IIACACCVM
INVESTMENT INDUSTRY ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE DU COMMERCE DES VALEURS MOBILIÈRES

LETTER FROM THE PRESIDENT

Vol. 89

Blazing a trail: IIAC helps Member firms counter the global cyber threat

HIGHLIGHTS:

The six key elements of an effective cybersecurity plan

Board and CEO participation in cybersecurity plan is a must

First step in cyber risk assessment is to understand what company assets you are trying to protect and why

There are a number of controls that can be employed to protect firms' systems

IIAC provides a forum to discuss problems and solutions to the cyber threat, and has the tools and templates to assist firms

On November 9, 2015, I spoke to IIROC- and MFDA-registered advisors at the Distinguished Advisor Conference on the threat of cyber attacks on investment dealers and their clients. The purpose of the speech was to describe the sophistication and global dimensions of the threat, the serious consequences of such an attack, the financial and information losses to firms and clients, and potential reputational damage to firms and their advisors. The presentation also gave me an opportunity to explain the role of the Investment Industry Association of Canada (IIAC) in raising awareness and assisting Member dealer firms to put in place defenses to counter the cyber threat. All IIAC Member firms have moved to implement adequate cyber defenses.

The cyber threat and its consequences have generated considerable interest and concern for IIAC Member firms. The global publicity generated by cyber attacks (for example, the "sprawling" JPMorgan hack described in a November 10, 2015 article in the Financial Times) is a case in point.

What might a cyber attack look like?

My presentation opened with two real-life business examples. In my first example, all computers in a firm have seized up and the firm-wide computer system is under complete lock-down. The firm then gets a message that hackers have taken control of the computers and, without payment of funds, the system will not be unlocked and the confidential data destroyed or made public. This seize-up of systems and follow-up ransom demand is referred to as "crypto-lock". In the second example, a senior officer in the IT department of a firm notifies senior executives that the firm's computer system has been hacked with the breach occurring sometime in the past six months. The firm is faced with the monumental task of determining the nature of the computer security breach and, more importantly, the extent of the financial and data loss.

In both cases, the firms need a comprehensive plan to shut down the hack quickly, limit the damage to clients and the business, and to get the business back up and running. All firms, large and small alike, need to design a remedial plan in the event of a computer hack. Evidence shows both large and small firms are susceptible to a cyber attack. Large firms obviously present a bigger and juicier target, but small firms are perceived as more vulnerable to hacking. The remedial plan involves many actions and actors to identify the source of the breach, either through the firm's internal system or the system of a third party vendor. It requires: access to technical and forensic experts; an understanding of the extent of losses (who has been affected and what information has been compromised); legal advice to ensure liability and regulatory costs are minimized; a communication plan tailored for appropriate messaging and sequencing to inform clients, the regulators, law enforcement and insurers; and an appropriate and effective remedial plan to put the firm on a secure footing.

Elements of an effective cybersecurity plan

The cybersecurity plan of an IIAC Member firm should have roughly six key features:

1. Governance and risk management

The first feature is to have the full support, buy-in and participation of the firm's Board of Directors and CEO for a cybersecurity plan. A commitment to cybersecurity at the top of the organization is important to ensure key executives from all parts of the firm are involved in the cybersecurity strategy. The cyber threat is far too sophisticated and serious to relegate it simply to the firm's IT department.

Chart 1: Cybersecurity Incidents in Canada
% Change: 2015 over 2014

Source: PWC*

2. Risk assessment

The firm needs to identify its critical assets vulnerable to cyber attack. An effective plan can be built only if the firm understands what its "crown jewels" are and why they are vulnerable to cyber attack. The firm must assess the strength of its internal defenses or technical controls, as well as the controls of third party vendors with access to the firm's systems. This means the firm must undertake due diligence of third party vendors, to ensure it covers all system entry points to reduce the ways in which cyber-criminals can access a firm's systems.

3. Technical / Process controls

There are a number of controls that can be employed to protect firms' systems. The appropriate controls will largely be determined by the nature of the firms' business, the assets that it seeks to protect, the ways in which it interacts with external systems, and, of course, the firm's budget.

One of the most important security controls that should be employed by all firms is the encryption of confidential information to protect data on the system, in general, and on individual computer devices. Additional information protection also requires effective "access control", which is characterized by the layering of security measures for designated individuals to access confidential information. It also means restricting access to confidential information on a "need to know" basis. For example, lower rank employees do not need access to the most vital information on market trading algorithms and detailed client information, and, for that matter, neither does the CEO (who would often be targeted by cyber criminals by virtue of his/her title, and the access that it implies).

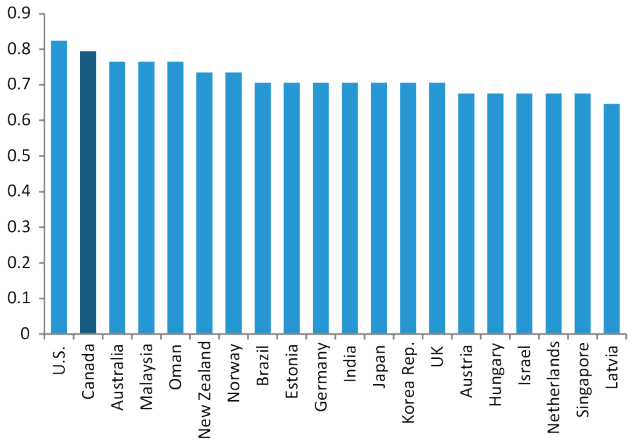
An important aspect of security control is managing the computer behavior of firm employees. Indeed, some cyber attacks have involved disgruntled employees, with Sony being an example. However, more likely cyber attacks typically target unknowing employees who end up being the dupes in a strategic attack. Emails that contain attachments with malware that can be embedded within the internal computer systems of the firm are sent to innocent employees, sometimes indiscriminately and sometimes deliberately. These emails are known as "phishing expeditions". The opening of these email attachments can inject malware into the computer system of the firm that can sit undetected for long periods of time, as the malware monitor and collect valuable firm information, and then activate to damage firms' systems, or release confidential information to the cyber criminals or the highest bidder. Staff must be trained to be vigilant for suspicious emails and instructed not to open them, if they arrive in their inbox.

4. Incidence Response Plan

It is probably inevitable, despite all precautions a firm can take, that it will at some point be the victim to a successful cyber attack. The detailed playbook outlining the steps that must be taken in the event of a computer breach is referred to as an Incidence Response Plan (IRP). The IRP assigns specific tasks to specific staff members and designated personnel with vendors, and sets out the sequence of tasks to be performed. If an IRP is not properly documented, much time will be wasted determining who should do what and when. Time is at a premium in the aftermath of a computer hack.

The Plan needs to be tested intermittently to ensure it works effectively and seamlessly across the firm.

Chart 2: Countries Best Prepared Against Cyberattacks



Source: ABI Research, ITU, Global Cybersecurity Index (GCI)**

5. Information sharing

Access to information on the techniques to bolster cyber defenses, and to understand the nature of threats to the investment industry, is valuable for the insights to help firms design and customize the appropriate cybersecurity plan to fit their needs. The most effective vehicle for information is internet-based information sharing platforms, typically focused on specific industries. One of the most popular platforms in the investment industry is the Financial Services Information Sharing and Analysis Center (FS-ISAC) platform which provides: i) real-time detailed information on recent cyber attacks and the response of the victims; ii) recommendations to implement an effective cyber plan, and offer best practices and protocols for effective response to a cyber attack; and iii)

access to in-house technical expertise for hands-on guidance.

6. Cyber insurance
Cyber insurance is compensation available for individual firms in the event of a cyber attack. The decision on whether to take out insurance, or the type of insurance appropriate for the firm, is complex and must take into account cost, the breaches covered by the insurance and the risk profile of the firm.

The role of the IIAC
The IIAC has undertaken several initiatives to assist Member firms address the cyber threat:

- More than a year ago the IIAC took steps to increase the awareness of cyber risks through discussions across various IIAC committees and working groups, and on the IIAC website.

- Throughout the past year, the IIAC has worked closely with the U.S. Securities Industry and Financial Markets Association (SIFMA) on the cyber threat agenda, particularly on ideas to promote industry awareness and specific initiatives that can assist dealers.

- In June 2015, the IIAC convened a well-attended cybersecurity conference that showcased a range of speakers knowledgeable about the threats and defenses to cyber hacking.

- The IIAC has established a new standing committee, the IIAC Cybersecurity Committee, to function as a roundtable for Member dealer firms to promote discussions on the cyber agenda, identify industry-wide initiatives to assist Member firms improve their cyber defense, and develop useful tools, such as best practices for an effective cyber defense and "check-lists" to carry out due diligence of third party vendors that provide cyber services to Member firms. The Committee also provides a forum for the industry to engage with regulators to develop appropriate guidance on establishing cybersecurity plans and procedures.

- In support of our members, the IIAC Board of Directors agreed to subsidize a one-year subscription to the FS-ISAC information sharing platform for our small and mid-sized firms. Members of the FS-ISAC worldwide receive timely notification and authoritative information specifically designed to help protect critical systems and assets from physical and cybersecurity threats.

- The IIAC is also currently negotiating with several technology vendors to provide industry discounts for important cybersecurity services.

Conclusion
The cyber threat to Member firms in the investment industry is serious, in terms of potential financial loss to clients and firms alike, the risk of exposure of confidential client and firm information, and the prospect of reputational damage to a firm. It is critical that all IIAC Member firms develop a comprehensive cybersecurity plan that protects the firm, and the assets and information of clients. An effective plan must have the full support of senior management and the Board of Directors, and full engagement of professionals right across the organization. Each firm will develop its own cybersecurity plan, customized to fit the particular risk profile of the firm.

The IIAC has a responsibility to provide the focus and resources to provide a forum for firms to discuss problems and solutions to the cyber threat, develop industry strategy and specific initiatives that include an industry awareness campaign, and tools and templates to assist firms. The IIAC will also bring together regulators and governments to work towards appropriate regulation and defense of the global cyber threat.

Yours sincerely,

Ian C. W. Russell, FCSI
President & CEO, IIAC
November 2015

*** Chart 1: Cybersecurity Incidents in Canada**
Source: Key findings from The Global State of Information Security®
Survey 2016 – Canadian Insights; October 28, 2015
http://goo.gl/VhSX32

*** * Chart 2: Countries Best Prepared Against Cyberattacks**
Source: ABI Research, ITU, Global Cybersecurity Index (GCI)
http://goo.gl/Ghbf84
Note: The CGI aims at capturing the cybersecurity commitment/preparedness of a country and not its detailed capabilities or possible vulnerabilities.