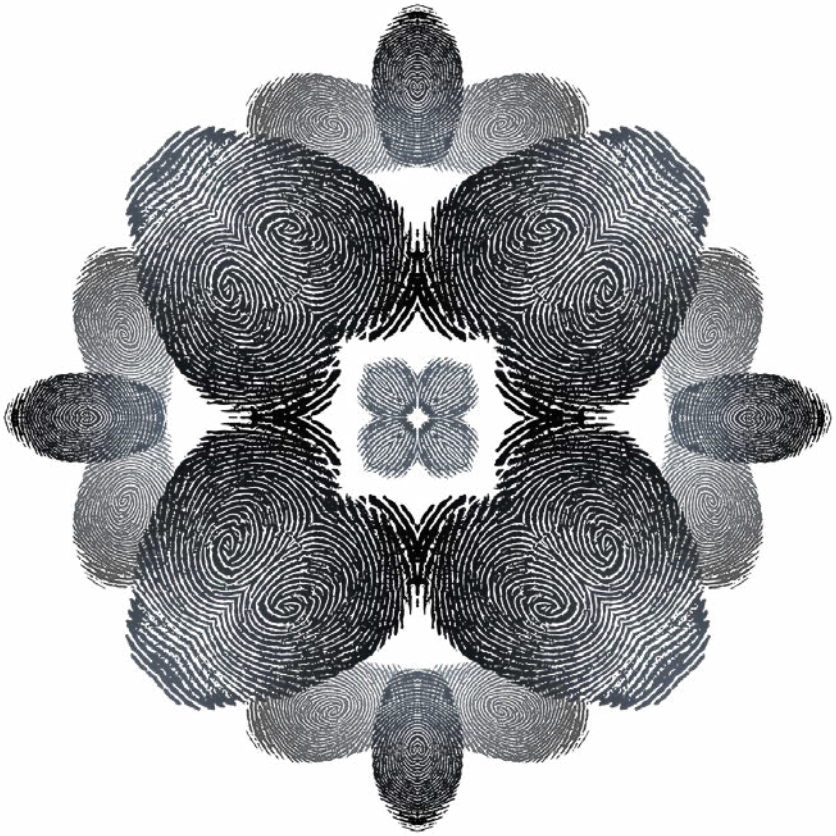
Deloitte.



Cyber security in the asset management sector

The recently published Central Bank of Ireland ('CBI') 'Dear CEO' letter regarding the Thematic Inspection of Cybersecurity Risk Management in Asset Management Firms follows on from the CBI's more general Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks published in 2016.

The March 2020 letter provides a number of observations regarding the preparedness of asset management firms based in Ireland to engage with and invest in proper cyber security. What is most striking from the CBI publications in 2016 and 2020 is the commonality of issues that have been raised and we have seen these same issues mirrored in the Risk Mitigation Plans that CBI has issued directly to firms in relation to Cyber Security.

Taking each of the CBI's points in turn, it's worth noting that there is a consistent theme in the six areas of focus – a better appreciation of the benefits of Cyber security within the firm.

Cybersecurity Risk Governance

The CBI is emphasising the need for the Boards and Senior Management of asset management firms to treat cyber security as importantly as any other area of the business. A good cyber strategy should in effect underpin and support the organisation's business objectives. Cyber is a risk as well as a business enabler. If a Board is unaware of a specific risk, then how can the Board be in a position to deliver its targets or even deal with the risk?

In essence the oversight required for Cyber security is no different to the oversight required for investment management for example. It is unlikely that a critical area of an asset management firm's business would be operated without oversight, hence the CBI is looking for similar oversight for Cyber security. Boards need to know where all their risks lie, and this includes IT and Cyber.

Cybersecurity Risk Management

In order to understand a risk, at first you must be able to quantify it. The use

of metrics in investment management and other areas of asset management highlight whether a decision has yielded the returns expected.. The CBI is indicating that the practice of quantification of metrics is generally not being applied to Cyber security. Correct metrics will provide a measure of reassurance that tooling/ asset management/ polices/ procedures are working for an organisation's cyber security maturity in the manner expected. These metrics can highlight areas of both strength and areas for development. For example, metrics relating to the number of users accessing a restricted system or the attempted access to that system can illustrate how successful access management and authentication services are performing or whether they require enhancement to meet a business' needs.

Even with metrics in place, the frequency of ongoing monitoring/assessment plays a key role in ensuring that the firm is keeping pace with security threats and developments. If assessments are conducted on a regular basis, the CBI intimates, that the Cyber risk will be as managed as much as it can. For asset management firms based in Ireland, who are part of a wider group of companies (as many are), it may be possible to leverage the ongoing assessment performed by a central Cyber team within the group. This approach and evidence of same should be documented.

IT Asset Inventories

In order to quantify risk, firms need to know their assets. In the case of Cyber security, these assets are in the IT space. The CBI has highlighted that the lack of an inventory of IT assets and one in a central location is a concern as it has the potential to give rise to a lack of visibility of risks and issues as they arise.

The reasoning behind the CBI's stance on the lack of visibility of the overall IT assets estate corresponds to the ability of an asset management firm to identify, to respond to and recover from a Cyber security incident. Additionally the lack of prioritisation of assets is highlighted because a firm may not be aware of what assets it actually relies on to keep its operations functional. This is particularly true in the event that the firm is relying on its group infrastructure.

The CBI suggests a holistic process that includes a review of the criticality of assets and a frequency review of the assets. In this way any deviation from baselines can be quickly identified and remedied.

Vulnerability Management

The CBI's highlight of vulnerability management indicates three key factors – inadequate vulnerability management, incomplete or unknown vulnerability scans and the inability to prepare tools to detect anomalies.

This would indicate not just a lack of appreciation of the impact of vulnerability management, but even more importantly a lack of user understanding as to the role vulnerability management plays in keeping asset management firms Cyber security safe. If a device is vulnerable, then an unauthorised third party may use it as an egress point to a network. If a company is unaware of a vulnerability then it is not in a position to defend its assets or potentially its business from unsecure devices that provide a platform for unauthorised third parties.

Security Event Monitoring

Event monitoring is a key component of any Cyber security program. It ensures that the assets and devices of an asset management firm are not only monitored by a security team but also alerts are sent to the firm in the case of an incident occurring, an alarm being tripped or unusual activity being detected. What the CBI letter indicates is that many asset management firms are not fully utilising the strength of a centralised security incident and event monitoring (SIEM) tool combined with the oversight and response of a security operations centre (SOC).

The use of an outsourced company, parent company, or centralised group function to manage these services is acceptable but asset management firms should ensure that service being provided meets their needs, is monitoring the correct assets and responds when the firm needs to and not when the provider wants to. Additionally the firm should have a view of their assets and be aware of the potential security threats that it faces.

The concern the CBI raises relates to the timeliness of response to incidents and the ability to understand when an incident, affecting your assets, has occurred.

Security Incident Management

The final comment from the CBI relates to Security Incident Management. This requires a governance framework, that if designed correctly, can be leveraged to deal with an incident expediently and also lend itself to recover operations in a managed manner. A robust framework with defined roles and responsibilities, that is tested on a frequent basis will provide a level of reassurance that if the worst were to occur, that the asset management firm can respond in a timely manner and resume normal operations as quickly as possible.

Conclusion

Examining all six areas of concern, the overriding thought is one of user appreciation of the role Cyber-security plays in supporting their business. If asset management firms appreciate that Cyber security can actually help their operations, rather than being viewed as a cost, then their security risks will decrease. This in turn will lead to more robust business that can withstand third party cyber-attacks as much as possible.

The effort to identity, quantify and rank assets and then to monitor these assets within defined parameters will be paid back in multiples if a security framework, with Board and Senior management oversight, is implemented and maintained on a regular basis. The use of outsourced providers for SIEM and SOC is only of benefit if an asset management firm knows its assets, knows its baselines and has visibility of events.

The CBI's Thematic Letter is timely in that in reminds the Industry that security is an enabler of a business and should be part of a company's culture. To ignore cyber security is to invite the unexpected, the unpredictable and the unknown to your door.

Contacts

Colm McDonnell
Partner | Head of Risk Advisory
cmcdonnell@deloitte.ie
+353 1 417 2348

Laura Wadding
Partner - Regulatory Risk
lwadding@deloitte.ie
+353 1 417 2934

Neil Redmond
Senior Manager
neredmond@deloitte.ie
+353 (0) 1 4175739

Dublin
29 Earlsfort Terrace
Dublin 2
T: +353 1 417 2200
F: +353 1 417 2300

Cork
No.6 Lapp's Quay
Cork
T: +353 21 490 7000
F: +353 21 490 7001

Limerick
Deloitte and Touche House
Charlotte Quay
Limerick
T: +353 61 435500
F: +353 61 418310

Galway
Galway Financial Services Centre
Moneenageisha Road
Galway
T: +353 91 706000
F: +353 91 706099

Belfast
19 Bedford Street
Belfast BT2 7EJ
Northern Ireland
T: +44 (0)28 9032 2861
F: +44 (0)28 9023 4786

Deloitte.ie

Deloitte.

MAKING AN IMPACT THAT MATTERS since 1845

At Deloitte, we make an impact that matters for our clients, our people, our profession, and in the wider society by delivering the solutions and insights they need to address their most complex business challenges. As the largest global professional services and consulting network, with over 312,000 professionals in more than 150 countries, we bring world-class capabilities and high-quality services to our clients. In Ireland, Deloitte has over 3,000 people providing audit, tax, consulting, and corporate finance services to public and private clients spanning multiple industries. Our people have the leadership capabilities, experience and insight to collaborate with clients so they can move forward with confidence.