FUNDfire

May 11, 2016

Opinion

Alts Managers Must Prep for Cybersecurity Battles Ahead

May 11, 2016

Alberto Yépez
Alberto Yépez is a managing director of Trident Capital Cybersecurity

If there were any questions about the wisdom of the **Securities and Exchange Commission** making cybersecurity a focus of its audits and exams of hedge funds, private equity firms, real estate funds and similar financial businesses in 2016, they were surely answered by the Panama Papers episode.

What was one reason for the hack of the law firm at the center of the leak? Reports have surfaced that its email client had not been updated for years and that its client portal had more than two dozen vulnerabilities.

The case clearly underscores the thinking behind the heightened cybersecurity focus at the SEC, which two years ago began warning asset managers, private equity firms, hedge funds and others to more effectively manage these risks.

Cybersecurity for Alts Managers: The Must-Do List

1. Analyze your internal systems and communications environment, perform a gap analysis, address vulnerabilities, and create a cybersecurity breach policy.

2. Build greater cybersecurity awareness for every employee. Use simulation tools and services to teach them how to manage cyberattacks.

3. Establish security procedures for employee activity outside of the office. Are employees following your cybersecurity procedures with their systems at home, at client or remote work sites, and on their smartphones, tablets, and laptops?

4. Encrypt all company data stored or transmitted on smartphones. It's not important to have an encrypted smartphone, but the data must be protected.

5. Know the companies providing strong cybersecurity products and services, such as specialists that can encrypt data in mobile devices, streamline internal security operations, enable e-signing for transactions, or provide outsourced cybersecurity services.

Source: Trident Capital Cybersecurity

Hedge funds and other alternative investment firms are under pressure to make the most changes of all, partly because – unlike many other institutions – they appear to not yet have been seriously breached, at least according to news reports, and have not been forced to become serious students of cyber warfare.

But digital security firms say hedge fund cyber-attacks have finally started to rise as hackers realize there has actually been nothing special about the protective measures at these firms – and that hedge funds and private equity firms control significant amounts of money and sensitive personal information about their investors.

Alts managers face a particularly complex cybersecurity landscape because in addition to the cyber-risks within their own operations, there is risk from the connections to their investors, portfolio companies, and service providers. And hedge funds, private equity firms and others know that a breach could cost millions of dollars and easily spark massive litigation.

Fund managers must take a number of steps to address the challenge, but perhaps most important is the need to create a culture attuned to the importance of cybersecurity precautions. A strong security culture is both a mindset and mode of operation integrated companywide into day-to-day thinking and decision-making.

Good cybersecurity technology cannot work independently from user awareness, policy guidelines and the sharing of information about threats. Developing this kind of culture intertwines security practices with business operations and demonstrates that security is not a function relegated to an understaffed and underfunded information technology department.

In addition to establishing this culture, hedge funds and other alternative asset firms must take specific steps to protect client data. In this vein, the SEC has distilled the National Institute of Standards and Technology Cyber Framework down to six focus areas reviewed during Office of Compliance Inspections and Examinations (OCIE) exams:

• **Governance and risk assessment** - the SEC wants to see a formal plan of action for how your firm addresses cybersecurity risks.

• **Access rights and controls** - examiners will look at the basic controls in place to prevent unauthorized access to your network.

• **Data loss and controls** – OCIE staff will want to see a disaster recovery policy and procedures.

• **Vendor management** - the SEC wants to know how you select vendors and how you monitor their access to your network.

• **Incident response** – you must show the examiners how your firm plans to respond to a specific cyber-attack, with a focus on the key steps of identification of the threat, data collection on the event, and a description of action steps after a breach.

• **Training** - managers need to make sure every employee and vendor representative understands cyber-risks and embraces installed security measures.

Of all these steps, training is most important. Fund manager CEOs must be willing to evaluate every employee, including themselves. Cybersecurity is typically weakest at the individual user level.

For a firm to protect itself, the effort needs to start from within. Every employee or vendor partner must be told what behavior is expected to protect the network, how to identify a breach and what to do if they think a network has been penetrated. This includes establishing protocols outside the office. Are employees following security procedures with their systems at home and on their smartphones, tablets and laptops?

Overall, the security-minded investment firm must ask four key questions: 1) Have all employees received training? 2) Do they understand the importance of security precautions? 3) Are the CEO and management team holding themselves accountable to the same level of awareness and security? 4) Has the security posture of the company become accepted as second nature?

The SEC's stepped-up enforcement of cybersecurity measures is more than welcome. The global cost of cyber-crime has reached an estimated $450 billion annually. It would be folly for a fund manager to not do everything possible to avoid becoming the next poster child of cyber-crime unpreparedness.