DATA AS HOSTAGE: PREPARING FOR CYBER THREATS

Steven King, director at Pershing LLC, explores the myriad of cyber threats facing the hedge fund industry today

As the world has grown more interconnected, so has the reliance on the flow of information. Stripped of the ability to interact electronically or unable to access internal data, most firms today would quickly be forced to severely reduce or cease operations entirely. This unprecedented pace and flow of information paired with systems and applications that require connectivity to function has heightened the awareness of the risks cyber-attacks present. For businesses of all kinds, interruptions of external information flow or breaches in internal information security have become critical risks that must be managed. While financial services have always been about managing risk, recent events are calling attention to the external risk presented by cyber-attacks. And in the data-intensive world of hedge funds, understanding and managing information security risk – which means managing data – has become a core requirement.

In case anyone doubted the gravity of the situation, The US Securities and Exchange Commission (SEC) announced in February that they plan to examine the policies and procedures asset managers have in place to prevent and detect cyber-attacks. Specifically, according to Reuters, SEC national associate director Jane Jarcho said: “We will be looking to see what cyber-security policies are in place to prevent, detect and respond to cyber-attacks [and] we will be looking at policies on IT training, vendor access and vendor due diligence, and what information you have on any vendors.”

Steven King

Steven King is a director for Pershing LLC, a BNY Mellon company, where he is responsible for the client technology subject matter expert team for the Prime Services and Collateral Funding and Trading businesses. In this role, he oversees the strategy for platform enhancements designed to meet the technology requirements of Pershing’s hedge and mutual fund manager clients and technology opportunities to expand the firm’s financing and securities lending platform.

The rapid expansion of information technology has thrown a harsh light on the state of hedge fund security. The fact is most organisations (in and outside of financial services) remain vulnerable to breaches, despite a doubling in spending on cyber-security in the last decade. According to Symantec’s latest *2014 Internet Security Threat Report*, 2013 saw a stunning 91% increase in targeted attack campaigns and a 62% increase in the number of actual breaches.

Financial services has long been a data-intensive industry. Complicating matters over the last dozen or so years – concurrent with the astonishing rate of miniaturisation of components housing data– has been the sheer speed with which transactions occur. It’s this reliance on data moving at light-speed that has ratcheted up the stakes when it comes to cyber-security for hedge funds more than any other factor. The advent of cloud computing for hedge funds is another factor that has heightened concern about data security.

Preparing for the most likely threats is informed by understanding what motivates hackers in the first place. Smash-and-grab hackers, who are in it for the sheer thrill of breaking in, grabbing whatever’s handy, and getting out, are less a threat to hedge funds than those who have specific goals in mind. Disrupting your business by simply selling critical data to the highest bidder or holding your data hostage for ransom remain the most prominent threats.

All this attention on external threats belies the most common cyber threat. Despite widespread perceptions of invaders lurking outside the gate, the principal threat may be from within. Firms that are too focused on outside threats can overlook an insider break-in, leading to theft of assets and intellectual property. Trading strategies, lists of holdings and cash positions, private investor-related data – much if not all of this is only a few keystrokes away for a staff member.

The sprawling adoption of personal mobile devices is another security factor. Take into consideration the mushrooming growth of BYOD (bring-your-own-device) in enterprises generally, and it’s no surprise that 38% of mobile users have experienced mobile cyber crime in the past 12 months, according to Symantec. The need to frequently work on the road and from home means employees are accessing sensitive data using personal devices that may not be sufficiently secure. Nonetheless, there are some things to keep in mind to lessen the chances of being exploited or at least limiting the damage caused by a breach.

Here are four categories of risk that require attention for hedge funds operating in today’s always-on, cyber active world, and insights on how to potentially remediate the risks:

1. Internal threats

Some of the most lethal attacks on a company’s computer network have been inflicted from inside a company’s walls. Perpetrators of these “inside jobs” can have a devastating impact armed with broad access to critical networks, systems and proprietary data of all kinds. To make matters worse, they can exploit the trust of their management and knowledge of company safeguards to avoid detection for lengthy periods of time. A well-known 2012 study funded by the US Department of Homeland Security, the CERT Insider Threat Center at Carnegie Mellon University's Software Engineering Institute and the US Secret Service, revealed that malicious employees in the financial services industry elude detection for nearly 32 months before they're caught. Common sense controls can reduce the risk and limit damage when inappropriate access occurs:

a. Have a strong internal security policy that awards access by role and has procedures for associates who change roles or leave the firm.

b. Regularly police all network share access. Keep common areas uncluttered.

c. Automatically disable any access that has been dormant.

d. Limit or eliminate removable writable data devices.

2. Friendly frauds

Most people like to be helpful, particularly in cases where little effort is required to do so. That simple fact of life can be a potent weapon in the hands of an external intruder. The classic ruse combines a spoofed email address (one that appears to come from your own organisation), an attachment or external link as part of the message, and a simple request such as: "Our local printer is down. Would you mind opening and printing this document for me? I'll come by shortly to pick it up. Thanks!" In this case, the commendable impulse to help a colleague can unleash a nasty virus, or worse. Taking precautions on email content and educating your associates on phishing methods can help avoid opening the gates to an intruder.

a. Train staff to never evoke a link or execute a file unless you know the sender and are expecting the communication. Delete suspicious emails.

b. Alert staff to look for contact information on mail from unknown senders, no contact information is a red flag.

c. Always think twice before providing any information in response to an email, especially from unsolicited emails.

3. The BYOD challenge

Embracing innovation while maintaining control introduces all kinds of challenges for businesses struggling to manage the bring-your-own-device (BYOD) trend. Users are increasingly using their own devices – from iPhones, Google Android phones and iPads to a flood of other devices – as they would use their PCs.

All of which means that the flood of devices turning up in workplaces are opening up another potential gateway for attackers. Striking the right balance between a complex mix of technologies and corporate IT policies is a never-ending challenge.

a. Implement a policy for erasure of firm data on private devices.

b. Eliminate associate use of guest or visitor accounts on Wi-Fi networks.

c. Require a kill switch for lost or stolen devices and an appropriate level of encryption.

> "A safe and secure track record in the face of today's IT threats starts with a culture that actively promotes best practices in all areas of network and data security. Being prepared is a full-time job when it comes to cyber-security"

4. Outside the "Wire"

It is essential to provide precise, comprehensive guidelines covering internet usage, acceptable use of firm email, so-called secure file, sync and share services, such as Dropbox, and social media sites such as LinkedIn and Facebook. Those responsible for IT and cyber-security need to ensure that firewalls, anti-virus software (security infrastructure) are up-to-date.

a. Block sites that have no business purpose. Social media sites should be the purview of associates responsible for the firm's communications.

b. Enforce TLS compliance on all vendor and client communications where confidential information is passed.

c. Require updated anti-virus and personal firewall software for any remote connections to the firm's network.

A safe and secure track record in the face of today's IT threats starts with a culture that actively promotes best practices in all areas of network and data security. Being prepared is a full-time job when it comes to cyber-security. That begins with a comprehensive understanding of these threats and what you can do to defend your business, your investors, and all of your stakeholders. The best news; you are not alone. Resources abound for help with cyber-security. As a start, get a vendor to perform internal and external vulnerability scans against your infrastructure. They are relatively inexpensive and can help guide you towards a plan to mitigate your weakest areas. ■