26 May 2015

Press release

Cyber risk: It's more than just an IT issue for asset managers

Risk: a situation involving exposure to danger; the possibility that something bad will happen.

Asset managers know the definition of risk better than anyone. They've built their careers, businesses, and investor's wealth by understanding risk. Asset managers are constantly evaluating when to take risk, when to increase risk, and when to reduce risk. Advanced computer systems and analytical models evaluate risk by ingesting tremendous amounts of data and information. The best and most successful asset managers know the reward and the consequences of every risk they take, at least they do when it comes to investing in stocks, bonds, real estate, and other capital rewarding vehicles.

What about their investments in technology, infrastructure, relationships, employees, customers, and most importantly, their reputation?

Advances in technology, infrastructure capabilities, and the ability to move data rapidly across the globe among business units, third parties, vendors, and customers has driven strong growth for assets managers over the past two decades. These advances in technology certainly require a high degree of attention and monitoring. Over the years asset manager technology platforms were constructed with a "business first" mentality, and in a race to seize a competitive advantage. This fast paced approach has made systems vulnerable as security was not always a primary consideration for all companies during their construction.

Asset Management Director at PwC Isle of Man, Nichola Christison comments,

“The assets and information that managers control and possess are prime targets for a multitude of attackers; including organized crime, nation states, insiders, and competitors. These attackers have also benefitted from technological advances. Their tools and attack weapons have become more sophisticated and scalable. The ability to attack numerous targets globally and simultaneously increases the challenge to defend and respond. Addressing these challenges is best done by evaluating the risk in a similar manner to the firm’s evaluation of investment risk. The oversight and monitoring of the risk must be constant with processes to continuously gather and analyze information. The resulting analysis and intelligence will help identify threats to the organization and the targeted assets.

Furthermore, asset managers should conduct a business risk analysis in regards to cyber-attacks and the targeted assets. This type of risk analysis differs from the investment risk analysis because there is no upside, which makes it more of a chore. Managers take risk because they want a reward. The mindset with evaluating cyber risk is the protection of revenue and marching down a path towards becoming cyber resilient.”

Reducing cyber risk and increasing resiliency is achieved by making sure these discussions are included in the firm’s highest level risk discussions. The leaders of the firm, who are involved in the risk decisions on how to generate revenue, also need to be discussing how to protect critical information and revenue streams and the enabling business processes and systems. These are not solely information technology discussions, but rather they are broader risk discussions that involve debates about threats, likelihood and tolerance. Leadership’s understanding of the risks, threats, and impacts must be clear and routinely updated.

Steve Billinghurst, Director of Data & Cyber Advisory Services at PwC Isle of Man believes that the following actions should be taken:

Establish a Cyber Risk Governance Committee – similar to the firm’s investment committee, there should be an established organization overseeing cyber risk. The organization should have an official charter defining their scope, objectives, members, and roles and responsibilities. Key responsibilities include strategy, monitoring and reporting of risks and threats, and resiliency initiatives. The organization should also have defined reporting lines into their group, and from the group to leadership. All lines of business and information technology should be represented in the organization’s membership, and co-chaired by a business leader and IT leader.

Understand the firm’s critical business process and assets– as mentioned earlier, a responsibility of the Risk Governance Organization is defining a cyber-risk strategy. Strategy should begin with identification of the critical business processes and assets, and the impact on the organization if they are disrupted. This understanding will help

the governance committee guide collaboration between information technology groups and business leaders on how best to deploy resources to reduce risk and avoid "boiling the ocean" by trying to eliminate all current and future threats.

Threat Intelligence, Monitoring, and Reporting – understanding the threats and attacks targeted towards an organization are critical when evaluating the risks to the firm. Systems generate tremendous amounts of data and various logs on access and attempted access to the firm's assets. This information is often disregarded until an event occurs and a forensic activity is required. By then it may be too late. System logs should be captured and routinely monitored for suspicious activity and attempted attacks.

Build Resiliency and Response Capabilities – lessons learned from system log analysis, industry news, and past incidents will help an organization strengthen resiliency and build an effective incident response plan. Firms must shift the mentality from "if we are attacked" to "when we are attacked". There needs to be clearly defined plan on how to detect, respond and recover. The most valuable crown jewel for asset managers is their reputation. An improper, ineffective, or incomplete response to an attack may be unrecoverable.

Ends

Notes to editor:

For more information on building a cyber resilient financial institution, download the latest report from PwC.

Media contact:

Linda Jackson, PwC media relations, Tel: 01624 689 689. Email: l.jackson@iom.pwc.com

About PwC - Globally

PwC helps organisations and individuals create the value they're looking for. We're a network of firms in 157 countries with more than 195,000 people who are committed to delivering quality in assurance, tax and advisory services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.