Bloomberg BNA

Corporate Law & Accountability Report™

DATA BREACHES

Recent Cyber-Attack Developments Highlight The Importance of Corporate Attention and Action






By Rajesh De, Marcus Christian, Richard Rosenfeld, Alex Lakatos, Mark Hanchet and Matthew Bisanz

Rajesh De is a partner in Mayer Brown's Washington, D.C., office and leads the firm's global Cybersecurity & Data Privacy practice.

Marcus Christian is a Washington, D.C., partner in Mayer Brown's Litigation & Dispute Resolution practice and White Collar Defense & Compliance group.

Richard M. Rosenfeld co-leads Mayer Brown's U.S. Securities Litigation & Enforcement group, working from both the Washington, D.C., and New York offices.

Alex Lakatos is a partner in the Washington, D.C., office of Mayer Brown's Litigation and Financial Services Regulatory and Enforcement practices.

Mark Hanchet is a partner in Mayer Brown's New York office and co-leads the firm's banking and finance litigation practice.

Matthew Bisanz is a Financial Services Regulatory and Enforcement associate in Mayer Brown's Washington, D.C., office.

The Department of Justice (DOJ) and Securities and Exchange Commission (SEC) recently announced the first prosecutions and first civil enforcement action resulting from an alleged scheme to obtain material, nonpublic information via hacking, and to use that information to make insider trades (13 CARE 1796, 8/14/15). Coming after FireEye's 2014 disclosure of "FIN4," a group that FireEye described as hacking companies' communications and possibly profiting from using stolen information for insider trades, the alleged facts in this prosecution illustrate the increasing variety, impact, sophistication and impact of cybercrimes. Gone are the days when cybercriminals overwhelmingly focused on personally identifiable information and payment card information. Although such attacks are still common, they represent only one type of an ever-expanding array and volume of attacks. Special Assistant to the President and Cybersecurity Coordinator Michael Daniel recently noted that cyber-attacks are taking up a "greater and greater percentage of the president's daily briefings."[1] Companies likewise must pay more attention to growing cybersecurity risks and implement appropriate responses.

[1] Drew Clark, "White House Cybersecurity Czar Highlights Escalation Paths for Cyberdefense, Highlights 'Risk-Management,'" BroadbandBreakfast (Aug. 17, 2015), http://goo.gl/LNu4QB.

 ISSN 2330-6300

Newswire Hacking

The August 2015 indictments in New Jersey and the Eastern District of New York and SEC enforcement action focus on the alleged hacking of three newswire services that held and disseminated press releases for publicly traded companies. To execute the scheme, the defendants primarily operated in two groups, ''Hackers'' and ''Traders.'' The Hackers compromised the computer networks of three newswires and stole unpublished press releases containing material information about public companies. The Hackers then shared these press releases with the Traders, who bought and sold the securities of public companies prior to the publication of the press releases. The Traders profited from the resulting price changes and paid the Hackers a percentage of the insider trading profits.

The newswire hacking scheme allegedly operated from February 2010 until May 2015 and involved the theft of more than 150,000 press releases. The defendants executed trades using more than 800 of these press releases and realized more than $100 million in illicit profits, according to the government. The defendants also allegedly disseminated the stolen press releases electronically to third parties to facilitate further insider trading.

The Hackers allegedly used a variety of attacks to compromise the newswires' servers. In some instances, they sent phishing e-mails to newswire employees that contained links to malicious software that enabled the Hackers to compromise a computer when an employee clicked on the link. In other instances, the Hackers used Structured Query Language or SQL injections, a well-known hacking technique, to compromise the newswires' networks. In particular, the Hackers used the technique to extract usernames and passwords from the newswires' websites. The defendants then used the usernames and passwords to remotely access the websites and download press releases.

On at least two occasions, one of the newswires detected the Hackers' activity and terminated their unauthorized access. It is unclear if the newswire reported the incidents to law enforcement, but the Hackers were undaunted. They merely shifted their focus to the other two newswires, while attempting to re-infiltrate the network that had terminated their unauthorized access.

FIN4 Hacking

The prosecution of the newswire hacking defendants came shortly after news emerged that the SEC had begun investigating the hacking-for-profit activities of a group generally known as ''FIN4.'' Cybersecurity firm FireEye disclosed the existence of FIN4 in a late-2014 report about the group. According to the report, FIN4 has attacked more than 100 companies, mostly in the pharmaceutical and health-care industries, to obtain material, non-public information to facilitate insider trading.

FIN4 has operated by hacking e-mail accounts belonging to people thought to have sensitive corporate information, such as lawyers, investment bankers and investor relations firms. FIN4 then used the hacked accounts to impersonate the e-mail account holders and send phishing e-mails to their fellow employees and to recipients at other targeted companies to acquire information useful to their insider trading activities, including draft SEC filings, ''merger activity, discussions of legal cases, board planning documents and medical research results.'' It is unclear whether FIN4 actually traded on the information it acquired, but the type of data that the group sought strongly suggests that it did.

Tips for Businesses

Organizational victims of cyber intrusions often fail to respond meaningfully to computer security events before significant damage occurs. To minimize the likelihood of this result, companies should ensure that their cybersecurity defenses and incident response preparations adequately address the challenges posed by evolving cyber threats. Among other things, this includes:

- **Participating in industry-specific Information Sharing and Analysis Centers (ISACs).** It is not known if the newswire that detected the hackers at an early stage disclosed the attack to an ISAC. Nevertheless, participation in an ISAC provides access to valuable information about current threats and facilitates the coordination of industry-wide action in response to emerging vulnerabilities.
- **Cooperating with law enforcement agencies strategically.** US Attorney General Loretta Lynch has stressed the need for companies to work ''collaboratively [with the DOJ] to identify and notify victims, minimize the impact of an intrusion and help prevent similar attacks in the future,''[2] and the pending newswire hacking cases reflect this trend of greater cooperation between the DOJ and other law enforcement and regulatory agencies during investigations. According to press releases, the DOJ and the SEC worked with the Department of Homeland Security, the Secret Service, the FBI, FINRA, the U.K. Financial Conduct Authority, and the Danish Financial Supervisory Authority to investigate the newswire hacks.[3] A recent report from the National Institute of Standards and Technology indicates that further coordination of this kind is not only likely, but also imperative to combating cybersecurity threats.[4] Companies realize the greatest benefits from law enforcement agencies by working proactively with them before crises, not simply during them. This approach allows the businesses to obtain useful preventative information, build rapport and strengthen incident response preparedness.
- **Use automated threat detection tools.** Many companies use passive defenses designed to ''harden''

[2] Attorney General Loretta E. Lynch, Remarks at the Department of Justice Cybersecurity Symposium (July 21, 2015), *available at* http://www.justice.gov/opa/speech/attorney-general-loretta-e-lynch-delivers-remarks-department-justice-cybersecurity (see also 13 CARE 921, 5/1/15).

[3] Press release, Department of Justice, ''Nine People Charged in Largest Known Computer Hacking and Securities Fraud Scheme'' (Aug. 11, 2015); press release, U.S. Securities and Exchange Commission, SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases (Aug. 11, 2015).

[4] Michael Hogan & Elaine Newton, *Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity* (NIST, 2015), NISTIR 8074 Volume 1 (Draft), *available at* http://csrc.nist.gov/publications/drafts/nistir-8074/nistir_8074_vol1_draft_report.pdf.

   ISSN 2330-6300

their IT infrastructure against attacks, while neglecting active threat detection tools. For example, if a company uses a VPN for off-site access to e-mail, it may want to cross-reference the login locations with expected employee locations. According to FireEye, FIN4 hackers used anonymizing Tor[5] webservers to log into employee e-mail accounts. Given hackers' common use of Tor servers to launch attacks, automated threat detection tools can bolster cyber defenses by instantly flagging login attempts from Tor servers.

- **Monitor all third-party service providers.** Companies frequently monitor the cybersecurity activities and implementations of certain key third-party service providers, such as credit card acquirers, payroll processors and health insurers, but fail to monitor other providers that have access to core systems. For example, a company providing company e-mail addresses to independent contractors should obtain the independent contractors' cybersecurity and HR policies to ensure that all persons with company e-mail addresses have appropriate backgrounds and follow consistent access policies. Another example would be requesting SSAE 16/SAS 70 reports from all third-party service providers, even if the services some provide are not deemed ''key'' to the company.[6]

These are but a few of the steps that companies can take to reduce their exposure to ever-growing cybersecurity and data privacy risks. The alleged breaches by the newswire hackers and FIN4 underscore that no company can rely upon the adage, ''What you don't know can't hurt you.'' Businesses at the forefront of protecting their sensitive information and digital assets realize that what they do know (and what they do as a result) can help them immensely.

[5] Tor, originally known as ''The Onion Router,'' is a service that permits users to conceal their location and activities by using a network of third-party relay computers to anonymize the source of any action on the Internet.

[6] SSAE 16 and SAS 70 are auditing standards for providing a ''Service Organization Controls'' (SOC) report that discloses a third-party service provider's activities and processes to its customers in a uniform reporting format.