Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

8 Critical Lessons From Morgan Stanley Cybersecurity Case

Law360, New York (June 24, 2016, 11:54 AM ET) -- This month, the U.S. Securities and Exchange Commission hit Morgan Stanley with a $1 million penalty for cybersecurity lapses that enabled a former financial adviser to tap into its computers and take client data home, where it was apparently hacked. Below are some key lessons drawn from the matter.

John Reed Stark

Background

The settled administrative order finds that Morgan Stanley Smith Barney (now rebranded as Morgan Stanley Wealth Management) failed to adopt written policies and procedures reasonably designed to protect customer data.

As a result of these failures, from 2011 to 2014, then-employee Galen J. Marsh impermissibly accessed and transferred the data regarding approximately 730,000 accounts to his personal server. A likely third-party cyberattack into Marsh's personal server resulted in portions of the confidential data being posted on the internet with offers to sell larger quantities. According to the SEC:

- Morgan Stanley's policies and procedures were not reasonable for two internal web applications or "portals" that allowed its employees to access customers' confidential account information;
- For these portals, Morgan Stanley did not have effective authorization modules for more than 10 years to restrict employees' access to customer data based on each employee's legitimate business need; and
- Morgan Stanley also did not audit or test the relevant authorization modules, nor did it monitor or analyze employees' access to and use of the portals.

The SEC's order finds that Morgan Stanley violated Rule 30(a) of Regulation S-P, also known as the "Safeguards Rule." Morgan Stanley agreed to settle the charges without admitting or denying the findings.

Galen Marsh

In a separate order, Marsh agreed to an industry and penny stock bar with the right to apply for re-entry after five years. In a parallel criminal prosecution by the U.S. Attorney's Office for the Southern District of New York, Marsh pled guilty to criminal charges filed last September of one count of unauthorized access to a computer. As announced by the SDNY, Marsh, presenting his side of the story in a filed sentencing memorandum, was sentenced later to 36 months of probation and a $600,000 restitution order.

Lesson 1: Morgan Stanley's Outstanding Response

The Morgan Stanley SEC enforcement action sets itself apart because: 1) the matter involves Morgan Stanley, a large, sophisticated and leading financial firm; 2) a now-terminated Morgan Stanley employee was charged criminally; and 3) the incident was not a data mishap but rather involved an institutional and systemic failure, which required immediate remediation. But what is most interesting about the SEC Morgan Stanley matter is that Morgan Stanley's conduct was exemplary; the firm did everything right.

While Morgan Stanley may have been at fault for the actual incident (because of its system failures regarding data access modules), every firm is going to experience cybersecurity lapses. No firm can boast of perfect cybersecurity, mistakes will always happen. So Morgan Stanley's response, the key to analyzing any cybersecurity-related incident, is what matters most. And the firm's response grades an A-plus. Here is why:

Morgan Stanley Detected the Online Sale of Its Client Data. Reports indicate that Morgan Stanley officials picked up on the posting almost immediately, after it triggered an alert by its routine surveillance of a number of websites that traffic in sensitive information. The offer was quickly taken down the same day after Morgan Stanley discovered the leak. Very impressive.

Morgan Stanley Dispensed with Marsh Quickly and Firmly. In short order, Morgan Stanley traced the breach to Marsh, a financial adviser working out of its New York offices. Marsh, who had been with Morgan Stanley since 2008, was quickly fired and ultimately charged criminally for his theft of Morgan Stanley client data. Very impressive.

Morgan Stanley Came Clean. Morgan Stanley quickly announced details, specifically that Marsh took data on about 10 percent of its 3.5 million wealth management customers, including transactional information from customer statements. Morgan Stanley found that Marsh did not take any sensitive passwords or Social Security numbers, and that it had not found any evidence that the breach resulted in any losses to customers. Very impressive.

Morgan Stanley Remediated. While the SEC's Morgan Stanley order does not detail the specific remedial steps taken by Morgan Stanley (which, by the way, Morgan Stanley should have insisted upon including therein), the order does imply that had it not been for Morgan Stanley's remedial actions, the penalty would have been more. Very impressive.

Morgan Stanley Engaged an Independent Consulting Firm and Law Firm to Investigate the Data Security Incident. Strong corporate leaders seek answers from independent and neutral sources of information. Otherwise, risks are not properly exposed and examined, and they become exacerbated rather than assuaged. The Morgan Stanley C-suite clearly understood the need for integrity in its response. Morgan Stanley responded swiftly, responded with transparency (especially with its regulators and with law enforcement) and, most importantly, according to Morgan Stanley managing director James Wiggins, conducted an independent investigation, using both an independent legal team and an independent consulting team, to understand its failures. Extraordinarily impressive.

Lesson 2: Cybersecurity Remains an Oxymoron

When my daughter comes home from school with a cold, it is not her fault. No one can protect her from catching a cold; they are inevitable. The same goes for data security incidents.

Cyberthreats fall broadly into external and insider issues, and the Morgan Stanley matter involved both. The hackers who attacked Marsh represented an "external" threat, which could have been state-sponsored — perpetrated by terrorists, military or other companies. Given the total weight of resources at the disposal of external threats (such as legions of soldiers), external threats can outgun any company, even one as large, complex and sophisticated as Morgan Stanley.

Marsh, on the other hand, represented an "internal" threat, a disgruntled, rogue or dishonest employee exploiting an available cybersecurity loophole. Like external threats, internal threats can wreak havoc upon any firm, no matter how rigorous its oversight — and internal threats need not be criminal in nature. Companies also face internal threats from careless, slipshod or otherwise slack employees. Just like corrupt employees, inattentive or disaffected employees exacerbate existing vulnerabilities, lapses or other weaknesses, inevitably introducing errors and policy failures.

Employees will always be: the weakest cybersecurity link, the root cause of data breaches, and the reason why cybersecurity is an oxymoron.

Lesson 3: The SEC's Use of the Safeguards Rule Remains the Cornerstone of the SEC's Cybersecurity Regulatory Framework

Violation of the SEC's nonscienter-based Safeguards Rule has become the standard minimum charge in SEC cybersecurity-related enforcement actions against financial firms, just like violation of the SEC's nonscienter-based SEC internal controls rules has become the standard minimum SEC charge in accounting-related enforcement actions against public companies.

Since its promulgation, the SEC has not brought many enforcement actions for violations of the Safeguards Rule, but the commission has now stepped up its cybersecurity efforts, including launching its Sept. 15, 2015, and April 15, 2014, cybersecurity examination sweeps.

Like the SEC's internal controls compliance requirements for public companies, the "Safeguards Rule" has broad regulatory bandwidth. The Safeguards Rule requires every broker-dealer and investment adviser registered with the SEC to adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information, and that are reasonably designed to:

- Ensure the security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
- Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Lesson 4: Its Administrative Forum Remains the SEC's Preferred Venue for Cybersecurity Failures

The SEC selected its administrative courtroom as the forum for the Morgan Stanley matter — even though there was a parallel criminal action against Marsh filed in federal court. In future SEC enforcement matters involving cybersecurity failures, the SEC will likely continue to file their charges administratively, especially if the alleged violations pertain to an SEC-regulated entity violating an opaque, technical and subjective regulation such as the Safeguards Rule.

Lesson 5: Victims are Presumed, Not Required

Not surprisingly, breached investors (i.e. customers whose data may have been exfiltrated or otherwise compromised) need not suffer any harm in order for the SEC to bring an enforcement action. Just like most of the recent data breaches making headlines, in the Morgan Stanley matter: 1) no one identifies the actual perpetrator of the cyberattack, and 2) actual harm to customers is presumed. The SEC, like every other regulator and law enforcement agency, relies on the ethereal axiom that some victim exists somewhere who has actually been hurt.

Lesson 6: Control, Monitor and Limit Employee Access to Data and to

Systems

The SEC was clear that Morgan Stanley failed to: (1) audit and/or test the effectiveness of the authorization modules for the portals; and (2) monitor employee access to and use of the portals.

Corralling, restricting and surveilling universal access to systems and data requires constant vigilance. Segregating data access by job classification is important, requiring strict policies, vigilant enforcement of those policies and meticulous attention to turnover and promotions. The same goes for administrative accounts, i.e. user accounts that allow IT administrators (or "admins") to make changes that will affect other users.

The use of admin passwords and admin rights should be tightly controlled, monitored and documented. Admins can change security settings, install software and hardware, and access all files on a computer, mobile device, tablet or network. Admins can also make changes to other user accounts. Cyberattackers prey in particular on admin passwords (to attain command and control of a system), especially those rarely used, which can fly under the radar. Inadvertently keeping old admin passwords or assigning too many admin passwords can lead to massive data breaches and is an easily avoidable vulnerability.

Lesson 7: The Importance of Penetration Testing

Perhaps the most serious SEC allegation was that Morgan Stanley had not conducted any auditing or testing of the authorization modules of the relevant portals over the 10 years that the portals were in use. This matter should serve as a reminder for all companies concerning the importance of hiring expert and thorough penetration (or "pen") testers, who take a meticulous yet holistic approach to their analysis. Morgan Stanley likely engages in a variety of routine and annual testing of its systems, yet its pen testers failed to discover Marsh's unlimited access and Morgan Stanley's failure to use appropriate authorization modules to limit access to the data. This sort of testing oversight can happen; the competency and methodology of pen testers varies wildly.

Lesson 8: The Need for a Virtual Big Brother

The SEC Morgan Stanley order states specifically that: "Morgan Stanley did not monitor user activity in the [data portals Marsh improperly and unlawfully infiltrated] to identify any unusual or suspicious patterns." Clearly, the SEC expects financial firms to implement intelligent and technological surveillance of employee activity and red-flag suspicious behavior.

Companies should consider data analytic and related artificial intelligence technological applications, which might have alerted Morgan Stanley to the individual's behavior (which took place over a three-year period). For instance, a financial firm employee (like Galen Marsh) who trades or is otherwise active in the penny stock market, should trigger enhanced supervision. The penny stock market is historically replete with fraud and populated by con artists, and requires enhanced internal controls, increased supervisory intervention, and a healthy, continuous rigorous skeptical oversight.

Additionally, by implementing new and emerging data analytic technologies, a company, especially a financial firm, demonstrates to regulators and shareholders that it takes seriously its cybersecurity-related internal controls.

Conclusion

Cybersecurity at SEC-registered entities like Morgan Stanley has become a top priority for the SEC inspections group and enforcement division. Every SEC-registered firm should anticipate the SEC's increasing commitment to regulating cybersecurity and lack of sympathy for any sort of cybersecurity failure.

Morgan Stanley clearly made a mistake with respect to their internal systems and their slip-up

probably allowed a scheming employee to steal private client data — which in turn left that data vulnerable to external threats.

But whether their mistake should have cost them a $1 million penalty and the scarlet letter of an SEC enforcement action is debatable. Moreover,
by responding with speed, transparency, independency, integrity and vigor, Morgan Stanley, rather than being punished, actually deserves to be commended.

—By John Reed Stark, John Reed Stark Consulting LLC

John Reed Stark is the president of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. Formerly, Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, including 11 years as the chief of its Office of Internet Enforcement. He has also been an adjunct professor of law for 15 years at the Georgetown University Law Center, where he taught several courses on the juxtaposition of law, technology and crime, and a managing director of a global data breach response firm for five years. Stark is also the author of "The Cybersecurity Due Diligence Handbook," available as an e-book on Amazon, iBooks and other e-book distribution sites.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.