Harvard Law School Forum on
Corporate Governance and Financial Regulation

SUPPORTED BY:
pwc

Insider Trading: When Hackers Target Corporate Shares

Posted by Evan Bundschuh, Gabriel Bundschuh & Assoc. Inc., on Sunday, May 14, 2017

Editor's note: Evan Bundschuh is vice president and commercial lines head at Gabriel Bundschuh & Assoc. Inc. This post is based on a GB&A publication by Mr. Bundschuh.

When data breaches target credit card numbers and personal information, the damage can be quantified, however when hackers explicitly target a company's shares that damage is much more unpredictable. Insider-Trading hacks are akin to coming home to find your house has been (somewhat silently) broken into—but was anything stolen? And how long will it take to discover? Did they vandalize anything in the process? Did they install any backdoors? These are big problems when shareholders are involved.

When discussing securities-related cyber threats and market manipulation, the first real warning shot was fired in December of 2014 when a hacktivist group FIN4 launched a targeted attack seeking M&A data for purposes of insider trading. The first significant data breach of its kind with the intent on "playing the market"—carefully executed and disguised through a sophisticated network. A few months later a significantly larger scheme was brought to light exposing a 5 year intrusion that affected PRNewswire and others, which netted an approximate profit of $100 Mill for the hackers. Today, the sound of that warning shot continues to echo louder and louder. In the past few months alone we have seen an IT employee at Expedia utilize false credentials to access and trade on inside information and the SEC and DOJ announce cases against Chinese traders who profited ~ $4 Mill by targeting M&A data held by law firms.

With each echo, the once blurry lines are becoming clearer. In perpetrating these schemes, cyber criminals will access information and place appropriate trades prior to public release, or access information and weaponize the data by slightly altering figures in order to illicit a direct response which they can then capitalize on. Most of the intrusions up until now, have been carried out by isolated but well-coordinated small groups, often originating from Eastern Europe or Asia. For obvious reasons, hacks deployed with the intent of manipulating the market revolve heavily around financial statements/restatements and information regarding upcoming mergers and acquisitions. But materiel non-public information comes in many shapes and sizes, and, as is the nature of cyber security, a certain level of foresight is required in order to strategize a defense. Other information that could become targeted includes: information related to the loss/gain of large contracts, new offerings and executive/personnel movements.

The duration of the intrusions and "time-to-discovery" appears to average 2-4 years which provides a large window which can inflict significant damage. While hackers are experimenting with increasingly sophisticated methods of deception/intrusion, most intrusions have been executed through fairly traditional means such as malware, obtaining of login credentials, social engineering, and spear-phishing campaigns. These intrusions are generally directed at the C-

suite, employees operating in the legal and accounting departments and 3rd party providers such as law firms in the care/custody of such information.

It's long been known that any organization with fingerprints on corporate non-public information are likely targets. While law firms and news publications have historically been the most lucrative targets thus far, all organizations that work with public companies should be paying close attention. It's safe to assume that any firm engaged with accounting/auditing, consulting or financial advising may be the next targets due to their custody of high value information. Most of the intrusions thus far have targeted larger firms, likely because public company contracts tend to be awarded to the larger firms, however smaller firms should be careful not to dismiss the risk. Boutique firms with specialties catering to public companies may be viewed as "soft targets" due to lacking cyber controls. Service providers should also be cognizant of the information they are in possession of, employing additional security controls around any material non-public information.

Most of these schemes are exploited through human error/vulnerabilities which is why employee training might seem like an obvious first step in deterrence. Many articles have touted employee training as the holy grail of cyber security, and while it is an important element which should undoubtedly be implemented, I disagree with that statement. It is far from the ideal solution. Ensuring compliance with such education and internal controls is extremely challenging. It is very difficult to train employees to consistently verify the validity of every…single…email (or file). The attacks are also becoming better at camouflaging themselves and employee judgement only becomes impaired when busy or tired. These intrusions are also a numbers game. In a flood of attacks it only takes one mistake for the introduction the hacker requires. The most recent hack demonstrates this perfectly, with the hackers relentlessly targeting the law firms in excess of 100,000 separate attacks. How can a company defend against that? It is like asking employees to perform 100% of the time, at a task that is already mundane when the numbers are entirely stacked against them. Unfortunately there is no one "magic shield"—the only solution at the moment appears to be a combination of employee training, internal policies/controls and implementation of advanced prevention and detection software. Additionally, companies can also explore network separation methods and/or the implementation of multi-factor authentication in order to verify authenticity. Companies looking for early identification of potential employee-based inside attacks have a number of options available, from software that identifies trading patterns to employee surveillance.

Insurance implications pose yet a separate challenge. Assume that a company learns of a breach that has prematurely exposed financial restatements. It's assumed that hackers will use this information for trading purposes. With no real damages having occurred, and a securities exclusion contained in the policy, the company's cyber insurance policy is generally viewed as unresponsive at this point. With that information, the company decides not to report the activity or file a claim, however a year and a half later it is discovered that the same hack had exposed the personal information of its customers. The insurance carriers are likely to decline coverage for any resulting costs on the grounds of being prejudiced by the late reporting of an incident that should have been reported earlier. If that same incident triggers a shareholder suit, the waters get even muddier. The solution to avoiding any unexepected insurance surprises post-loss, is to partner with a broker/attorney with a concentration on executive/cyber risk, reviewing all incidents as they are detected. Due to the fact that cyber policies are not currently crafted to respond to resulting securities claims, the C-suite should perform extra diligence in the placement of well-

structured D&O insurance, paying careful attention to the numerous potential cyber exclusions (and the required carve backs). Back to the example of the home robbery we opened with—the difficult nature of not knowing exactly what else the hackers may have accessed, combined with the long time-to-discovery is problematic to say the least. For this reason, D&O programs should be supplemented with cyber insurance to address any residual damage. These hacks also pose a unique problem—as opposed to theft of personal information which can be viewed as more smash-and-grab, hackers executing these intrusions prefer to remain as silent as possible which can make them more difficult to detect.

Lastly, in order to stay one step ahead, it's important to consider how these schemes may evolve. It is conceivable that these attacks may progress to target particularly volatile stocks, including smaller companies who may be viewed as softer targets. In addition, hackers may place trades well in advance of deploying manipulation tactics in an attempt to bypass detection. Combine this with more creative means of manipulation and things become messy. Something as seemingly innocuous as social media account takeover could be utilized to spread misinformation. Seemingly small announcements can result in large swings as demonstrated by the Facebook announcement from the CEO of Netflix which saw shares increase ~15%. Consider the scenario of a hacker gaining access to the social media accounts of a CEO at a company whose stock is particularly volatile. The hackers spread misinformation such as a declining consumer-base or impending regulatory investigation. This information in its own right would be enough to illicit a stock drop, however, when you consider that the announcement may also appear as a regulation FD violation (due to its announcement over social media), that drop may become compounded. While the stock will likely rebound upon the news of foul play, concerns of cyber security issues at the company may continue to plague shareholders. Luckily this is an area in which the SEC has been paying close attention to and investing considerable resources. They have also been extremely effective at detecting suspicious trading patterns through the usage of enhanced surveillance software and sophisticated analytic tools.