LK SHIELDS
YOUR LEGAL COUNSEL

FINANCIAL SERVICES

Cyber Security Threats: Implications for Irish Fund Boards and Managers

by

Cyber Security Threats: Implications for Irish Fund Boards and Managers

24th August 2016 | by

This briefing assesses the potential impact of cyber-attacks, particularly in the context of the asset management industry in Ireland, and provides guidance for fund boards and managers regarding the appropriate procedures and systems that should be in place to adequately prevent or deal with cyber-attacks.

The Threat of Cyber-attacks

An increasing number of reported cyber-attacks on businesses worldwide, including businesses in the international asset management industry, together with increased regulatory scrutiny around the area of cyber security, have led many fund boards and managers to review their cyber security strategies with a view to implementing preventative controls and timely responses.

Due to the nature of their business, asset management firms hold large amounts of capital and control large amounts of valuable data relating to their clients, both institutional and high net worth individuals. This provides an adequate incentive for an attack from cyber criminals. The financial implications of such an attack, together with the subsequent reputational damage if such an attack was not dealt with adequately, means that the issue of cyber security is generating increased focus from senior personnel within such organisations.

Regulatory position in Ireland

In early 2015, the Central Bank of Ireland (Central Bank) undertook a thematic review of fund managers and investment firms to assess the management of cyber security and related operational risks. The objective of the review was to examine if firms had adequate policies and procedures in place to prevent and detect cyber security breaches. The review found that many firms deemed cyber security to be the sole responsibility of the I.T. department within the firm with limited involvement, if any, from the board of the firm.

Following the thematic inspection, the Central Bank published a non-exhaustive list of best practices which boards should consider. A summary of the best practice guidelines (the Guidelines) are as follows:

- 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.
- Cyber security should be a standing agenda item for discussion at board meetings.
- 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.
- A clear reporting line to the board should be established for cyber security incidents.
- 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, who has received

appropriate training on cyber security, should assume responsibility for cyber security matters.
- The board should satisfy itself that the firm has a procedure to deal with a successful attack and/or intrusion to its systems.
- Firms should have appropriate processes in place to verify the legitimacy of all requests, (such as redemption requests, change of bank account details and information requests) received via all methods of communication.
- Firms should ensure compliance with relevant client verification and anti-money laundering obligations when making a payment to a third party bank account.
- Firms should conduct stress tests at least annually to discover any vulnerabilities to their systems. Firms should consider appointing a third party cyber security specialist to carry out such an audit.
- Firms should satisfy themselves that the cyber security standards of the service providers that they utilise are comprehensive and that they minimise the direct impact to the firm should such a service provider be subject to a cyber-attack.
- Firms should report any successful breach or substantial attack to their systems to the Central Bank.

The Guidelines provide a valuable resource for fund boards in applying best practice in all cyber security matters. The Central Bank has indicated that they will have regard to the Guidelines in the event that a firm is not compliant with any relevant regulatory requirements. In addition to the Guidelines, fund boards should consider taking out a cyber security risk policy covering a number of areas including intellectual property, hacking, viruses, etc. The fund board should also consider disclosing specific cyber security risk factors in fund offering documents.

Conclusion

It is the board's responsibility to ensure that a firm is properly governed and has the necessary processes and systems in place to protect the firm and all of its assets. Cyber risk management should not be left solely to a firm's I.T. department but should run throughout the organisation and should include active involvement from the board. In addition, due to the requirement for fund boards and managers to delegate duties to third party service providers such as Depositaries and Administrators, fund boards and managers should look to ensure that such service providers have endeavoured to put robust processes in place to minimise the threat of cyber-attacks and ensure compliance with relevant legal obligations.

If you would like to discuss any matters in relation to cyber security, please contact any member of the Financial Services Team.

About the Authors