May 2015

Central Bank Themed Inspections on Cyber-Security

As flagged in its Enforcement Priorities for 2015, the Central Bank of Ireland (the "**Central Bank**") has commenced a process of themed inspections with regards to cyber-security readiness. Those who have not yet been subject to such an inspection should bear the questions raised by the Central Bank in mind. They should also ensure that they are able to answer such questions should they be the subject of such a Central Bank themed inspection.

We have set out below the list of questions which the Central Bank raised in certain of its themed inspections with regards to cyber-security at Appendix 1. As a general comment the Central Bank's questions relate to the processes, controls and risk mitigants that such firms should have in place in order to minimise the risks attaching to cyber-security.

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

APPENDIX 1

General Information
1.
What does the Firm presently consider to be its three most serious cyber-security risks, and why?
2.
Please indicate whether the Firm has conducted a risk assessment to identify cyber-security threats, vulnerabilities, and potential business consequences. If yes: a. Who (business group/title) conducts/conducted them, and in what month and year was the most recent assessment completed? b. Please outline any findings/recommendations from the most recent risk assessment.
3.
Please indicate whether the Firm has conducted a risk assessment to identify physical security threats and vulnerabilities that may impact on cyber-security. If yes: a. Who (business group/title) conducts/conducted them, and in what month and year was the most recent assessment completed? b. Please outline any findings/recommendations from the most recent risk assessment.
4.
Does the Firm have a business continuity plan? And does this plan address mitigation of the effects of a cyber-security incident?
5.
Does the Firm have a Chief Information Security Officer or equivalent position? If so, please identify the person and their title. If not, where does principal responsibility for overseeing cyber-security reside within the Firm?
6.
Does the Firm maintain insurance that specifically covers losses and expenses attributable to cyber-security incidents?
Protection of Firm Networks and Information
7.
Please identify any published cyber-security risk management process standards which the Firm has used to model its information security design and processes on.
8.
Please indicate if the Firm utilises any of the following practices and controls regarding the protection of its networks and information. a. The Firm provides written guidance and training to employees concerning information security risks and responsibilities. If the Firm provides such guidance and/or training, please provide a copy of any related written materials (*e.g. guidance and/or* presentations). b. Access to systems and assets is controlled, incorporating the principle of least functionality

(only what is needed).

c. The Firm maintains an environment for testing and development of software and applications that is separate from its business environment.

d. The Firm maintains a baseline configuration of hardware and software, and users are prevented from altering that environment without authorisation and an assessment of security implications.

e. The Firm has a process to manage IT assets through removal, transfers, and disposition.

f. The Firm has a process for ensuring regular system maintenance, including timely installation of software patches that address security vulnerabilities.

g. The Firm's information security policy and training addresses removable and mobile media.

h. The Firm maintains a written data destruction policy.

i. The Firm maintains a written cyber-security incident response policy. If so, please provide a copy of the policy. Please also indicate whether the Firm conducts tests or exercises to assess its incident response policy, and if so, when and by whom the last such test or assessment was conducted.

j. The Firm periodically tests the functionality of its backup system. If so, please provide the month and year in which the backup system was most recently tested and any findings that were identified

9.

Please indicate whether the Firm makes use of encryption. If so, what categories of data, communications, and devices are encrypted and under what circumstances?

10.

Please indicate whether the Firm conducts periodic audits of compliance with its information security policies. If so, please provide a copy of the most recent findings/recommendations and confirm by whom the audit was conducted?

Risks Associated With Remote Customer Access and Funds Transfer Requests

11.

Please indicate whether the Firm provides customers with on-line account access. If so, please provide the following information:

a. The name of any third party or parties that manage the service.

b. The functionality for customers on the platform

c. How customers are authenticated for on-line account access and transactions.

d. Any software or other practice employed for detecting anomalous transaction requests that may be the result of compromised customer account access.

e. A description of any security measures used to protect customer PINs stored on the sites.

f. Any information given to customers about reducing cyber-security risks in conducting transactions/business with the Firm.

12.

Please provide a copy of the Firm's procedures for verifying the authenticity of email requests. If no written procedures exist, please describe the process.

13.

Please provide a copy of any Firm policies for addressing responsibility for losses associated with attacks or intrusions impacting customers.

a. Does the Firm offer its customers a security guarantee to protect them against hacking of their accounts? If so, please provide a copy of the guarantee if one exists and a brief description.

Risks Associated With Vendors and Other Third Parties

14.

Do outsourced IT resources comply with the same requirements as in house resources (and are there processes in place to manage that)?

15.

Does the Firm regularly incorporate requirements relating to cyber-security risk into its contracts with vendors/clients? If so, please describe these requirements and the circumstances in which they are incorporated and please provide a sample copy.

16.

Does the Firm assess the segregation of sensitive network resources from resources accessible to third parties? If yes, who (business group/title) performs this assessment? Please provide a copy of any relevant policies and procedures.

17.

Can vendors, business partners, or other third parties conduct remote maintenance of the Firm's networks and devices? If so, please describe any approval process, logging process, or controls to prevent unauthorised access. Please provide a copy of any relevant policies and procedures.

Detection of Unauthorised Activity

18.

For each of the following practices that may be employed by the Firm to assist in detecting unauthorised activity on its networks and devices, please briefly explain how and by whom (title, department and job function) the practice is carried out.

a. Identifying and assigning specific responsibilities, by job function, for detecting and reporting suspected unauthorised activity.
b. Maintaining baseline information about expected events on the Firm's network.
c. Aggregating and correlating event data from multiple sources.
d. Establishing written incident alert thresholds.
e. Monitoring the Firm's network environment to detect potential cyber-security events.
f. Monitoring the Firm's physical environment to detect potential cyber-security events.
g. Using software to detect malicious code on Firm networks and mobile devices.
h. Monitoring the activity of third party service providers with access to the Firm's networks.
i. Monitoring for the presence of unauthorised users, devices, connections, and software on the Firm's networks.
j. Evaluating remotely-initiated requests for transfers of customer assets to identify anomalous and potentially fraudulent requests.
k. Using data loss prevention software.
l. Conducting penetration tests and vulnerability scans. If so, please identify the month and year of the most recent penetration test and recent vulnerability scan, whether they were conducted by Firm employees or third parties, and describe any findings from the most recent risk test and/or assessment that were deemed to be potentially moderate or high risk but have not yet been addressed.
m. Testing the reliability of event detection processes. If so, please identify the month and year

of the most recent test.

n. Using the analysis of events to improve the Firm's defensive measures and policies.

Other

19.

Since January 1, 2014, has your Firm experienced any of the following types of events? If so, please provide a brief summary for each incident. The summary should include the number of such incidents, the description of the significance and any effects on the Firm (or 3rd parties), and if these incidents resulted in any financial loss to the firm or connected 3rd parties.

a. Malware was detected on one or more Firm devices. Please identify or describe the malware.

b. Access to a Firm web site or network resource was blocked or impaired by a denial of service attack. Please identify the service affected, and the nature and length of the impairment.

c. The availability of a critical Firm web or network resource was impaired by a software or hardware malfunction. Please identify the service affected, the nature and length of the impairment, and the cause.

d. The Firm's network was breached by an unauthorised user. Please describe the nature, duration, and consequences of the breach, how the Firm learned of it, and how it was remediated

e. The compromise of a customer's or vendor's computer used to remotely access the Firm's network resulted in fraudulent activity, such as efforts to fraudulently transfer funds from a customer account or the submission of fraudulent payment requests purportedly on behalf of a vendor.

f. The Firm received fraudulent emails, purportedly from customers, seeking to direct transfers of customer funds or securities.

g. The Firm was the subject of an extortion attempt by an individual or group threatening to impair access to or damage the Firm's data, devices, network, or web services.

h. An employee or other authorised user of the Firm's network engaged in misconduct resulting in the misappropriation of funds, securities, sensitive customer or Firm information, or damage to the Firm's network or data.

20.

Since January 1, 2014, if not otherwise reported above, did the Firm, either directly or as a result of an incident involving a vendor or other 3rd party, experience the theft, loss, unauthorised exposure, or unauthorised use of or access to customer information. If so, please provide a brief summary of each incident or a record describing each incident.

21.

For each event identified in response to Questions 19 and 20 above, please indicate whether it was reported to the following, if so please provide the date on which the report was made:

- An Garda Siochana
- The Central Bank of Ireland or relevant regulatory body
- Other parties (please specify)

22.

Please feel free to provide any other information you believe would be helpful to the Central Bank of Ireland in evaluating the cyber-security posture of the Firm or the financial services industry.

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.

Hong Kong
604 6F Printing House, 6 Duddell Street, Central, Hong Kong. Tel: +852 352 10352.

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.