Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Financial Firms' Worst Mistakes With Cybersecurity

By **Carmen Germaine**

Law360, New York (August 21, 2017, 10:55 PM EDT) -- Although the U.S. Securities and Exchange Commission said earlier this month that broker-dealers, investment advisers and funds have improved their "cybersecurity preparedness" in recent years, it found a majority of firms still had issues.

The findings came in an Aug. 7 risk alert released by the SEC's National Exam Program detailing observations from its exams of registered firms, and were mirrored in survey results released last week by Cipperman Compliance Services.

Cipperman found that 57 percent of surveyed alternative managers — a category that includes hedge fund and private equity fund managers — felt their cybersecurity policies didn't meet regulatory requirements.

While broker-dealers were more certain their policies passed muster, they were less sure about their programs overall, with 64 percent saying they weren't confident in their respective firms' cybersecurity.

John Araneo, managing director and general counsel of Align Cybersecurity, said he's seen many investment advisers and broker-dealers who wait to "jump into the cybersecurity pool" out of fear they'll immediately find deficiencies.

"When you approach cybersecurity, there's an apprehension that, 'I almost don't want to open the door because I don't want to see what's in the closet,'" Araneo said. "That's very shortsighted, and it's only going to get you into trouble."

Seward & Kissel LLP partner Marlon Q. Paz, who previously served in the SEC's Division of Trading and Markets, said financial firms face particular risks that make cybersecurity especially important. While data breaches or incidents in other sectors like retail can lead to financial losses if customers' credit card information is stolen, hackers that breach a broker-dealer or investment adviser get direct access to client assets, he said.

"The issue of safeguarding and protecting other people's money is paramount," Paz said. "That's not the same in other industries."

With that in mind, here are some of the biggest mistakes firms in the financial industry make with cybersecurity.

Their Systems Aren't Tailored

The failure to reasonably tailor cybersecurity policies and procedures topped the list of issues the SEC identified in its latest sweep, and experts said they've noticed just such ill-fitting practices at many broker-dealers and investment advisers.

Among other things, agency staff said they observed policies that gave only general guidance, were narrow in scope, or gave confusing instructions, including policies governing remote customer access to accounts that contradicted instructions for investor fund transfers.

The alert illustrates that firms can't just buy a cookie-cutter cybersecurity program off the shelf, Paz said, as untailored policies will not protect firms from their particular risks.

"I feel like there's too many snake oil salesmen, just saying, 'Here, I've got a nifty policy that's been reviewed and vetted by the SEC,'" Paz said. "That doesn't matter a bit — it's got to be tailored for that business."

Araneo said the risk alert also illustrates that the "devil was in the details," as the SEC faulted firms both for failing to customize their programs and for failing to follow through on cybersecurity plans. The agency noted, for example, that some firms that required annual customer protection reviews conducted them less frequently, while others that required ongoing reviews to see if additional security protocols were needed performed those reviews "only annually, or not at all."

"It can't be a one-stop, buy this policy, buy this technology, hire this person and stop there — this really is an exercise that needs to cascade through the entire enterprise and involve different employees or at least different functions," Araneo said.

To design policies that are adequately tailored to fit the firm, experts said, broker-dealers and investment advisers need to perform a deep risk assessment to identify exactly what the procedures must address.

An assessment will help a firm focus its limited resources and personnel, so that written procedures are followed in practice, said Mayer Brown LLP partner Jeffrey P. Taft. But the assessment has to focus on the firm itself and its unique systems, customer base and other potential risks.

"Taking someone else's risk assessment or looking at the risks applicable to other companies doesn't do you much good," Taft said.

Their Plans Are Too Long

In addition to broader cybersecurity policies, experts said firms need incident response plans with instructions on how to deal with an unauthorized intrusion — but the SEC said more than one-third of examined investment advisers and funds didn't have such plans.

"We've seen many organizations that have been caught flat-footed, don't have a plan, and when an incident happens they don't know what to do," said Robert Prucnal, the president of Cipperman Compliance Services.

Of plans firms have implemented, many are too long to be of use in a critical situation when employees need to know exactly who is in charge of what part of the response, Stroz Friedberg Managing Director Chad M. Pinson said in a panel discussing cybersecurity at the SEC's National Compliance Outreach Program for Broker-Dealers in July.

"All the IR plans I see look like a Stephen King novel where they were being paid by the word to write them," Pinson said. "You cannot use those things in an emergency, they are completely unusable."

Instead, firms need to draft simple plans that delineate which employees are responsible for which aspects of the response, and update the plan regularly to ensure details like contact information are accurate, said Erik Rasmussen, North American cyber practice leader for the cybersecurity and investigations practice at risk consulting firm Kroll.

They also need to define clearly when the response plan will be invoked. Triggering the plan in too many scenarios, Rasmussen said, could create "noise" and make it harder to respond efficiently to a larger crisis.

And while there's no such thing as a perfect plan, Rasmussen said, firms can get closer by practicing incident responses regularly to simulate the real conditions of a breach or other attack.

"Everybody has a plan until they get punched in the face," Rasmussen said.

Their Vendors Aren't Vetted

As firms identify the weaknesses and vulnerabilities their cybersecurity policies need to address, experts said one area many overlook is the risk that lies outside their doors, with third-party vendors and service providers.

"A lot of investment firms, a lot of Wall Street firms, spend time on their own systems, but then give access to third-party providers who create vulnerabilities," Paz said.

Paz noted that vendors and service providers like document review teams, outside counsel and consultants often have extensive access to their clients' systems and the information therein. If an employee at a provider leaves their laptop on an Amtrak train, Paz said, whoever picks up that computer can then get full access to the firm they were advising.

Indeed, many hacks and breaches have occurred because a vendor providing some kind of access to another firm was hacked, Taft said.

"It's imperative that companies do something with respect to those weak links," he said.

The issue is especially important because broker-dealers and fund managers have legal and regulatory obligations to protect the types of client data frequently stored at outside service providers, Araneo said.

To safeguard that information, firms need to reach out to vendors to ensure they have standards in place that meet expectations — a conversation Araneo said has thankfully become easier in recent years.

“The industry as a whole and the vendor community now understand what the advisers and the broker-dealers are asking, so they’re sort of getting their own cybersecurity controls in a language that people can share,” Araneo said. “That part of vendor management has been made a lot easier to accomplish.”

Their Employees Aren’t Trained

Even if firms have secured and protected access points from all their third-party vendors, experts said they’ll still be vulnerable if their employees are clicking on every suspicious-looking message that lands their inbox.

“Employees are human, and as long as employees are human they’re going to make mistakes,” Taft said. “Clicking on links that they shouldn’t click on, sending money or responding to emails that they shouldn’t respond to.”

Araneo noted that the “human element” is typically the weakest link in an organization’s cybersecurity, especially in investment firms where regulatory transparency requirements can facilitate hackers. For example, Araneo said, the Form ADV filed by investment advisers with the SEC contains much of the information needed to begin a phishing campaign.

With the addition of social media, Araneo said, would-be hackers can use LinkedIn or Facebook to identify targets or discern when points in an organization might be vulnerable, for example if key employees are on vacation. Together, that information allows hackers to manipulate a firm’s employees with tailored phishing campaigns.

“We’ve seen a high sophistication and effective rate of those types of attacks,” Araneo said.

As part of that training, Rasmussen said, firms should be making security “run through the fabric of the company,” so that cybersecurity becomes an everyday thing and employees know they have an important role to play in keeping their company secure.

“It can be very daunting to people, or [they can be] very dismissive because they look at it as an inconvenience rather than a part of their daily routine,” Rasmussen said.

At the same time, Paz said, firms can’t focus on lower-level employees to the exclusion of the C-suite. He said that while the high tech aspects of cybersecurity are often handled by younger staff, executives need to also be aware of and trained in cybersecurity issues to set the right tone at the top.

“They need to give it high importance, if for no reason than the fact that their entire business could perish as a result,” Paz said.

--Editing by Mark Lebetkin and Pamela Wilkinson.
