Fin|News
INDUSTRY NEWS
02.15.22

Security Check: Institutions, Regulators Address Cybersecurity Vulnerabilities

An uptick in cybercrime within the institutional investment community including two recent cyberattacks on pension boards has exposed vulnerabilities with the industry and led to questions around the resources needed to combat network intrusions.

According to the *Securities and Exchange Commission*, cyberattacks have increased at an “alarming rate” in recent years, with the number of data compromises increasing by more than 68% in 2020.

The Public Employee Retirement Administration Commission, a Massachusetts regulatory authority which oversees 104 statewide

retirement boards, recently experienced two cybersecurity matters firsthand.

The authority released a memorandum in January 2022 stating that a fraudster impersonated a board administrator seeking funds from the board's custodian.

The fraud attempt was unsuccessful because of due diligence by the board and its custodian, but it did provide a "rare real-time situation," PERAC Executive Director John Parsons said, in an interview. Parsons confirmed that the investigation is ongoing, with state and federal authorities looking into it.

Meanwhile, more than $3 million went missing from the Quincy (Mass.) Retirement Board following an e-mail phishing scam that an investment manager fell victim to, according to a recent report.

One of the plan's managers received an e-mail from a former employee's board e-mail account, which had been hacked. The fraudulent e-mail included instructions for a $3.5 million wire transfer that the manager made in February 2021.

The plan did not learn of the fraudulent transfer until months after it happened and PERAC, which is investigating the incident, learned of it in October 2021 when the board reported it to the commission.

Parsons asserts the transaction was a result of “human error and a breakdown of security controls,” and indicated in the report that the investigation is expected to last several more months.

Michael Sacco, legal counsel to the Quincy retirement board, did not respond to an e-mail seeking comment.

Parsons explained that while PERAC, as a state agency, has “very experienced IT staff” itself as well as “the resources of the state IT folks to support us and back us up,” many retirement systems are smaller and generally do not have internal information technology staff, making them a “popular target” for fraudsters.

“These types of entities, many that are small, it’s not their daily business to engage in cybersecurity, the daily business is to run a retirement fund,” he said, noting that Massachusetts systems are not unique from other state retirement boards.

While these types of attacks are rare, they are not unheard of – and the shift to hybrid or fully-remote work environments is causing concern for some.

Senior V.P. and Head of Tax-Exempt Defined Contribution Research Ben Taylor of investment consultant Callan finds that having the necessary resources to combat cyberattacks is “always important,” however, a work from home environment does introduce “significant vulnerabilities.”

“You have network security, you have on-premise security, you have physical access security and a host of other measures in addition to the ability to be physically segregated from family members when you’re having work conversations in a workplace, which is very distinct from a home environment,” Taylor said.

“Similarly, not every human being in the world is an expert at securing things like a local Wi-Fi network or their own personal device,” he continued.

Founder and CEO Gabriel Friedlander of security awareness training company Wizer, a two-year-old firm used by PERAC for its 2021 cybersecurity training, believes that working from home increases the opportunity for cyberattacks.

In a work from home environment, “We have to follow the processes, more than ever, we have to actually pick up the phone and call some people. It requires even more training, because we have to make sure that the processes are in place and people follow them, otherwise there is no hallway talk [such as] ‘Hey, did you just do that?’” Friedlander said.

Having been victimized by a cyberattack incident that affected an e-mail account several years ago, the Communities Foundation of Texas is of the belief that working from home adds additional security risk.

The Dallas-based plan has “further tightened the rules/user permissions on any changes that could be made remotely to minimize the opportunity for compromising the system,” said Senior V.P. and Chief Financial and Administrative Officer Beth Bull.

Senior Security Researcher Jonathan Tanner of cybersecurity solutions company Barracuda Networks thinks that at the very least, a remote workforce “complicates” security, if not making it more difficult, and maintains that having the proper resources in place is important to prevent attacks.

“Resources are certainly a factor since what traditionally could have been achieved with a few pieces of security hardware protecting the local network is not a feasible approach to remote work for the first part. There are certainly solutions out there to provide the same security coverage to a remote workforce, but where things become more complicated is in understanding the risks and what requires protection in the first place and whether or not it can even be protected,” Tanner said.

Cybersecurity education and training for staff members and clients, in addition to regulation, are important for many institutional investment organizations to be aware of, and many employ third-party experts to thwart attacks while some also seek help internally.

As cybersecurity is a “consistently evolving threat,” continuous training is “critical to ensure our staff are up to date on the latest exploits and threats they face during the course of business,” said **Joe Wilson**, director of information technology at investment consultant **Verus**, which operates under the guise of a ‘zero-trust’ environment.

Massachusetts requires retirement board members to have mandatory education on cybersecurity, according to PERAC’s Parsons.

“Cybersecurity has been an ongoing topic of our education training sessions for the last two or three years. We bring in third-party experts with experience, either private companies that do cybersecurity assessments and education or we use the expertise of Massachusetts state government,” Parsons said, noting that state police are going to conduct one of the trainings and the state comptroller will do a session on internal controls for security overall.

Wizer’s Friedlander finds regulation has a lot to do with security as “there is a huge compliance component” to it.

“Almost every company today [is required] to address some regulations. That’s why security awareness training is applicable to all sectors,” he said.

Callan is less focused on the mechanics of cybersecurity and more on regulation or best practice resources that the industry is utilizing as well as “how evolutions in both court cases and regulation and the assistance of various federal agencies can assist clients,” Taylor said.

Likewise, **Verus** does not provide formal cybersecurity training directly to clients, but does encourage them to follow best practices with regard to sharing sensitive information.

“To assist them in this, we provide our clients with tools to encrypt communication via e-mail and to use document management systems that provide data encryption,” **Wilson** said.

Barracuda, whose cybersecurity services are entrusted by more than 200,000 organizations worldwide, contends that a basic understanding of cybersecurity practices and common threats is important for institutions, according to Tanner.

“Especially where financial information is concerned, the impact of an attack could be much the same as having a wallet or purse stolen containing credit cards and IDs. Humans are most often the weakest links in any security plan, and attackers know this well. Therefore, it is critical for everyone to have an understanding of cybersecurity as it relates to them and their jobs,” Tanner said.

“For staff handling others’ sensitive information, there is obviously a larger depth of knowledge that is required than for users. Still,

nobody can simply expect someone else to be responsible for the entirety of their security. Even with the most comprehensive phishing and malware protections available, things will get through. But, if the person seeing the email or suspicious file takes the time and has the right training to question it, that could mean the difference between stopping a possible attack or not," he continued.

Wizer's software platform, which is used by over 10,000 organizations from various sectors, uses "short and to the point" videos to train its clients, according to Friedlander.

In addition to using games, various topics and stories in its training process videos, Wizer conducts phishing simulations where the firm simulates an attack.

"Basically, the companies attack their own employees, but instead of obviously stealing their information, they tell them, 'Here is what you need to do next time if something like that happens.' You train them as part of the training problem process," Friedlander said.

The Communities Foundation of Texas also believes all staff should receive appropriate training and education to understand the risks.

"There are many threats in today's online environment, and they are constantly changing and becoming more sophisticated.

Investing in ways to keep staff informed and updated with the latest information on how to protect our systems and information is key to fighting cyberattacks," Bull said.

The foundation's third-party vendors handle the security on its various websites and the foundation has risk mitigation plans in place with its providers, who take the lead on managing attacks if they occur, she said.

Additionally, the foundation maintains strong procedures and protocols such as an active antivirus solution and strict firewall rules for traffic entering the network. Meanwhile, "crucial" databases are encrypted and isolated within the network, according to Bull, who noted that staff is also required to complete cybersecurity training models on spam, phishing/spoofing, hacking and other online scams on a monthly basis.

"Progress/results [are] tracked and shared with the leadership team, who will follow up with any of their staff if they fall behind in the trainings," Bull said.

She further indicated that such training and education are essential for the foundation's staff being that the plan feels cybersecurity represents one of the most significant business risks.

"[We] take data integrity very seriously as a nonprofit foundation. Any system user could create a point of vulnerability, which

makes it especially important that all users receive appropriate training and education and understand the risks and know how to identify phishing, et cetera," Bull said.

Friedlander finds training is essential so that people can change their online behaviors.

"If knowledge was enough, then accidents wouldn't happen. It's about routines and habits and being careful. People can be easily fooled. You have to do your due diligence no matter what," he said.

Verus has a formal cybersecurity training policy for internal staff that includes a third-party vendor training the staff on various aspects of cybersecurity, according to **Wilson**.

"Currently our curriculum consists of six training topics delivered every other month throughout the year," **Wilson** said.

The Seattle-based consulting firm also actively monitors e-mail and chat communication for fraud and cyberattacks with the help of several outside firms.

"We utilize several outside firms and third-party tools to assist with cybersecurity-related monitoring and prevention. **Verus** also maintains an internal committee that meets on a regular basis to discuss and improve our cybersecurity-related posture," he said.

Callan employs a “three-pronged approach” to mitigate cybersecurity threats, according to COO Inga Sweet.

The approach includes “employee training about phishing and information/data management best practices, systems technology that blocks inbound threats and strict vendor and systems requirements,” Sweet said, noting that “all of these programs, policies and procedures are audited periodically by an outside cybersecurity auditing firm.”

Like every state agency in Massachusetts, if a cyberattack were to occur at PERAC, the organization has a disaster recovery plan in addition to its built-in security, Parsons indicated.

“We have an internal control plan that we provide to the state and a disaster recovery plan if anything happens,” he said.

Barracuda’s Tanner asserts that ensuring that a company’s software and operating systems are up to date and properly configured are “definitely a must.”

“Comprehensive security protection from threats stemming from e-mail, malware, web applications, and any publicly exposed network resources is key. Physical security is also important since even with comprehensive security, an attacker walking into the office could bypass most of these measures. Security monitoring and remediation plans are also important should an attacker get a foothold in the network. Lastly, security training and awareness

are important for reducing the risk of any threats that make it past security solutions or that can't be covered by solutions," Tanner said.

Some in the industry have faith that their peers are properly securing themselves against cyberattacks and larger regulatory entities are doing their part in the fight against cybercriminals.

The Financial Industry Regulatory Authority provided updated guidance in 2020 for investors on how to address increased vulnerabilities to cybersecurity attacks on firm and home networks in response to the pandemic.

At the SEC, an Event and Emerging Risks Examination Team was created in July 2020 to proactively engaged with financial firms about emerging threats, including preventing fraud.

And last week, the SEC proposed a new rule that would require asset managers and investment advisory firms to establish written policies to address cybersecurity risk, report cybersecurity incidents to the SEC within 48 hours, enhance cybersecurity disclosure requirements and maintain records of the events.

Within the institutional investment industry, Parsons said that he often sees training on cyberattack prevention as part of the conference agendas for the national organizations that PERAC belongs to.

Cybersecurity experts and the industry alike believe that given the sensitive nature of the information that they are trying to protect, it is not uncommon for financial institutions to be more concerned about cyberattacks and threats.

While indicating that the threat landscape for financial institutions is not notably different from most other businesses, Barracuda finds that the importance of proper security is far greater due to the access to more sensitive data.

“One specific type of threat that financial institutions may have to deal with is cybercriminals either impersonating or taking over the accounts of legitimate users. Even for those who have full-featured online services, the risk of account takeover can still enable attackers to harm users,” Tanner said.

Callan’s Taylor made note of the “obvious reality” that cybersecurity is important and that no one wants privileged information taken or have a critical system disabled when handling private information and assets.

“In terms of our professional practice, there are evolutions with respect to fiduciary and regulatory obligation for both plan sponsors and for asset owners and at times consultants and other entities operating in the industry where it’s important for our clients to understand both their fiduciary duties and also the best methods to act on those as pertains to cybersecurity,” Taylor said.

Parsons finds that many entities, including retirement boards, are seeking cyber insurance, yet it is becoming more difficult to obtain due to the number of attacks that happen and service is usually limited.

“They want to ensure your IT system meets a certain level of security, so it forces you to go through a number of steps to demonstrate to the insurer that you are a worthy candidate to be insured. It’s a good process to go through in terms of an analysis of your own security,” he said.

When it comes to money, Friedlander advises the institutional investment community to conduct due diligence through verification by phone.

“If somebody sends me a text message, it doesn’t mean that that person is who I think it is. Even if the e-mail is exactly the same [or] part of a thread that we had going on. You have to pick of the phone, call and verify. It’s up to you to do that due diligence. It’s probably the number one thing to do to help,” he said.

While network intrusion and data breaches are concerning for all organizations regardless of size or industry, it becomes more concerning where sensitive customer information, the possibility of financial gain, and/or critical infrastructure come into play, according to Tanner.

“Every organization should assess risk of attacks and take what an attacker might gain into account as a factor in addition to simply what attacks might be faced,” he said.