Cyber security: The biggest risk to financial services?

The Central Bank of Ireland (CBI) recently undertook a review of the cyber security policies and procedures across investment firms, fund services providers and brokers. In this article (first published in Finance Dublin Yearbook 2016), **Padraig Kenny, Managing Director, RBC Investor & Treasury Services, Ireland,** discusses the scale of this increasingly sophisticated threat and what more the funds industry can be doing.

A wave of increasingly sophisticated and much publicised cyber-attacks on institutions of all types continues to make news headlines. Entertainment groups, retailers, insurers and even dating agencies have been targeted. Nobody it seems is immune. The effects of such attacks go much further than the tarnishing of an institution's brand and reputation, with the victims in most cases being the individual customers and employees. There is clearly an obligation for businesses to act, and why governments and regulators are voicing the need for increased defence.

The cost of cyber-crime has been estimated by Grant Thornton to be at least $315 billion a year[1] with the financial industry unsurprisingly being the most concerned over the threat. The sector continues to be the most frequently targeted by criminals. According to the cyber-security company Websense[2], it is subjected to 300% more attacks than any other sector.

Besides the obvious financial reasons for attacking banks and investment firms, the sophistication of their security makes them a tempting target for hackers who often undertake these activities for the thrill of the challenge. Concerned by this growing threat, the CBI recently distributed a questionnaire to investment management firms to assist them in designing robust cyber security policies for their operations.

Financial institutions around the globe have been adding thousands of skilled technology employees, placing them at the heart of their cyber-security infrastructure to detect, monitor and repel potential external threats to data. These individuals often possess atypical profiles compared to most financial services employees.

President Roosevelt said when appointing Joseph P. Kennedy to the Securities and Exchange Commission after the Great Depression that 'it takes a thief to catch a thief'. These words resonate significantly as; many financial institutions are seeking the services of former hackers who can identify the weaknesses in their cyber security defences.

With any technology system, the risk of it being compromised is increased if it is poorly designed or potential vulnerabilities have not been identified. For example, many applications that market participants may use are often added to incompatible legacy platforms. Security, as a result, can often be bolted on at the end of the process, rather than an integral part of the design.

> "President Roosevelt said when appointing Joseph P. Kennedy to the Securities and Exchange Commission after the Great Depression that 'it takes a thief to catch a thief."

The importance of taking cyber-security seriously was underlined in a recent report from Standard & Poor's (S&P)[3], which suggested that banks and other financial institutions may see their credit ratings cut if they fail to sufficiently protect themselves against cyber-attacks, or are subject to a damaging breach.

It is important that all financial services providers remain abreast of the latest detection and prevention intelligence. Ongoing investment in analytics capabilities is critical to enhance security models and ensure timely responses to any identified or potential data breach. However, that is only part of the answer. Going forward, S&P's evaluation of banks' credit ratings are expected to include a number of questions, including:

- How do you measure the exposure and report on cyber risk?
- Do you have a robust, well-documented program to monitor cyber risks?
- How many times was the business the target of a high-level attack during the past year, and how far did it reach in the system?
- How does the bank ward off phishing and diminish the likelihood of having data compromised from an internal breach?
- What's the internal phishing success rate?
- How long has it typically taken to detect a cyber-attack?
- What containment procedures are in place if the bank is breached?
- Are emergency scenarios test-run?
- What kind of expertise about cyberattacks exists on the board of directors?
- What are the bank's capabilities versus peers, and how are they assessed? Is there information shared with peers?
- Does the bank have any insurance to compensate for a cyber-attack?

> "Ongoing investment in analytics capabilities is critical to enhance security models and ensure timely responses to any identified or potential data breach. However, that is only part of the answer."

As the funds industry is required to collect and hold more data on investors, safeguarding the integrity of that data is becoming increasingly important. The industry needs to continue to make the necessary investments in hardware, software and people, while constantly educating their staff, to ensure its technology and expertise is appropriate and effective to defend itself and, fundamentally, its clients.

Padraig Kenny, Managing Director, RBC Investor & Treasury Services, Ireland.

1. Grant Thornton International Business Report, September 2015. 2. Websense Security Labs, 2015 industry drill-down report - financial services 3. Standard & Poors - How Ready Are Banks for the Rapidly Rising Threat of Cyber-attack?, September 2015

RBC Investor & Treasury Services

In the News

Cyber security: The biggest risk to financial services?

The Central Bank of Ireland (CBI) recently undertook a review of the cyber security policies and procedures across investment firms, fund services providers and brokers. In this article (first published in Finance Dublin Yearbook 2016), **Padraig Kenny, Managing Director, RBC Investor & Treasury Services, Ireland,** discusses the scale of this increasingly sophisticated threat and what more the funds industry can be doing.

Distribution Services | Securities Processing & Administration | Information Management | Transaction Banking | Optimisation