IAWatch
WEEKLY BRIEFING
COMPLIANCE NEWS, GUIDANCE & BEST PRACTICES

INSIDE...

February 6, 2017

Final part of a series

Time matters if your firm finds itself under a ransomware attack

Bruce Leibstone lives cybersecurity, so when he received an e-mail recently from **Verizon** alerting him that there was urgency that he click a link and sign into his account, skepticism washed over him.

Such "phishing" lures often entice an employee. One click could bare your system to cyber treachery, including the encrypting of your sensitive data that could prompt the hostage-taker to issue a ransomware demand: your money or your data.

We've shared five steps to take when you suspect you're a cybersecurity victim in part one of this series (**IA Watch**, Dec. 15, 2017). Now we focus on what to do when you're under a ransomware demand (**IA Watch**, Nov. 19, 2015).

Fly into action

First, know you have "only minutes" to act, says Leibstone, who runs the cybersecurity consulting firm **Warren Systems Group** in New York.

"Rip their network cable out of the wall. Turning the machine off is not enough," he says of the employee's computer that unleashed the attack. If you're fast enough, you may limit the damage to that one device.

The way a ransomware attack works is once the malicious software latches onto a network, it sends a message back to home base and retrieves "an encryption key." Then the data on the system – file by file – gets

(Squeezed, continued on page 5)

What's hot on OCIE exams

Ask examiners if news of your exam will reach your clients, then make a decision

Words are powerful. Take the custodian that, when notified that OCIE examiners were conducting an exam of an investment adviser, sent correspondence to the IA's clients noting that the **SEC** was "investigating" the firm.

"That was somewhat problematic," says **Michelle Martin**, CCO at **Longfellow Investment Management** ($8B in AUM) in Boston. A couple of clients called. The words "conducting a routine examination" may well have better fit the situation.

The IA relies on 30 custodians and only one used that unfortunate wording. She draws a lesson for other advisers: "Let your clients know that they may get a request from the custodian regarding an exam," said Martin, who spoke during **IA Watch**'s Jan. 24 webinar *Red Hot SEC Exams Topics*.

(Exam Activity, continued on page 2)

Sample the many ways your peers raise their compliance flag at their firms

Out of sight, out of mind, goes the old phrase. Your peers try to combat this notion by keeping their colleagues constantly thinking about compliance.

Having fun along the way doesn't hurt.

At quarterly staff meetings, **Thomas Knipper** addresses hot compliance topics and hands out "an incentive pep talk award," says the VP/CCO at **Ameritas Investment Partners** ($12.2B in AUM) in Lincoln, Neb. The winner, selected through a drawing, receives such prizes as wireless ear buds, a Bluetooth speaker or a remote battery charger. The award serves the dual purpose of showcasing that "technology is important to compliance," says Knipper.

But there's a catch. Knipper holds a drawing only if the staff has 100% complied with submitting on-time compliance reports. The game works. Only once in more than a year has there been no drawing at one of the quarterly meetings, he says.

A new compliance attention-drawing tactic tried by

(Wave Your Flag, continued on page 3)

Exam Activity (Continued from page 1)

By contrast, **Hamilton Lane** ($252B in AUM) in Bala Cynwyd, Pa., decided not to alert its private equity clients to its year-long OCIE exam in 2016, said **Fred Shaw**, the firm's director of compliance.

One reason was because of the nature of Hamilton Lane's clientele and its business model, and also because examiners "made it clear they were just going to speak only to the custodian" not the investors, says Shaw.

Another lesson from the two experiences is to ask your examination team if it will attempt to contact investors and then decide if you wish to notify your clients beforehand.

Prepare a presentation now

A New York CCO tells of the firm's recent exam, and the challenge in getting examiners to comprehend its business model. The takeaway: Devise a cogent presentation for examiners that would clearly explain your business model and do this long before they show up, says the CCO (**IA Watch**, Sept. 29, 2016; video).

Another New York firm created "first-day memos" that feature a synopsis of the firm's approach to regulatory compliance along with prep questions for staff. The firm's compliance officer will use them to prep senior managers for examiner interviews, to "get a feel for whether they're actually prepared to respond" to the real thing, says the officer.

The firm has also set up a system designed to be able to speed response to an OCIE document request letter. The firm has used recent document request letters as examples to identify "who owns what" documents and how quickly they could be gathered. [**IA Watch** offers many examples of document request letters. Click here to see them].

Shaw used a similar approach and it paid off in his exam. "Preparation can put you so far ahead of the game," he said. Examiners would go on to request more than 200 items.

Fortunately for Hamilton Lane, the firm had also recently hired someone to conduct a mock exam just before the real thing occurred. By contrast, Longfellow's Martin hadn't taken some of the steps that Shaw did, so when examiners called and then sent their request letter, "it was all hands on deck during those two weeks to prepare the data for the SEC," she noted.

A move that did pay dividends for Martin was the creation of mini-booklets to educate examiners on the firm. "We had presentations for every single interaction we did" with examiners, she said. "It helped guide the conversation and the staff seemed to respond very positively to those presentations."

On being organized

A CCO at a New England advisory firm found that maintaining identical folders – one electronic, the other paper – numbered to match the examiners' request letter aided its exam, which concluded with no findings. "I think having everything in hard copy, easily retrievable, was huge," says the CCO.

Examiners poked around a number of topics: **cybersecurity** (the firm pointed to its P&Ps); **whistleblowers** (they wanted to ensure the firm didn't discourage them); **personal trading** (have proof of your reviews); **disaster planning** (show you have tested your plan); **outside business activity** and **staff designations**.

"They were big on designations," says the CCO. "They went to the **AIF** site and did some background checking" on the designations, the CCO adds.

(Exam Activity, continued on page 3)

IA Watch.com's Compliance Corner

Don't miss our Compliance Toolbox. It's easy to find tools-you-will-use. You must be logged in to www.regcompliancewatch.com to retrieve items in the **IA Watch** Compliance Toolbox. **TIP**: Never click "Log Out" at **regcompliancewatch.com** and you'll never have to reenter your ID and password. You'll be able to click straight to any item. Use our search box at **IAWatch.com** and put in the name of each tool listed below or click now directly to each one if you're a reader of our PDF version:

Compliance Alerts at regcompliancewatch.com

You decide. Pick a compliance topic that interests you, set your compliance alert and get notice of news on that topic. Go to **regcompliancewatch.com** to set your alert.

1. Performance Advertising Example
2. OCIE's Exam Priorities
3. Marketing Approval Form
4. SEC Document Request Letter
5. Personal Trading Report ■

Exam Activity (Continued from page 2)

Make sure you have a process that documents when staff credentials' renewals are due (consider putting them on your calendar) and to confirm that their designations are active. "It wasn't something that was on my radar," admits the CCO. "Before they left, we had already updated our manual" with a plan to oversee designations, the officer continues.

Out of left field

"You may get requests from the exam staff that are not necessarily requests related to the exam that they're running," said Shaw. "You can sort of figure it out," though, he adds. The questions can relate to topics about the industry for which the SEC is looking to gather information generally.

Know that you can negotiate with examiners on their requests. Both Shaw and Martin had success with this. You could consider setting up a phone call with a key staffer to talk with the non-exam staff about the off-exam topic they're interested in as an alternative to supplying documents.

Negotiations can work in the exit interview, too. "We've been able to get the staff to withdraw comments before they're written up," said **Chuck Daly**, a principal of **Constellation Advisers** in New York.

Other issues that popped up during recent exams include:

√ **Due diligence of cloud-based providers**.

√ **Revenue from affiliates**. Be sure your Form ADV disclosures about these relationships are robust.

√ **Valuation**. Document everything, including printing out and saving **Bloomberg** screen shots.

√ **Risk assessment**. Don't just remove items from past assessments without documenting why they no longer pose a risk.

Editor's Note: **IA Watch** subscribers can listen to the exam webinar, and all of our recent webinars, on-demand on our website. ■

OCIE Director Marc Wyatt to return to the private sector

The **SEC**'s Director of the Office of Compliance Inspections and Examinations **Marc Wyatt** will be leaving the agency next month. Wyatt, whose tenure has been marked by a substantial increase in investment adviser examinations and a reallocation of OCIE resources to bolster its IA exam staff, plans to return to the private sector.

OCIE benefitted from Wyatt's industry experience. He came to the Commission after having served as a principal and senior portfolio manager of a global multi-strategy hedge fund. In December 2012, Wyatt was first brought on as a senior specialized examiner and also co-founded OCIE's Private Fund Unit. After the departure of then-OCIE director **Andrew Bowden**, Wyatt was named as acting director in April 2015 and was later formally promoted to director in November 2015.

Last year, under Wyatt's direction, OCIE reached a seven-year high in examinations. The division's IA/IC exam staff also increased by more than 20% in the 2016 fiscal year (**IA Watch**, Nov. 17, 2016). "His efforts on enhancing our risk based exam program and the organizational changes he has put in place will leave a lasting mark on the Commission," said the SEC's Acting Chairman **Michael Piwowar**.

Peter Driscoll, OCIE's current chief risk and strategy officer, will serve as the division's acting director. Driscoll, who has been with the SEC in various capacities since 2001, previously was OCIE's managing executive from 2013 through early 2016.

Editor's Note: Acting OCIE Director Driscoll will speak at **IA Watch**'s *IA Compliance: The Full 360 Degree View* conference April 5-7 at the Capitol Hilton in Washington, D.C. To see the full agenda and to register, click here. ■

Wave Your Flag (Continued from page 1)

Joseph McGill, CCO at **Lord, Abbett & Co.** ($136B in AUM) in Jersey City, N.J., was to create a laminated summary of securities laws applicable to his portfolio management and retail sales team and to hand out the sheets to the team's members.

Below are more activities your peers are using to keep compliance front and center in their colleagues' minds.

Maurice Tallini, COO/CCO at **Domini Impact Investments** ($1.5B in AUM) in New York expanded his quarterly "compliance committee" meetings to include the firm's entire staff.

A recent compliance roundtable held at **Neville Rodie & Shaw** ($1.3B in AUM) in New York included a visit by the firm's consultant, who shared with the staff his view of hot compliance topics, says CCO **Frank Anastasi**.

Cybersecurity training has worked at **GuideStream Financial** ($86M in AUM) in Spring Arbor, Mich. CFO/CCO **Daniel Kurtz** invested in **Security Mentor**, which hands him a monthly training module. "That's

(Wave Your Flag, continued on page 4)

Wave your Flag (Continued from page 3)

been very helpful," he says.

Another CCO tells **IA Watch** she raises compliance at the firm's weekly all-staff meetings. Recent topics have included cybersecurity, phishing e-mails and IT best practices. She also has laminated a copy of the firm's most recent **SEC** exam results letter that contained no findings, and uses it as a reminder of what good compliance can achieve.

Nothing like the real thing

An SEC exam served to wave the compliance flag at an RIA in the mountain west, according to the firm's compliance officer. Employees were briefed before and after the exam, a real-life demonstration of the role compliance plays.

A CCO at a New York firm uses the company's intranet portal to broadcast compliance reminders. Periodic posts highlight new SEC enforcement actions or remind staff that their company mobile phones cannot archive instant messages. The forum is used "not to scare people but, if it does, that's ok," says the CCO. The theme is backed by the firm's internal newsletter, which features compliance reminders, e.g., that the firm's code of ethics tool is to be used to pre-clear personal transactions.

Compliance training sprinkled in two or three times throughout the year, along with occasional e-mail reminders about items, such as a new P&P, help to spread the word for **Christina Walters**, CCO at **Croft Leominster** ($677M in AUM) in Baltimore. It also doesn't hurt that "our whole business team is right here within ear shot," she says.

Like many compliance shops, **Barrow Hanley** ($90B in AUM) in Dallas emphasizes an open-door policy for staff. **Laura Jirele-Borleske**, GIPS officer/compliance specialist, raised awareness about GIPS compliance recently with a "lunch and learn" meeting for staff.

Pressing the flesh

Many CCOs, like **Vinita Paul** at **Heartland Advisors** ($2.6B in AUM) in Milwaukee, engage in a "lot of face time" with staff. She augments these conversations with calls, e-mails, an open-door policy and compliance training.

"Part of it is just being out there, talking to people," says **Fred Shaw**, in describing his success. The director of compliance at **Hamilton Lane Advisors** ($252B in AUM) in Bala Cynwyd, Pa., relishes leaving his office and striking up conversations with colleagues. He works in how valuable compliance is and how he's there to protect them. The result: compliance is now "one of the first groups consulted" on new business ventures, he says.

Whenever your firm has an all-hands meeting – whether it's weekly or annually – be sure to place compliance on the agenda, even if it's only for a 3-4 minute presentation, recommends **Victoria Hogan**, president of **NorthPoint Compliance** in Point Pleasant Beach, N.J.

Time your e-mail reminders to events, suggests Hogan. For instance, an e-mail reminding folks of your gifts and entertainment P&P makes sense in December. But avoid sending too many e-mails, she adds. If you inundate staff, they won't read them.

Ask colleagues for their opinions about your P&Ps. Inquire if your traders regard your G&E policy as too strict. Soliciting their opinions and listening make it more likely staff will embrace a policy specifically and compliance generally.

Hogan shares another idea: Give out gift cards to staff who answer compliance questions correctly, e.g., what's the threshold for reporting political contributions? Make such games quick – lasting only 3-4 minutes – but try the technique frequently, she recommends. ■

Former CCO/AML officer charged for SARs failures tied to scheme

In January, the **SEC** shouted from the rooftops that it remains laser-focused on money laundering and brokerage firms' AML programs. The Commission's 2017 exam priorities letter highlighted AML as a key area of interest, OCIE generated an AML "source tool" for broker-dealers and the SEC brought yet another AML enforcement action—this time ensnaring a firm's former CCO/AML officer.

The SEC's 2017 exam priorities letter specifically stated that examiners would "review how broker-dealers are monitoring for suspicious activity at the firm." The Commission added that it will continue to "assess broker-dealers' compliance with SAR requirements and the timeliness and completeness of SARs filed."

Windsor Street Capital (formerly known as **Meyers Associates**) and its former CCO/AML Officer **John Telfer** allegedly fell short of the mark when it came to monitoring suspicious activity and filing SARs. The New York-based firm, along with Telfer, was charged Jan. 25 with failing to file SARs for $24.8 million in suspicious transactions, including a classic pump-and-dump scheme.

The SEC alleges that Meyers Associates and Telfer, who occupied his role from November 2013 until last

(CCO Charged, continued on page 5)

CCO Charged (Continued from page 4)

September, should have known about the suspicious circumstances behind many transactions occurring in its customer accounts. Customers reportedly deposited large blocks of penny stocks, typically liquidated them amid substantial promotional activity, and then transferred the proceeds away from the firm.

The SEC claims that on numerous occasions from at least June 2013 to the present, Meyers Associates violated Securities Act section 5 by facilitating the unregistered sale of hundreds of millions of penny stock shares, without performing adequate due diligence regarding the sales' section 5 compliance.

Meyers Associates also repeatedly violated Exchange Act rule 17a-8 by failing to file suspicious activity reports with **FinCEN**. The firm earned a total of at least $493,000 in commissions and fees from the penny stock sales and unreported suspicious transactions, the SEC noted.

A separate complaint

The activity in accounts controlled by microcap financiers **Raymond Barton** and **William Goode** was cited. The SEC separately filed a complaint in federal court against the pair, along with **Matthew Briggs**, **Kenneth Manzo**, and **Justin Sindelman**. The parties' pump-and-dump scheme included acquiring shares of dormant shell companies, falsely touting news and products stemming from those companies, and then dumping the shares on the market for investors to purchase at inflated prices, the Commission alleges.

As Meyers Associates' AML officer, Telfer was personally responsible for monitoring customer transactions for suspicious activity and ensuring the firm's compliance with SAR reporting requirements. By failing to monitor customer transactions and failing to cause the firm to file the required SAR reports, Telfer aided and abetted, and caused, Meyers Associates rule 17a-8 violations, the SEC found. He's not the first CCO/AML officer to face legal troubles stemming from his role (**IA Watch**, Jan. 21, 2016).

Due diligence appears to have been lacking on Telfer's part. Barton and Goode represented to Meyers Associates that their stock sales were exempt from section 5 under Securities Act rule 144's safe harbor. These representations were allegedly accepted at face value, without inquiry, the SEC stated. "A reasonable inquiry of the Stock Sales by Meyers Associates would have, at the least, cast doubt on the factual underpinnings for the customers' reliance on rule 144," according to the agency.

Red flags aplenty

There were evidently many red flags that ultimately weren't followed up on. Meyers Associates even conducted a **Google** search for Barton that yielded a post warning about him on the website "pumpsanddumps.com." The SEC determined that, despite multiple red flags, the firm failed to reasonably investigate whether SAR filings would be necessary and routinely accepted physical deposits of large blocks of penny stocks and allowed its customers to liquidate them, followed by the customers transferring out the sale proceeds.

The SEC will be watch this issue. "The SEC's Broker-Dealer Task Force AML initiative is focused precisely on the conduct charged against Meyers Associates, which we allege systemically flouted its obligations under the securities laws to report suspicious activity," said **Andrew Calamari**, director of the SEC's New York Regional Office. ■

Read more from this story at www.regcompliance-watch.com. ■

Squeezed (Continued from page 1)

encrypted, with only the bad guy holding the code to unlock the files.

To pay or not to pay

Leibstone is adamant. Never pay a cyber ransom. **Jeffrey Squires**, owner of **Relativity Investment Management Consulting** in Milwaukee, agrees. "We would not have this issue if nobody paid the ransom," maintains Squires. Paying only inspires bad guys to expand their enterprise, he adds.

But there may be times when you would want to pay the ransom, according to **Rajesh Goel**, CTO of **Brainlink** in New York. If you don't have good backups of your data or those backups are corrupted, "then decide if the data are valuable enough to pay the ransom," he says. "It's a lot cheaper to pay the ransom than to pay an IT expert to recover the data," he adds.

Squires offers a four-step plan for ransomware attacks:

1. Develop a strategy ahead of time. Create a P&P. Decide when and if you'll pay. Focus on a method for restoring your data as quickly and completely as possible.

2. Weigh if your IT vendor's up for the job. "Are you an important enough customer" for the vendor to drop what it's doing and spring into action for you, asks Squires. If not, you may need to search for a new vendor because "time is of the essence" after a ransomware attack.

(Squeezed, continued on page 6)

Squeezed (Continued from page 5)

3. Test the process with your IT vendor. See how quickly your data can be restored adequately enough so you can continue to work.

4. Train staff to communicate with you pronto when they receive an electronic notice of a ransom request.

Try to "identify your problem children ahead of time," says Squires, meaning pinpoint your colleagues who may be more susceptible to clicking through a strange e-mail link.

But training has its limits "because you're dealing with humans, not robots," he continues. Goel recommends you encourage staffers to report possible cyber events by maintaining an open communications channel and not punishing phishing victims.

The computer user is "the last line of defense," echoes Leibstone.

He's running into a trend of some of "the smartest people I know" falling prey to this attack. It's the weekend and they get a call at home from **Microsoft** announcing a critical security issue that requires the caller to be granted remote access to their computer.

Mistake. Microsoft will not call you about this, Leibstone warns.

Copies of copies

Keep several backups, Leibstone recommends. He tells of a private equity fund adviser that suffered a devastating ransomware attack that not only penetrated its network but poisoned its live, online backup. Maintaining a second, off-line backup saved the day but several hours of data were permanently lost.

Some ransomware attacks are minor. The bad guy simply wants a little money or a pile of bitcoins and he's on his way. Others, like the famous **Sony** intrusion, are intentional malicious acts, says Goel. The latter would require "deeper surgery" to expel the cyber invaders, he adds.

TIP: Once a year, trigger a "pull the plug exercise" that tests your readiness for an attack, suggests Goel. Document its lessons learned, update your procedures and adjust your training accordingly.

TIP: Teach your staff to permanently delete suspicious e-mails. In Outlook, hit shift+delete to achieve this outcome, continues Leibstone.

After receiving the *Verizon* e-mail, Leibstone went to its website, logged in and discovered there was no such emergency. It was a hacker. He sums up his advice with three words: "Trust no one." ■

Group Publisher: Hugh Kennedy
301-287-2213
hkennedy@regcompliancewatch.com

Publisher: Carl Ayers
301-287-2435
cayers@regcompliancewatch.com

Contributing Reporter: Richard Schmitt

IA Watch strives to provide you with accurate, fair and balanced information. If for any reason you believe we are not meeting this standard, please let us know.

Our Address: IA Watch
Two Washingtonian Center
9737 Washingtonian Blvd., Suite 502
Gaithersburg, MD 20878-7364

Subscriptions:
For questions about newsletter delivery, address changes or online access, call our Customer Service department toll-free at 844-421-6333. Our toll-free conference hotline: 888-234-7281.

This symbol means a direct link to the web in our online version.