's IT related risks, as well as clearly defined roles and responsibilities including a senior role which is responsible for IT and cyber security matters.

Group driven IT strategies and governance documents must be appropriately tailored for the Irish firm from a regulatory and operational perspective. The governance structure must also provide for independent assurance on the effectiveness of the IT risk management, internal controls and governance processes within the firm.

Risk management

Firms must develop, implement, maintain and communicate an appropriate IT Risk Management Framework ("**ITRM**") which incorporates, as appropriate, relevant best practices and internationally adopted frameworks for IT risk management. They must establish and maintain a thorough inventory of IT assets, classified by business criticality, and put in place a Business Impact Analysis process to regularly assess the business criticality of IT assets. Firms must also develop and maintain an up-to-date IT risk register as well as adequate management processes and plans for IT incident detection, notification, and escalation. Critical or sensitive data must be correctly identified and adequately safeguarded. Firms must ensure that the effectiveness of IT controls is subject to periodic independent review and that penetration testing is carried out if warranted.

A firm must be able to demonstrate that it has assessed the risks associated with the maintenance of older IT systems and must have a strategy in place for dealing with those systems where they support critical business operations. More broadly, firms must have formal IT change management processes in place. Major proposed changes to the IT infrastructure must be subject to a thorough prior risk and impact analysis.

The Central Bank also expects firms to dedicate sufficient resources to support IT disaster recovery and business continuity planning, test and execution. Firms must have a documented disaster recovery and business continuity plan in place as well as a strategy for backing up critical data.

A firm must notify the Central Bank when it becomes aware of an IT (or cyber security) incident that could have a significant and adverse effect on the firm's ability to provide adequate services to its customers, its reputation or financial condition.

Cyber security

Cyber risk must be managed within the context of overall IT risk management. Firms must have a well-considered and documented Board approved strategy to address cyber risks, as well as documented cyber security policies and procedures. Cyber risk assessments must be performed regularly and robust safeguards put in place to protect against cyber security events and incidents.

Firms must implement strong controls over access to their IT systems. They must also put in place processes and procedures to detect a breach in a timely manner and have a documented cyber security incident response plan as well as a documented recovery plan for the rapid resumption of critical services.

Outsourcing

Firms must have adequate governance and risk management processes in place to effectively address the risks associated with the outsourcing of IT services, including cloud services. There must be clear lines of responsibility for ongoing management, operational oversight, risk management and regular review of the firm's outsourcing service providers ("**OSPs**").

Firms must conduct thorough due diligence on prospective OSPs. In addition, the contract between the firm and its selected OSP must include a documented service level agreement ("**SLA**") or its equivalent, which deals with, among other things; the nature, quality and scope of the service to be delivered; the roles and responsibilities of the contracting parties; the requirements for service levels, availability and reliability; and system and information/data security, business continuity and disaster recovery.

Firms must also:

- develop and maintain an exit management strategy to reduce the risks of business disruption should key IT outsourced services be unexpectedly withdrawn by the OSP, or voluntarily terminated by the firm;
- monitor for the development of potential concentration risks and take appropriate action if the firm is, or is likely to become reliant on a small number of OSPs to provide critical IT services; and
- ensure that the outsourcing policy includes a provision that any outsourcing arrangements do not impede effective on or off-site supervision of the firm by the Central Bank; this must also be reflected in any specific contracts entered into by the firm.

Comment and Next Steps

IT risks present ongoing challenges for financial services firms, both because of the increasing importance of technological developments in the sector and the increasing sophistication of criminal attacks. The financial services sector is among the most heavily targeted sectors by cyber criminals and recent years have seen a number of different types of attacks including data breaches, ransom demands and distributed denial of service attacks. For example, in February 2016, cyber criminals gained access to the Swift Codes of the Bangladesh Central Bank and attempted to transfer $951 million from its accounts. While the cyber criminals ultimately "only" obtained $81 million this is still likely to have been one of the biggest (individual) bank robberies in history. A year previously, Europol and other investigative authorities uncovered the theft of up to $1 billion from financial institutions worldwide, over about a two year period.

Regulators, including the Central Bank, have taken note of these risks. According to the Central Bank, it intends to continue to intensify its supervisory oversight of IT and cyber security related risks over the coming years and the Guidance will inform its supervisory approach. Consequently, each financial services firm should consider the issues outlined in the Guidance when reviewing its existing IT related governance and risk management arrangements and use the Guidance to inform the future development of those arrangements.

Central Bank Guidance on IT and Cyber Security Risks
(continued)

More broadly, firms, including in particular the Board of Directors and senior management, will need to keep up-to-date with the ever changing nature of IT risks and their potential impact. Best practice in countering IT risks is also evolving and firms will need to ensure that they keep up-to-date as IT/cyber security best practice continues to develop.

In this respect firms should in particular take note of the EU's Network and Information Security Directive which will apply from 9 May 2018. The Directive is designed to boost the overall level of cyber security in the EU. It will bring about significant changes to cyber security laws and will impose cyber security obligations on 'operators of essential services', including financial market infrastructures, and digital service providers. See our related briefing here.

Firms updating their IT and cyber security in response to the Central Bank's recommendations may also wish to review their data protection policies and procedures in anticipation of the General Data Protection Regulation's entry into effect in 2018, as there is some overlap between the two.

Further information is available from:

Karyn Harty
Partner, Dispute Resolution & Litigation Group

DDI +353-1-607 1220
EMAIL karyn.harty@mccannfitzgerald.com

Adam Finlay
Partner, Technology & Innovation Group

DDI +353-1-607 1795
EMAIL adam.finlay@mccannfitzgerald.com

Josh Hogan
Partner, Finance Group

DDI +353-1-607 1720
EMAIL josh.hogan@mccannfitzgerald.com

Alternatively, your usual contact in McCann FitzGerald will be happy to help you further.

McCann FitzGerald

Principal Office
Riverside One
Sir John Rogerson's Quay
Dublin 2
D02 X576

Tel: +353-1-829 0000

London
Tower 42
Level 38C
25 Old Broad Street
London EC2N 1HQ

Tel: +44-20-7621 1000

New York
Tower 45
120 West 45th Street
19th Floor
New York, NY 10036

Tel: +1-646-952 6001

Brussels
40 Square de Meeûs
1000 Brussels

Tel: +32-2-740 0370

Email

inquiries@mccannfitzgerald.com

www.mccannfitzgerald.com