McCann FitzGerald

Timely focus by Central Bank on cyber-security

BRIEFING

Does your board know its virus from its worm, its Trojan horse from its botnet? Has it yet encountered denial of service, phishing or spoofing? If not, a recent review by the Central Bank of Ireland of cyber-security and operational risk should serve to focus minds in regulated entities on the serious threat to modern business of cyber attack.

In February 2015, the Central Bank of Ireland published its programme of themed inspections in Markets Supervision, to reflect a number of supervisory priorities for this year. This included an inspection in relation to the management of operational risk surrounding cyber-security. The Central Bank's objective in the review was to examine firms' control environment (including policies and procedures) designed to detect and prevent cyber-security breaches as well as board oversight of cyber-security. The Central Bank has just completed this review and the results and recommendations have been communicated to the boards and senior management of investment firms, funds, fund service providers and stock-brokers.

Evolution and scale of cyber threat

Cyber attack is one of the foremost risks for modern business. Whilst attacks against electronic systems have been reported for decades, the modern cyber criminal bears little resemblance to the U.S. phone phreakers of the 1960s who used toy whistles to manipulate tones on telephone systems to place long distance calls free of charge. Since then cyber attacks have continued to increase in frequency and sophistication. This has coincided with more businesses moving key assets and systems to the electronic sphere.

The potential scale of the problem for Irish business is illustrated by figures released in 2015 by the UK Government who commissioned an Information Security Breaches Survey in that jurisdiction. It reported that 90% of large organisations and 74% of small organisations surveyed had experienced a security breach in the last year with 59% expecting an increase in security breaches in the coming year. 14 was the median number of breaches suffered by large organisations in the last year with four being the median for small organisations. The average cost to a large organisation of its worst security breach ranged from £1.46 million - £3.14 million. The average cost for a small organisation ranged from £75,000 - £311,000. In light of these statistics, the review and recommendations made by the Central Bank are timely.

Timely focus by Central Bank on cyber-security

(continued)

Central Bank recommendations

The Central Bank has published a list of suggested best practice measures to be taken by firms with a culture of security and resilience to be driven from board level. These measures include:

- Adequate training for staff with periodic testing of responses to cyber attack scenarios;
- Cyber-security as a standing agenda item at board meetings;
- An understanding at board level of the assets and information of most value to the firm;
- Board satisfaction that the firm's policies and procedures are robust and can comprehensively facilitate the firm's cyber-security needs. If an entity relies on the IT infrastructure of their parent/group, formal sign-off of a localised version of the policies is recommended to ensure that they are appropriate for the local firm;
- A clear reporting line to the board for cyber-security incidents;
- The possible appointment of a Chief Information Office (or equivalent) with accountability for information security. If this is not possible, a board member with appropriate training, should assume responsibility for cyber-security agenda items;
- Established procedures to deal with a successful attack bearing in mind that communication channels such as email may be unavailable;
- Appropriate processes to verify the legitimacy of all requests, *eg* change of bank account details, received via all methods of communication;
- The granting of requests for payment to a third party bank account only after client verification and compliance with anti-money laundering obligations;
- Regular system penetration tests by external specialists;
- Confirmation that cyber-security standards of third parties with whom the firm engages are comprehensive so as to minimise direct impact on the firm should the third party be subject to cyber attack;
- Contingency plans in the event of a systems breach or data compromise;
- Reporting any substantial attack/successful breach of their systems to the Central Bank;
- Protection of mobile devices with passwords, encryption *etc*;
- Keeping up to date on current cyber-security threats.

The Central Bank goes on to state that these measures should not be regarded as exhaustive. Rather, firms should evaluate on an ongoing basis their own cyber risks and decide on how they are best managed or mitigated. The Central Bank provides a questionnaire to assist firms in carrying out an assessment of their cyber-security capabilities.

Finally, it advises that, where there is non-compliance with regulatory requirements, the Central Bank will have regard to these recommendations, when exercising its regulatory and enforcement powers. In light of this statement, boards of these firms should consider carrying out an in-depth analysis of their current cyber-security controls so as to ensure they can demonstrate that effective systems and procedures are in place to protect against cyber attack.

Other measures to combat cyber attack

The Central Bank is not alone in its focus on cyber-security. Its action mirrors a number of other measures being taken at domestic and EU level to combat the threat of cyber attack. These include a Criminal Justice (Offences relating to Information Systems) Bill to be published in the coming Dáil session. This will enable ratification of the 2001 Council of Europe Convention on Cybercrime and the transposition of the EU Directive 2013/40 on attacks against

Timely focus by Central Bank on cyber-security

(continued)

Information Systems. Also, October is European Cyber-security Month, the EU's campaign to promote cyber-security. In addition, the EU's Digital Single Market Strategy aims to improve the supply of secure technological solutions by EU industry. There are plans to establish a public-private partnership on cyber-security in technology and online networks and to review the ePrivacy Directive in 2016.

These are all welcome initiatives as the threat of cyber attack continues to increase. With 2014 findings from the UK that 70% of organisations keep their worst security incident under wraps, we can be sure that what's in the news is just the tip of the iceberg.

Further information is available from:

Catherine Derrig

Partner, Dispute Resolution & Litigation

DDI

+353-1-607 1710

EMAIL

catherine.derrig@
mccannfitzgerald.ie

Fiona O'Beirne

Partner, Dispute Resolution & Litigation

DDI

+353-1-607 1311

EMAIL

fiona.obeirne@
mccannfitzgerald.ie

Paul Lavery

Partner, Technology & Innovation

DDI

+353-1-607 1330

EMAIL

paul.lavery@
mccannfitzgerald.ie

Annette Hogan

Consultant, Technology & Innovation Group

DDI

+353-1-607 1207

EMAIL

annette.hogan@
mccannfitzgerald.ie

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
Fax: +353-1-829 0010

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

Tel: +44-20-7621 1000
Fax: +44-20-7621 9000

Brussels
40 Square de Meeûs
1000 Brussels

Tel: +32-2-740 0370
Fax: +32-2-740 0371

Email
inquiries@mccannfitzgerald.ie

www.mccannfitzgerald.ie