FOCUS ON

CYBER SECURITY

Marc Songini, of Intralinks, talks to *HFMWeek* about the growing need for hedge fund managers to acknowledge the severe risks posed by cyber-attacks

Marc Songini has worked in the information technology field for many years as a journalist, analyst and marketing communications specialist. During his 10 years with International Data Group (IDG), Songini wrote for Network World and Computerworld, both award-winning magazines. Currently, he is lead writer for corporate communications at Intralinks.

In the past two years, hackers have penetrated a number of hedge funds, according to *The New York Times*. To what degree is unclear and, regrettably, it's not surprising, as hedge funds are ideal targets for hackers. These enterprises represent billions of dollars and they all too often have inadequate security to protect their assets.

As experts note, hedge funds have spent, individually, many thousands of dollars to take their operations online and to automate them. However, they haven't sufficiently invested in anti-hacking and other security technologies, or in the proper training of staff in best practices that support cyber security.

We can easily imagine how the cost of being hacked and losing data would be catastrophic to a hedge fund manager. A successful network penetration could mean the loss of reputation and clients, as well as official sanction and lawsuits. Despite the enormous risks, many in the business tend to think all is well as long as someone else is hacked, and not oneself.

However, you can safely assume that after information is created and out of your hands, it will live forever. It will exist in some version, and not necessarily catalogued or protected. So how are you to protect your client information – to say nothing of your intellectual property?

BETWEEN THE NSA AND HACKERS

First, some background. Increasing amounts of data must be moved around in the cloud, as well as in controlled and secured corporate networks. To remain competitive, fund managers (just like similar professionals in other industries), have a growing number of audiences to communicate with for marketing and collaboration, or for regulatory purposes.

So to begin, you should consider where you might be facing exposure. Potentially sensitive data types include:

- Your clients' IDs, social security numbers, and bank and custodial account information
- Your 'secret sauce' – the investment strategy data that makes you successful

The recipients of the data sent include: administrators, prospects and clients, state or federal regulators, vendors and colleagues. They are often geographically distributed and there is no way for you to know the relative strength of each network and server that will house the data.

With the proliferation of shared information and its wider distribution, the risk of their exposure increases. We never know who is sniffing at it; as indicated by the revelations about official surveillance from Edward Snowden of the National Security Agency.

For retailers, as well as for Wall Street and beyond, hacking is a runaway problem. As the *Washington Post* reported last spring, the federal government notified 3,000 businesses they'd been hacked in 2013. Each week there seems to be another announcement of a major penetration – to cite one of the bigger ones, we need only name Target Corp, which lost records on 40 million payment cards. Subsequently, that amount was exceeded by The Home Depot Inc, which possibly had 56 million records compromised.

Network hacks are occurring constantly, and if anything, the problem of cyber-theft is underestimated.

THE CONSEQUENCES OF BREACHES

As we mentioned earlier, a hack would most likely result in the loss of clients and the ruination of the business. Today, it's reasonable to assume existing and potential clients will begin to demand a baseline of hardened security. Only then will they begin entrusting their assets and their private information to hedge funds. The increased frequency of operational due diligence procedures by sophisticated investors means security and related safeguards will be under review.

THE GOVERNMENT IS TAKING A HARDER LINE

Breaches are becoming less and less of a private matter. The Securities and Exchange Commission is pushing for more disclosure of data breaches. In fact, the agency is reportedly investigating multiple companies that were hacked, to find out if they had adequately guarded their data. As part of its investment adviser examination program, the SEC has promised it will conduct a review on the policies and safeguards asset managers have in place, to mitigate the risks of cyber-attacks.

Some areas where hedge funds are, or will be, reporting about to the government include:

- Form ADV basic firm and fund information
- Form PF portfolio information
- AIFMD Annex IV reporting for EU member states with detailed portfolio information (scheduled 2015)

HEDGE FUND MANAGERS DON'T KNOW HOW TO RESPOND AND PREPARE

As hedge funds' assets have swelled, many managers' operations and infrastructures are still playing catch-up. Hackers know this and have devised a number of targeted methods designed to access and capture a firm's most sensitive data.

They attack by:

- Hacking a broker's account to steal user names and passwords, and then trade securities using the victim's ID
- Denial-of-service assaults (DoS attacks)
- Using ransomware to lock down data until a bribe is paid

Securing IT infrastructure is now a requirement, not an option. Managers must double-down and commit more resources and focus to data security. Making this task more complex is the fact that, frequently, IT operations

are outsourced, so managers must be ready to demand documentation from their service providers.

HOW TO PREPARE

Cyber security is now of growing concern for many hedge fund firms. You don't want to be left behind, given that hardened security will most likely prove to be a competitive advantage. Regulators and clients are going to press managers to offer the most ironclad assurances that their data is as secure as reasonably possible. We recommend you start by changing your mindset.

Remember, success and growth aren't just matters of managing investments. They are also about prioritising your IT, operations and security. You need to begin examining your approach and to collaborate more closely with your IT personnel or service provider to make security as strong as possible.

A useful way to look at cyber security is to identify potential risks in your networks and data storage systems in advance. Some checklist specifics:

- Educate yourself. Learn about the importance of security, data privacy and compliance
- Do a deep risk assessment dive. It's impossible to forecast and mitigate data privacy risks without knowing all of the technologies your organisation employs
- Keep track of your assets. Organisations should keep detailed logs of all activity around their data.
- Ask yourself: are the basics in place, such as antivirus or monitoring applications? Besides the basics, you also need to see where else you must make improvements
- Evaluate your collaboration assets. Make sure you use the most suitable and secure (and easily adoptable) work apps.
- Consider vulnerabilities that might arise during remote customer access sessions, or when there is a fund transfer request
- Ask yourself: does my current vendor or homegrown system come up lacking?

> "CYBER SECURITY IS NOW OF GROWING CONCERN FOR MANY HEDGE FUND FIRMS. YOU DON'T WANT TO BE LEFT BEHIND, GIVEN THAT HARDENED SECURITY WILL MOST LIKELY PROVE TO BE A COMPETITIVE ADVANTAGE"

- Proactively learn how to detect suspicious network activity
- Review how you interact remotely with third-parties
- Define best practices for security and confidentiality and establish a procedure for internal governance that ensures compliance to these guidelines
- Train your employees in these best practices, such as when and how an employee accesses or shares a customer record
- Think about protecting information, both at rest and in transit. High-level advanced encryption standard (AES) protection is desirable
- Shop for the right tools
- Pick your partner wisely: Working with responsible and knowledgeable vendors can ease your burden – a poor partner can make the load much heavier
- Get down to the document level. Any vendor worth its salt must provide centralised visibility and compliance monitoring capabilities – for the lifetime of every document you own.

TAKE YOUR DATA AND APPS SERIOUSLY

Remember, as a steward of investor capital, safeguarding your clients' information is your responsibility; the burden is on you. Start now. ■