10 KEY SECURITY CONSIDERATIONS

JAIME KAHAN OF **ERNST & YOUNG** RECOMMENDS 10 AREAS RELATED TO CYBER-SECURITY THAT FIRMS SHOULD FOCUS ON AS THEY OPERATE IN AN ENVIRONMENT OF CONTINUOUS AND EVOLVING THREATS

Jaime Kahan
is a principal at Ernst & Young LLP where she leads the wealth & asset management sector for information technology risk & assurance. She assists firms with their cyber-security programs, risk and control frameworks, service organisation control reports, benchmarking assessments, and financial statement audits. She also develops and delivers security, risk and technology training.

As the dangers posed by cyber-attacks continue to rise, and with financial services firms being increasingly targeted, the ability to prevent, detect, respond and recover from virtual attacks is of growing importance to the asset management industry. This has been further highlighted in the recent risk alert from the SEC's Office of Compliance and Inspection Examinations (OCIE). We have outlined 10 areas that we believe firms should focus on as they improve their security posture to protect themselves from cyber-attacks.

1. BOARD SUPPORT AND GOVERNANCE

Board support and governance is the first component of an effective cyber-security program. It sets the tone at the top, including policy approval. Executive support is needed to establish a clear charter for the information security function, strategy for its growth and funding. Since understanding cyber-risk is everyone's responsibility, asset managers are moving towards a collaborative approach by forming risk committees, which include representation from all the firm's key stakeholders.

Board members should take an interest in hearing about what you are doing to protect the assets. According to the EY 2013 Global Information Security Survey (EY Study), a third of the asset management firms said that they were never/rarely asked by the board to present on information security matters. Some board members also acknowledged that they did not possess the technical knowledge required. In these situations, boards should consider bringing in outside experts to ensure they are asking the right questions of their security personnel on a frequent basis.

2. POLICIES AND PROCEDURES

Firms should establish robust cyber-security policies and procedures. This would allow for a consistent approach to defining, communicating and implementing steps in managing cyber-security matters, as well as meeting regulatory requirements. Procedures should be detailed, step-by-step instructions for achieving the policies, and they will provide the blueprint for the day-to-day technology operations, including roles, responsibilities, tasks, hardware, application and process.

3. PEOPLE

Today's information security function requires a person with a broad range of skills as well as a clear articulation of roles, responsibilities and reporting lines. Relevant skills include an understanding of business/technology risk, knowledge in designing and executing technology controls that mitigate those risks, and the willingness to keep up-to-date with the latest technologies and potential cyber-threats. Technologists should also participate in forums with peers where information on the latest threats and potential solutions can be discussed.

According to the EY Study, 44% of asset managers indicated that the lack of skilled personnel was preventing them from implementing a successful security program. In these instances, firms should consider supplementing their team with vendors and training their own employees.

4. TECHNOLOGY

The threats firms face are evolving on a daily basis due to technological innovation, the increasing reliance on technology, and increasing number of access points to data (i.e. email, mobile devices, websites, laptops, etc.). Hackers have become more sophisticated and they exploit loopholes in technology. Firms need to keep up with software that is available in the market that can help with detection and monitoring. However, the cost of cyber-threat management can be daunting. If there are budget constraints, having the dialogue with board members and the risk committee can help to determine the most critical areas and prioritise resource allocation.

5. AWARENESS

The first line of defence against cyber-crimes is the firm's employees. By providing employees with security awareness training, a firm can make it more difficult for attackers to gain unauthorised access, and to identify phoney/suspicious activities more quickly. Training should occur at least annually, and followed up with periodic refreshers. Common areas of focus include: password security and composition, how to identify and report phony emails, protecting data while in public, effective use of social media, and protecting against the latest cyber-attack methods used to access confidential firm data.

It is important that your employees know what to look for and when something doesn't feel right, they have a responsibility to report it. Attackers typically gather information on a firm for seven to 12 months before an attack. Employee notification of a suspicious email is a warning sign that your organisation may be targeted and it can help you to take preventative measures.

6. ASSET INVENTORY

Firms need to be able to identify who has access and to what physical and electronic assets within the organisation. This would include but not be limited to laptops, computers, servers, software, iPads, mobile devices and electronic files.

In addition to managing user access, firms should consider maintaining an inventory of their electronic and physical assets so that all the assets can be backed up when an employee leaves the organisation. The inventory is also a way to account for lost devices such as mobile devices and laptops, which are more susceptible to theft. Firms must have a way to degauss lost devices and prevent unauthorised data access.

7. VENDOR OVERSIGHT

Organisations need to understand the security measures in place for their vendors, who has access to their data at each point within the transaction life cycle, from inception to recording, and that data is secured in transit, in use, and at rest. Firms need to determine what checks are in place to ensure that their vendors are protecting information and data assets with the same level of security controls that are adopted internally. Such vendor oversight is particularly important in the asset management industry as many asset managers outsource much of their middle and back office functions and processes.

8. CONTINUOUS MONITORING

The EY Study found that a third of respondents had spent more on cyber monitoring than in the past and had increased funding for the upcoming year. Types of attacks that firms monitored included: denial of service (an attack that makes a computer, website or service unavailable to users), spoofing (attacker impersonates another user), port scanning (attacker determines which servers are active), sniffing (capturing transmitted data such as password credentials) and compromised key attacks (a virus that records keystrokes made by the computer's owner).

Signature and rule-based tools that perform monitoring are no longer as effective in today's environment. Instead, information security functions may wish to consider using behaviour-based analytics against environmental baselines and have incident response plans in place. This allows companies to pinpoint any anomalies within their network and stay abreast of potential new threats.

9. REPORTING

Information security reporting requires a well-maintained enterprise event monitoring and incident/problem tracking and reporting system to manage events associated with business priorities and assess the true risk to the organisation. Creating metrics can help to quantify the firm's security posture as well as provide perspective on the firm's current threats, risks and actual breaches. By having a system or tool in place to document and categorise different security incidents, the organisation can perform trend analysis and identify potential attack patterns as well as the types of threats the organisation is most susceptible to. In addition, having reporting capabilities in place can help firms report security breaches to regulatory organisations when required.

Information that should be reported includes: the type of attack, tools utilised by the attacker, amount of time it took to detect the breach, processes impacted by the attack, number of impacted users and financial damage of the attack.

10. CONTINUOUS IMPROVEMENT

There is not a one-size-fits-all or operating model approach for a cyber-security program. As firms put cyber-threat management programs in place – they can't just be thinking about today, but what is coming tomorrow. Cyber-security programs need to have strong lines of communication and protocols in place, awareness, knowledge, and getting everyone working together so that your organisation can be quick and nimble to react to new threats. Firms are always trying to innovate to keep ahead of their competitors, but there needs to be an awareness of how such changes can impact your technology protection. Firms need to keep the lines of communication open – and ensure that they are constantly obtaining information on new threats and vulnerabilities from multiple sources such as industry events, peer discussion groups, newsgroups and security vendors.

By focusing on the areas above, firms will be able to improve their security stance and reduce risk. The more you know and prepare today, the better you can detect, respond and recover tomorrow and minimise the impact to your business. ■