



Banc Ceannais na hÉireann
Central Bank of Ireland

Eurosystem

T +353 1 224 6000 F +353 1 671 6561

Cúirt Uíbh Eachach, Bloc D, Bóthar Fhearchair,
Baile Átha Cliath 2, Éire.

Iveagh Court, Block D, Harcourt Road, Dublin 2, Ireland.

www.centralbank.ie

22 September 2015

Review of the management of operational risk around cyber-security within the Investment Firm and Fund Services Industry

Dear Chair,

The Central Bank of Ireland (the 'Central Bank') recently undertook a thematic review to assess the management of cyber security and related operational risks across Investment Firms, Fund Service Providers and Stockbrokers. The objective of 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.

Cyber security is steadily emerging as an individually recognised risk in all firms. This is primarily due to the increasing reliance by firms in all sectors on information technology ('I.T.'), the evolving sophistication of cyber-crimes and the growing frequency in the type and number of cyber related breaches, attempts, attacks and intrusions. Valuable assets including confidential data, cash and intellectual property should therefore be protected by appropriate security, processes and policies.

Firms should be aware that cyber security risk is a real and live threat and a successful attack could have a significant negative impact on daily operations. Firms need to recognise that a successful cyber-attack can also have far reaching financial and reputational implications; therefore appropriate levels of security are required to be in place.

It is the board's responsibility to ensure that a firm is properly governed and has the necessary processes and systems to protect the firm and all of its assets. The review found that in a number of firms I.T. security, including cyber security, is deemed to be the sole responsibility of the I.T. department with limited involvement, if any, from other business areas or from the board itself.

The Central Bank is of the view that an ethos of effective corporate governance, coupled with appropriate I.T. and cyber-security risk management, can be the foundation of successful protection against cyber-crime. The board should develop a culture of security and resilience throughout the firm and ensure that the firm has the necessary plans in place to deal with both internal and external cyber security breaches.

Examples of best practice that firms should consider are set out in **Appendix A**. This Appendix is not an exhaustive list of best practices. Firms should, at all times, be evaluating their own cyber-risks and deciding on how they are best managed or mitigated.

Please be advised that, where there is non-compliance with relevant regulatory requirements, the Central Bank will have regard to these recommendations, when exercising its regulatory and enforcement powers.

Firms may find the questionnaire attached at **Appendix B** useful when carrying out a self-assessment of their cyber-security capabilities. Firms are not required to return this questionnaire to the Central Bank.

It is requested that this communication is brought to the attention of each of your board members as well as the senior management at your firm.

Yours sincerely,



Patricia Dunne
Deputy Head - Investment Firms and Fund Services
Markets Supervision Directorate

Appendix A

Cyber Security – Best practice guide

1	The board should drive a culture of security and resilience throughout the firm.
2	Firms should ensure that all staff members receive adequate training in relation to cyber-security and the threats that they may encounter. Furthermore, firms should periodically test staff responses to various cyber-attack scenarios.
3	Cyber-security should be a standing agenda item for discussion at board meetings.
4	The board should understand what assets and information are of most value to the firm.
5	The board should satisfy itself that the policies and procedures of the firm are robust and can comprehensively facilitate the firm's cyber-security needs. Where entities rely on the IT infrastructure of their parent/group, it is recommended that there is formal sign-off of a localised version of policies to ensure that these procedures are appropriate for the local firm.
6	A clear reporting line to the board should be established for cyber-security incidents.
7	The board should consider the appointment of a Chief Information Officer or equivalent with accountability for information security. Where this is not possible, a board member should assume responsibility for cyber-security agenda items. The appointed board member should ensure that they receive appropriate training to deliver on their new role.
8	The board should satisfy itself that the firm has a procedure to deal with a successful attack and/or intrusion to its systems while cognisant of the fact that following a cyber-incident, the normal communications such as email may not be accessible.
9	Firms should have appropriate processes in place to verify the legitimacy of all requests ¹ received via all methods of communication (including telephone and email).
10	Where a firm is requested to make payment(s) to a third party bank account and such a request is granted; client verification and compliance with relevant anti- money laundering obligations are essential.
11	In order to discover vulnerabilities, firms should consider engaging the services of an external specialist to carry out a penetration test of their systems on a regular basis; best practice would be to carry out such tests at least annually.
12	Firms should satisfy themselves that the cyber-security standards of the vendors/third parties they utilise are comprehensive in that they minimise direct impact to the firm, should the third party be subject to a cyber-attack.

¹ For example: redemption requests, change of bank account details, information requests etc.

13	Each firm should have contingency plans in place for the steps that they would take should their systems be breached or their data compromised.
14	Firms should report any successful breach of their systems to the Central Bank.
15	Firms should also report any substantial attacks (that may not have led to a successful breach) to the Central Bank.
16	Firms should ensure that mobile devices with access to their systems, applications and/or network are protected. This can include, but is not limited to: encryption, remote wiping, password protection etc.
17	Firms should ensure that they are kept up to date on current cyber security threats. Firms should consider joining a threat information sharing forum on this topic.

Appendix B

Central Bank of Ireland – Self Assessment Questionnaire

General Information	
1	What does the Firm presently consider to be its three most serious cyber-security risks, and why? What steps has the Firm taken to prevent these risks from materialising?
2	Please indicate whether the Firm has conducted a risk assessment to identify cyber-security threats, vulnerabilities, and potential business consequences. If yes: - Who (business group/title) conducts/conducted them, and in what month and year was the most recent assessment completed? - Please outline any findings/recommendations from the most recent risk assessment.
3	Please indicate whether the Firm has conducted a risk assessment to identify <u>physical</u> security threats and vulnerabilities that may impact on cyber-security. If yes: - Who (business group/title) conducts/conducted them, and in what month and year was the most recent assessment completed? - 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. If the answer to any section is 'No' please explain why. - 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 (<i>e.g. guidance and/or presentations</i>). - Access to systems and assets is controlled, incorporating the principle of least functionality (only what is needed). - The Firm maintains an environment for testing and development of software and applications that is separate from its business environment. - 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. - The Firm has a process to manage IT assets through removal, transfers, and disposition. - The Firm has a process for ensuring regular system maintenance, including timely installation of software patches that address security vulnerabilities. - The Firm's information security policy and training addresses removable and mobile media. - The Firm maintains a written data destruction policy.

	• 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. • 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 Client Access and Funds Transfer Requests

11	Please indicate whether the Firm provides its clients with any on-line account access. If so, please provide the following information: • The name of any third party or parties that manage the service. • The functionality for customers on the platform • How customers are authenticated for on-line account access and transactions. • Any software or other practice employed for detecting anomalous transaction requests that may be the result of compromised customer account access. • A description of any security measures used to protect customer PINs stored on the sites. • 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 from clients/vendors. 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. • 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.
- Identifying and assigning specific responsibilities, by job function, for detecting and reporting suspected unauthorised activity.
 - Maintaining baseline information about expected events on the Firm's network.
 - Aggregating and correlating event data from multiple sources.
 - Establishing written incident alert thresholds.
 - Monitoring the Firm's network environment to detect potential cyber-security events.
 - Monitoring the Firm's physical environment to detect potential cyber-security events.
 - Using software to detect malicious code on Firm networks and mobile devices.
 - Monitoring the activity of third party service providers with access to the Firm's networks.
 - Monitoring for the presence of unauthorised users, devices, connections, and software on the Firm's networks.
 - Evaluating remotely-initiated requests for transfers of customer assets to identify anomalous and potentially fraudulent requests.
 - Using data loss prevention software.
 - 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.
 - Testing the reliability of event detection processes. If so, please identify the month and year of the most recent test.
 - 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. If the answer to any section is no, is the firm satisfied that it has sufficient protection in place to prevent such an incident from occurring.
- Malware was detected on one or more Firm devices. Please identify or describe the malware.
 - 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.
 - 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.
 - 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

	• 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. • The Firm received fraudulent emails, purportedly from customers, seeking to direct transfers of customer funds or securities. • 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. • 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 Síochána • The Central Bank of Ireland or relevant regulatory body • Other parties (please specify)