SEC and DOJ Hacking Prosecutions Highlight SEC’s Increased Interest in Cybersecurity Risks

posted on: Tuesday, September 15, 2015

Companies are reminded of the need for strong internal controls.

The US Securities and Exchange Commission (SEC) and the Department of Justice (DOJ) recently filed civil and criminal actions in the largest hacking and securities fraud scheme of its kind ever prosecuted.[1] During a five-year period, the defendants allegedly stole approximately 150,000 confidential press releases from the servers of three newswire companies that contained information prepared by scores of public companies. Unbeknownst to the companies, the defendant hackers, who appear to all be foreign nationals, then sold the press releases to traders who traded ahead of the confidential information’s public release and reaped millions of dollars in illegal profits.

This case highlights the need for companies to ensure that they have adequate internal controls that cover data transfer at all stages of the use and life cycle. Any weak link in a cybersecurity program may be exploited or used by hackers as a back door to gain access to information. In this case, the cyber attack targeted third-party newswires and not the companies that originally created and possessed the information. A strong cybersecurity program is essential for companies to protect valuable and sensitive information and to avoid possible enforcement actions, fines, reputational harm, loss of business, and class action or other lawsuits brought for damages suffered by customers or clients.

The SEC's focus is not limited to public companies. Recent findings by the SEC confirm the widespread nature of cybersecurity attacks in the financial industry. In February 2015, the SEC’s Office of Compliance Inspectors and Examinations (OCIE) released a Risk Alert announcing that it had examined scores of broker-dealers and investment advisers’ cybersecurity protocols.[2] Among the areas that the Risk Alert report focused on were identification and assessment of cybersecurity risks, risk associated with vendors and other third parties’ systems, detection of unauthorized activity, risks associated with remote customer access, and the absence of a chief information security officer and/or cyber insurance.[3] Strikingly, OCIE found that 88% of the broker-dealers and 74% of the investment advisers examined had experienced a cyber attack, either directly or through a vendor.[4]

The SEC’s increased emphasis on the adequacy of internal controls (generally) and cybersecurity at all stages of data transfer (specifically) should particularly interest public companies and financial institutions in their approach to detecting and mitigating cyber risks.

The Attack Targeted Newswires, Not Companies

In the newswires cases, although the material, nonpublic information belonged to public companies, the hackers did not attack the companies directly; rather, they focused on the three newswires. As alleged by the government, the public companies uploaded draft releases to the newswires’ restricted, nonpublic servers pursuant to contractual relationships whereby the newswires agreed to
keep the information confidential until public release. The press releases contained material nonpublic information about publicly traded companies, including unreleased earnings, revenue, and mergers information. In one instance, the defendants were able to access and trade on information in the 36 minutes between when the newswire received the information and its public release.

The government alleged that the hackers used a range of strategies—some rather simple, such as phishing email and stolen login information, and some more advanced, such as SQL injection attacks[5] and brute force attacks[6] to access the newswires’ servers. For years, the hackers allegedly possessed contact and credential information for one newswire’s employees, clients, and business partners. As alleged in one indictment, web server logs from one newswire show repeated and regular improper accesses to its servers.

Rather than attacking each public company, it is clear that the defendant hackers recognized that the newswires offered one single repository and single access point to highly valuable, confidential information about hundreds of companies. The newswires may have also presented a weak link by having weaker cybersecurity measures than the public companies themselves.

As the scheme matured and its success grew, traders allegedly sent “wish lists” of the publicly traded companies about which they sought inside information. The DOJ and SEC alleged the following lucrative nature of the scheme: the hackers obtained confidential information about hundreds of public companies, and the trader defendants executed approximately 1,000 inside-the-window trades, resulting in $30 million in profits.

The SEC has previously targeted hackers who obtain and trade insider information. In 2007, the SEC brought an enforcement action against a computer hacker who accessed confidential quarterly earnings reports by hacking into an investor’s public relations firm and obtaining material nonpublic information about upcoming negative earnings of a publicly traded company. In 2010, the hacker was ordered to pay roughly $580,000 in disgorgement, prejudgment interest, and a civil penalty.[7]

A Strong Detection System Is Necessary for Avoiding Liability

Companies must have a robust system in place, based on internal controls, to prevent, detect, and mitigate direct and indirect cyber attacks. Experts agree that the question is no longer whether an organization will suffer a cybersecurity breach, but when a breach will occur—or whether a breach has already occurred, as yet undetected by the company. Indeed, in the current environment, the key to fighting a cyber attack may be an organization’s ability to detect and quickly respond to a breach when it inevitably does occur. Although these recent enforcement actions targeted intentional efforts to steal and profit on material nonpublic information, the SEC’s focus goes beyond cybersecurity and insider trading. SEC Chair Mary Jo White has made clear that the agency will continue to bring actions against companies for inadequate internal controls under the “Broken Windows” theory.[8]

The SEC recently brought an action for failing to have adequate controls in place.[9] It also reportedly asked eight listed companies to provide information on data breaches in connection with a sophisticated hacking group “that has tried to hack into emails at more than 100 companies looking for information on mergers and other market moving events.”[10] In a June 25 speech, SEC Commissioner Luis Aguilar emphasized that the SEC is “proactively examining how it can bring more cybersecurity enforcement actions” and suggested the need for further SEC guidance.[11] The SEC has also noted that companies may have disclosure obligations after a cyber attack.[12]

Other Recent Enforcement Developments

Other federal and state agencies are also initiating aggressive enforcement actions when a company fails to have an adequate cybersecurity program, and the courts have been validating these enforcement efforts. As most recently evidenced by the FTC v. Wyndham decision, the US Court of Appeals for the Third Circuit agreed that the Federal Trade Commission (FTC) had stated a claim for unfair and deceptive trade practices by, inter alia, alleging that the defendant, which experienced three cyber attacks resulting in a theft of consumer data, had not used commercially reasonable methods for protecting consumer data and overstated its cybersecurity protections in its published privacy policy.[13] Further, the Third Circuit rejected the defendant’s argument that it did not have fair notice of its cybersecurity obligations, citing past FTC actions regarding cybersecurity.

This case confirms that companies’ failure to adequately protect valuable and sensitive confidential
Preventing and Responding to Data Security Breaches and Keeping Ahead of the Changing Regulatory Environment

What can you do today to protect data? Be proactive. Here are some recommended steps that companies can take now to prevent cybersecurity loss and to strengthen your cybersecurity program.

1. Protect Valuable Data
   Effective cybersecurity requires a tailored program to protect data that may be at risk. Companies should first identify information of value, such as trade secrets, other intellectual property, confidential business or customer information, or financial assets. A risk assessment should be conducted to mitigate against any weak links that hackers or insiders may exploit. An information protection plan should be carefully tailored and designed to protect the information against risk of attack, theft, or loss.

   Hackers come in all forms with different agendas, from profiteer to “hacktivist.” Do you understand which information hackers value and which will cause your company harm? Is high-value information found in multiple locations, including some that might be more vulnerable than others? Have you assessed possible weak links, such as third parties?

2. Manage Cyber Risk
   Enforcers expect that companies have appropriate oversight and review controls to manage cyber risk. Commissioner Aguilar noted on this point, “Given the significant cyber-attacks that are occurring with disturbing frequency, and the mounting evidence that companies of all shapes and sizes are increasingly under a constant threat of potentially disastrous cyber-attacks, ensuring the adequacy of a company’s cybersecurity measures needs to be a critical part of a board of director’s risk oversight responsibilities.”

   Consider the following: How do you manage cyber risk? Do you have dedicated information security personnel? Is your board of directors cyber savvy, educated on cybersecurity risks, and able to conduct appropriate oversight, such as reviewing budgets for cybersecurity programs and receiving reports on breaches and risks? Does your board’s risk committee consider cyber risks? Does your company have cyber insurance that covers not only the breach, but also data loss and restoration of services?

3. Monitor and Detect
   Have a clear understanding of your company’s ability to monitor and detect attacks. The ability to detect cyber intrusions and attempted intrusions is critical to stopping access. Do you have a detection program in place? How good is it? How well are you monitoring for cyber threats and attacks? In the attack discussed above, the allegations suggest that the newswires varied widely in their detection abilities. The SEC has repeatedly noted the value of detection and monitoring cyber attacks.

4. Prepare and Test Incident Response Plans
   Does your company’s data response plan include a data map that shows your systems, data, needs, and risks? Does it address detection and monitoring of risk, as well as remediation? Does it show when and to whom confidential information is transferred? Does it include third parties that have access to your company’s confidential information? Does the data breach identify a response team, including your internal contacts and decisionmakers as well as outside contacts, including counsel, insurance, crisis management, and the appropriate law enforcement? When was the last time that you tested your data response plan?

5. Third-Party Vulnerabilities
   Review your contracts with third parties and insurance coverage for third-party breaches. The SEC has mentioned third-party vendors as an area of concern, and the recent indictments demonstrate that hackers are targeting third parties. A hack of your company’s information by a third party is still a data breach of your information. Have you done due diligence with regard to the cybersecurity system used by third-party vendors? Do your contracts with third-party vendors that have access to your company’s confidential information clearly outline obligations...
in the event of a data breach and cyber attack? Does the third party have appropriate insurance coverage for cyber risks?

6. **Assess and Audit**

Consider auditing a third-party vendor’s cybersecurity protocol. Again, a hack of your company’s information from a third party is still a data breach of your information. What is your obligation to make sure that your confidential information shared with a third party is protected? Are the third parties that your company trusts with sensitive data taking appropriate steps to protect your confidential data? What is your liability for a breach at a third party? These issues need to be discussed.


[4] OCIE found that most broker-dealers incorporate requirements relating to cybersecurity risk into their contracts with vendors and business partners (72%) while only a few investment advisers were found to have incorporated such requirements (24%). Similarly, only a slim majority of broker-dealers maintain policies and procedures related to information security training for vendors and business partners authorized to access their networks (51%), whereas fewer than 15% of investment advisers have such policies (13%). Id.

[5] SQL injection attacks are methods of gaining access to computers connected to the Internet by using malicious SQL instructions (SQL is a computer programming language to retrieve and manage data in a computer database).

[6] “Brute force” refers to a method of decrypting data through exhaustive efforts that can be used to reveal unencrypted passwords.


Copyright © 2015 by Morgan, Lewis & Bockius LLP. All Rights Reserved.