Bloomberg BNA

Daily Report for Executives™

Cybersecurity

In August, DOJ and SEC charged hackers and securities traders in an alleged $100 million scheme that hacked and profited from unpublished market-moving financial press releases. Authors Matthew Baughman, Chris Burris, Nick Oldham, and Jimmy Michaels of King & Spalding LLP say the case demonstrates the growing importance of managing third-party cyber-risks; the increasing activity of DOJ and SEC in this area; and the need for counsel to better understand the evolving nature of cyber-forensics.

Unprecedented Hacking and Trading Scheme Highlights Key Cybersecurity Lessons

By Matthew Baughman, Chris Burris, Nick Oldham, and Jimmy Michaels

On Aug. 11, 2015, federal prosecutors in the District of New Jersey and the Eastern District of New York unsealed indictments against nine individuals in the U.S. and Ukraine who were allegedly involved in a five-year, widespread hacking and trading scheme.[1] On the same day, the Securities and Exchange Commission filed a complaint in federal district court in New Jersey making similar allegations.[2] The defendants allegedly hacked into major news wires that distribute press releases, stole advance, not yet public copies of financial press releases, and traded on the basis of the information, reaping over $100 million in unlawful profits.

I. An Unprecedented Hacking and Trading Scheme

According to the indictments and parallel SEC civil complaint, the scheme involved two key groups of defendants. The first group is alleged to be comprised of sophisticated hackers who broke into the computer and data networks belonging to PR Newswire, Business Wire, and Marketwired. The hacking team allegedly used brute force attacks, SQL injection attacks, and phishing attacks to gain access to the media organizations' networks, and then after illegally obtaining access they stole advance, nonpublic copies of financial press releases. Hundreds of publicly traded companies, including some of the biggest names in corporate America, use these three media services to disseminate news to the market place, including earnings reports and other financial information. As standard practice, publicly traded companies may send current versions of their financial press releases to the media services several minutes to several days before publication.

[1] *See* Indictment, *U.S. v. Turchynov et al.*, No. 2:15-cr-00390 (D.N.J. Aug. 6, 2015), Doc. 1; Indictment, *U.S. v. Korchevsky, et al.*, No. CR-15-381 (E.D.N.Y. Aug. 5, 2015), Doc. 1.

[2] *See* Complaint, *Securities and Exchange Commission v. Dubovoy et al.*, No. 2:15-cv-06076 (D.N.J. Aug. 10, 2015), Doc. 1.

Matthew Baughman *is a partner in King & Spalding's Atlanta office, and a former SEC enforcement attorney.*

Chris Burris *is a partner in the Atlanta office. His practice focuses on white collar criminal defense, corporate internal investigations, defense of regulatory enforcement actions.*

Nick Oldham *is a counsel in the Washington office. He is a former Assistant U.S. Attorney focused on cybercrime and former Counsel for Cyber Investigations for DOJ's National Security Division.*

Jimmy Michaels *is an associate in the Atlanta office.*

 ISSN 0148-8155

The second group of defendants is alleged to be comprised of traders who received the stolen financial press releases from the hackers. The traders allegedly used the market-moving information contained in the releases as the basis for trading in the stock and options of the relevant companies prior to the news being made public, anticipating (usually correctly) that the news in the releases would cause the value of the securities to rise or fall in their favor.

The traders had to work quickly: in some instances, they had under an hour to execute trades based upon the draft press releases. For example, on Aug. 3, 2011, the hackers allegedly stole a draft press release that was uploaded to one of the media organizations at 3:34 PM, traded on the basis of the information in the draft release at 3:56 PM, and then reaped a windfall profit of over $2.3 million after the press release was made public at 4:01 PM.

The traders involved with the scheme paid the hackers handsomely for the stolen information, providing the hackers with either a flat fee or a percentage of profits on a per-trade basis. In all, over 150,000 news releases were allegedly stolen by the hackers, and the traders allegedly made over 800 trades based upon the information in those news releases. Some of the individual trades discussed in the complaint and indictments yielded over $1 million in profit.

II. Important Takeaways

The recent indictments and SEC complaint highlight several important lessons:

A. Third-Party Risk Management: Cornerstone of Well-Functioning Cybersecurity Programs

Although the indictments and SEC complaint in the most recent action do not provide details about the contractual relationship between the public companies whose financial releases were stolen and the media services that had custody of those not yet public releases, the fact that company information was misappropriated underscores the importance of knowing who has access to a company's most critical assets, and assuring that protections are in place to protect those assets. Moreover, recent regulatory actions have revealed an increased interest by regulators in exploring how companies manage third-party cybersecurity risks.

Third party vendors are common in the modern corporate environment. The cybersecurity chain is only as strong as its weakest link, so evaluating the cybersecurity measures taken by those third parties—and confirming that strong measures have been implemented—should be considered a basic prerequisite to the sharing of sensitive information with those third parties or allowing those third parties network access. Companies that share information with third parties or grant third parties network access without confirming the effectiveness of the third parties' cybersecurity programs could be challenged as acting unreasonably, and could themselves be criticized as having deficient cybersecurity programs due to their failures to account for these third party risks.

More generally, cybersecurity issues can quickly cause good business relationships to turn sour. It is often better for companies to negotiate the right contractual and governance protections on the front end, *i.e.* when parties are originally contracting, instead of being left to deal with cybersecurity issues on an *ad hoc* basis after the fact. Thus, companies should consider robust cybersecurity due diligence processes before engaging third parties, and should also consider including appropriate protections in their contractual agreements, such as: express definitions of the security policies and procedures third parties must follow (along with rules governing audits of those security policies and procedures); liability and indemnification provisions that fairly address the risks posed; and how and when third parties must provide notification of cybersecurity incidents. Because the cybersecurity risks and the related legal risks created by allowing third parties to access sensitive data can be highly fact specific and intricate, and because this is a constantly evolving area of law, we urge companies to review and revise third party risk management programs with the advice of experienced technical advisors and counsel. When dealing with cybersecurity threats, an ounce of prevention is almost always worth more than a pound of cure.

The SEC has specifically identified third party risk management as an area of concern for the financial institutions it regulates. The results of a recent cybersecurity examination sweep conducted by the SEC staff confirm that many financial institutions do not consider the cybersecurity implications of their relationships with third party vendors to the degree the SEC staff believes they should.[3]. The SEC survey specifically asked financial institutions several questions about cybersecurity risks arising from granting network access to vendors and other third parties. According to the sweep, while 84 percent of broker-dealers require cybersecurity risk assessments of third party vendors that are given access to a company network, only 72 percent incorporate cybersecurity requirements into their contracts with those vendors. The results for the surveyed investment advisers paint a more sobering picture: only 32 percent of investment advisers require cybersecurity risk assessments from third party vendors, and only 24 percent incorporate cybersecurity requirements into vendor contracts.

Other regulators have also recently made statements showing that they consider third party risk management to be a key element of a robust cybersecurity program. For example, the New York Department of Financial Services published a report in April 2015 detailing the results of a survey about the measures taken by banks to ensure that the banks' third party service providers maintained reasonable cybersecurity programs.[4]

B. Interactions Between Companies and DOJ and SEC on Cyber Issues Are Dramatically Increasing

The DOJ and the SEC have aggressively stepped up their efforts to address cyber threats. As a result of this increased governmental activity, the level of interaction between companies and these agencies on cyber issues

[3] *See* U.S. Securities and Exchange Commission, Office of Compliance Inspections and Examinations, *Cybersecurity Examination Sweep Summary*, National Exam Program: Risk Alert (Feb. 3, 2015), available at https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

[4] *See* New York State Department of Financial Services, *Update on Cyber Security in the Banking Sector: Third Party Service Providers* (April 2015), available at http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf.

  DER ISSN 0148-8155

has increased—and will continue to increase—dramatically, and therefore companies must be prepared to explain the security measures they have in place to maintain the confidentiality of sensitive information. The increased attention to cyber threats creates a greater burden on businesses in responding to government investigations and requests for information, and highlights companies' need to become more familiar with the process of responding to cyber-related government inquiries.

The DOJ, for example, has made cybersecurity a primary focus of its attention. Two common scenarios in which companies interact with the DOJ on cyber issues are: (1) ongoing investigations into data breaches or other security incidents, some of which involve an investigative agency affirmatively notifying a company that it is a cybercrime victim; and (2) general public-private party outreach efforts including sharing of potential threats and vulnerabilities. In each of these scenarios, companies might interact with one or more of the following three principal DOJ components involved in cybercrime prosecutions: the Criminal Division's Computer Crime and Intellectual Property Section (''CCIPS''), the National Security Division (''NSD''), and any one of the 93 individual United States Attorney's Offices (''USAOs''). CCIPS is the DOJ's cybercrime subject-matter experts. NSD is the DOJ's national security subject-matter experts and combats cyber-based threats to national security. USAOs are the DOJ's front lines in prosecuting cybercrime, and frequently interface with cybercrime victims. These three groups combined form a network of over 300 DOJ cyber prosecutors.

In addition to its bread-and-butter investigations, the DOJ has also addressed cybersecurity from a policy perspective. For instance, earlier this year, the DOJ hosted a ''Cybersecurity Industry Roundtable'' to discuss data breaches, best practices in responding to data breaches, and ongoing cybersecurity legislative initiatives. During the Roundtable, the DOJ issued a document titled *Best Practices for Victim Response and Reporting of Cyber Incidents*.[5] The guidance provides a checklist of steps that companies can take before, during, and after a cyber incident, and restates DOJ's position regarding network monitoring and offensive actions colloquially known as ''hacking back.'' [6]

The SEC has been active in the cybersecurity arena as well. In addition to overseeing the cybersecurity practices of regulated entities such as broker-dealers and investment advisers, the SEC has interpreted its broad and overarching mandate to ensure transparency in the securities marketplace as permitting the agency to regulate cybersecurity-related disclosures of public companies and to bring cybersecurity-related enforcement actions. It is likely that the SEC will continue to police matters, such as those seen in this hacking case, where criminals have used new, cyber techniques to commit old-fashioned crimes like securities fraud and insider trading. The SEC has also proactively reached out to victimized companies to gather information in the course of its investigations. In the ''FIN4'' matter, for example, a group of hackers allegedly obtained inside information from various corporate bankers, lawyers, accountants, and consultants, and the SEC staff investigating the matter reached out to several victim companies requesting information about the data breaches and the tactics used by the FIN4 group to gain access to their networks. As sensitive information becomes more widely circulated through electronic means, businesses' vulnerabilities to cyber attacks will increase, and the SEC will likely expand its oversight of the cyber arena as it relates to the financial markets. When faced with a subpoena or request for information from the SEC, companies must be prepared to answer tough questions about their cybersecurity measures, including being able to fully describe the steps they have taken to maintain the confidentiality of sensitive information in their possession.

C. The Importance of Forensics In Modern Cases

The indictments and SEC complaint highlight the growing importance of forensics in government investigations, especially investigations involving cyber-related issues. As a result, in many cases, it is essential for counsel to understand the types of forensic tools that prosecutors and other forensic computer experts have at their disposal when interacting with the government, especially as more and more cases are relying upon advanced forensic techniques to uncover misconduct. The SEC complaint in the most recent hacking case, for example, notes that the defendants ''took extensive measures to conceal their fraud.'' In some respects, the defendants were successful—their scheme lasted for five years. However, one of the apparent missteps the defendants made was believing that pictures taken with ''a smartphone application that does not retain data'' would be permanently deleted and therefore unrecoverable. While such data may be unrecoverable from the picture taker's device, as soon as that data is transmitted to a recipient, the recipient can do as he pleases with it, which could include retaining it. If, as here, the data is later sent via e-mail, it will likely be retained in some form.

Also of note here is that computer forensic technologies have advanced by great measures in recent years, such that data that is merely deleted from a hard drive or an inbox might still be recoverable in some form. Without extraordinary measures being taken to evade detection, it is usually a fair bet that a user's steps can be traced and that any data the user believed was deleted can, in fact, be recovered.

III. Conclusion

Hackers and other criminals seeking to profit off of material non-public information have found a new avenue for obtaining this valuable information: exploiting third parties that are given access to this data in good faith. It is important to remember that a well-crafted cybersecurity program must consider the protections afforded to sensitive data even once it has left a company's possession, especially in the face of increased cybersecurity enforcements by the DOJ, SEC, and other law enforcement entities and regulators.

---

[5] *See* U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, Cybersecurity Unit, *Best Practices for Victim Response and Reporting of Cyber Incidents* (April 2015), available at http://tinyurl.com/q5g82pv.

[6] *See* King & Spalding LLP, *Data Privacy & Security Practice Report* (May 4, 2015), available at http://www.kslaw.com/News-and-Insights/PublicationDetail?us_nsc_id=8781.