U.S. Securities and Exchange Commission Finally Getting Serious about Cybersecurity

By Craig A. Newman, of Patterson Belknap Webb & Tyler LLP, New York.

The U.S. Securities and Exchange Commission is finally getting serious about cybersecurity—and for good reason. If the ever-growing business and headline risk aren't enough to scare investment advisers and broker-dealers into action, they now have added motivation to make cybersecurity a top priority—impending regulatory examinations and enforcement proceedings.

Cybersecurity has been on the SEC's radar for the past few years, but only recently has the agency intensified its scrutiny of firms' data security and governance protocols. And, in a series of bold public statements, the SEC is even promising to hold chief compliance officers accountable if they look the other way when it comes to implementing meaningful cybersecurity plans— including incident response protocols—to guard against and remediate when cybercriminals and hackers burst through a firm's firewalls, even when it's the fault of a hapless employee or outside vendor.

It's no surprise that the SEC is clamping down. Cyberattacks on major financial institutions, healthcare providers, and even retail banks are already under way. In fact, the SEC's own cybersecurity sweep exams conducted from 2013-2014 revealed that, of the more than 100 firms examined, 88 percent of the broker-dealers and 74 percent of the investment advisers had experienced a cyberattack, either directly or through a third-party vendor.

**New Cybersecurity Examination Initiative**

In September 2015, the SEC issued the so-called "cyber alert," as the SEC's Office of Compliance Inspections and Examinations issued a Risk Alert announcing a new cybersecurity examination initiative. The Risk Alert sets forth the Securities and Exchange Commission's regulatory expectations for the conduct of examinations of broker-dealers and investment advisers.

The SEC's expectations are not a "check the box" compliance measure, but rather a series of significant steps toward creating a broad platform of cybersecurity—compliance that touches upon key areas of a firm's business operations. In addition to identifying specific areas of focus for regulated firms—including governance and risk assessment, IT and network access, data loss prevention, third-party vendor management and safeguards, training and incident response plans—and placing greater emphasis on information security, the risk assessment methodology requires firms to look to the future and consider what the threats and vulnerabilities might be.

The SEC has also promised to conduct well-thought-out examinations that take into account the firm's overall business and operations. The examinations will be tailored to the firm's size, complexity, and technology environment, and will be conducted by experienced examiners who will work closely with the firm's management to develop a comprehensive plan for addressing cybersecurity risks.

**Cybersecurity Measures**

The Risk Alert sets forth a detailed list of cybersecurity measures that firms should implement to address potential risks. These measures include:

1. **Risk Assessment:** Firms should perform a comprehensive risk assessment that identifies and evaluates potential cybersecurity risks and vulnerabilities.
2. **Goverance:** Firms should establish a board-level oversight committee that is responsible for cybersecurity risk management.
3. **IT and Network Access Controls:** Firms should implement strong access controls for their IT systems, including strong authentication and access controls.
4. **Data Loss Prevention:** Firms should implement effective data loss prevention measures to protect sensitive information.
5. **Third-Party Vendor Management:** Firms should conduct thorough due diligence on third-party vendors to ensure that they meet the firm's cybersecurity standards.
6. **Training and Incident Response:** Firms should implement robust training programs and incident response plans to address potential cybersecurity incidents.

These measures, along with other requirements set forth in the Risk Alert, are designed to help firms build a strong foundation of cybersecurity measures and help mitigate the risks of cyberattacks.

The SEC has made it clear that it will hold chief compliance officers accountable for the implementation of these measures. Firms that fail to take the necessary steps to address cybersecurity risks may face regulatory actions, including enforcement proceedings and significant fines.

In conclusion, the SEC's new cybersecurity examination initiative is a welcome development for the securities industry. By adopting a comprehensive approach to cybersecurity risk management, firms can better protect their clients and the broader financial system from the growing threat of cybercrime.
However, the SEC determined that R.T. Jones willfully allowed an incident to occur as a result of the attack. "We don't have any evidence that any of the clients suffered financial harm," said Andrew Ceresney, in a speech to the National Society of Compliance Professionals—national-conference-keynot/. R.T. Jones did not have such written safeguards in place in advance of the cyberattack, and instead a $75,000 fine was issued.

The SEC's message couldn't be clearer: Cybersecurity is not just an IT issue, and it's time to get your house in order and implement a thoughtful and detailed cybersecurity plan before the hackers strike.

Two days later, SEC Chair Mary Jo White announced that "electronic cybersecurity attacks cannot be easily eliminated, and we must be proactive in our regulatory efforts to ensure that the actions of firms are taken to prevent, detect, and respond to such intrusions." The SEC's September 22, 2015, enforcement action against R.T. Jones Capital Equities Management, Inc., a small St. Louis-based broker-dealer, couldn't be clearer: Cybersecurity is not just an IT issue, and it's time to get your house in order and implement a thoughtful and detailed cybersecurity plan before the hackers strike.

SEC Enforcement Director Andrew Ceresney's November 4, 2015, speech to the National Society of Compliance Professionals—national-conference-keynot/ was a wake-up call for compliance officers (CCOs) to be "proactive" in their work, and to clarify the circumstances in which CCOs would find themselves in the agency's cross-hairs, emphasizing that "[w]e look hard at the facts and fairness concerns in every case."

First Cybersecurity Enforcement Action

The SEC's remarks came in the aftermath of the agency's first cybersecurity enforcement action — a lengthy mandate that forces the firm — R.T. Jones Capital Equities Management, Inc. — to implement a "comprehensive policy and procedure" in advance of a breach that compromised personally identifiable information (PII), including Social Security numbers for 85,000 individuals, beginning September 2, 2015.

The SEC's message to investment advisers and broker-dealers couldn't be clearer: Cybersecurity is not just an IT issue, and it's time to get your house in order and implement a thoughtful and detailed cybersecurity plan before the hackers strike.

First Cybersecurity Enforcement Action

The SEC's remarks came in the aftermath of the agency's first cybersecurity enforcement action — a lengthy mandate that forces the firm — R.T. Jones Capital Equities Management, Inc. — to implement a "comprehensive policy and procedure" in advance of a breach that compromised personally identifiable information (PII), including Social Security numbers for 85,000 individuals, beginning September 2, 2015.

SEC Enforcement Director Andrew Ceresney's November 4, 2015, speech to the National Society of Compliance Professionals—national-conference-keynot/ was a wake-up call for compliance officers (CCOs) to be "proactive" in their work, and to clarify the circumstances in which CCOs would find themselves in the agency's cross-hairs, emphasizing that "[w]e look hard at the facts and fairness concerns in every case."

First Cybersecurity Enforcement Action

The SEC's remarks came in the aftermath of the agency's first cybersecurity enforcement action — a lengthy mandate that forces the firm — R.T. Jones Capital Equities Management, Inc. — to implement a "comprehensive policy and procedure" in advance of a breach that compromised personally identifiable information (PII), including Social Security numbers for 85,000 individuals, beginning September 2, 2015.

First Cybersecurity Enforcement Action

The SEC's remarks came in the aftermath of the agency's first cybersecurity enforcement action — a lengthy mandate that forces the firm — R.T. Jones Capital Equities Management, Inc. — to implement a "comprehensive policy and procedure" in advance of a breach that compromised personally identifiable information (PII), including Social Security numbers for 85,000 individuals, beginning September 2, 2015.

First Cybersecurity Enforcement Action

The SEC's remarks came in the aftermath of the agency's first cybersecurity enforcement action — a lengthy mandate that forces the firm — R.T. Jones Capital Equities Management, Inc. — to implement a "comprehensive policy and procedure" in advance of a breach that compromised personally identifiable information (PII), including Social Security numbers for 85,000 individuals, beginning September 2, 2015.

First Cybersecurity Enforcement Action

The SEC's remarks came in the aftermath of the agency's first cybersecurity enforcement action — a lengthy mandate that forces the firm — R.T. Jones Capital Equities Management, Inc. — to implement a "comprehensive policy and procedure" in advance of a breach that compromised personally identifiable information (PII), including Social Security numbers for 85,000 individuals, beginning September 2, 2015.
Tyler LLP in New York and Chair of the firm's Privacy and Data Security Practice. He is recognized as a leading authority on cybersecurity issues, and advises global institutions, Fortune 500 companies, investment funds, their boards and leadership teams on data security practices, policies and governance issues, including investigations, regulatory matters and litigation. He may be contacted at cnewman@pbwt.com.