SEC crackdown on cyberfraud looms large

Understanding the cybersecurity risk and prevention methods

Prepared by:

Andrew Weidenhamer, Director, RSM US LLP
andrew.weidenhamer@rsmus.com, +1 703 336 6572

Sean Renshaw, Director, RSM US LLP
sean.renshaw@rsmus.com, +1 312 634 4757

March 2019

On Oct. 16, 2018, the U.S. Securities and Exchange Commission (SEC) issued a report[1] stating that inadequate prevention of cyber-related fraud may violate the internal accounting control provisions of the Securities Exchange Act of 1934. This report summarizes the SEC's investigations of nine issuers spanning numerous industry sectors that lost millions of dollars as a direct result of cyber-related frauds.

The report goes on to indicate that in those frauds, company employees received a targeted phishing email appearing to be from a company executive or a major vendor, either from a spoofed address or from a compromised account. The email directed the victim to wire large sums of money to, or pay invoices to, seemingly legitimate accounts that were actually controlled by the fraudster. The FBI estimates that these business email compromise (BEC) attacks have caused over $5 billion in losses since 2013, with an additional $675 million in adjusted losses in 2017 alone.

While the SEC has declined to pursue enforcement action in these matters to date, the report reminded companies of their control requirements and has left open the potential for future enforcement actions. The Commission is advising issuers that "internal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds."

These statements by the SEC indicate a shift towards stricter practices to address cyberthreats, underscoring the importance for internal education.

The SEC made it clear that public companies subject to section 13(b)(2)(B) of the Securities Exchange Act—the federal securities law provision covering internal controls—have an obligation to assess and calibrate internal accounting controls for the risk of cyberfrauds and adjust policies and procedures accordingly.

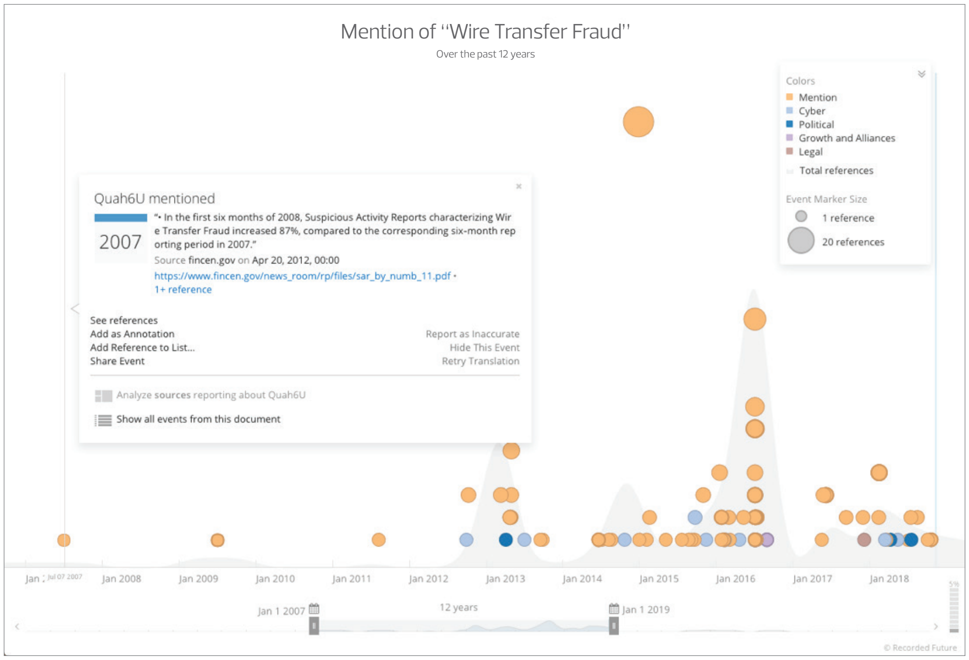
[1] "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements," Securities and Exchange Commission, accessed Feb. 25, 2019, https://www.sec.gov/litigation/investreport/34-84429.pdf.

Wire fraud over the years

Wire transfer fraud attacks have been around for decades. Over the past few years, these attacks have increased significantly and the method of attack has become more sophisticated. Largely gone are the days of the exiled "prince" who is trying to get his money out of his home country via phone or written letters, as the fraudsters turn to email and other technology as the primary medium to perpetuate their fraud.

Based on an analysis using Recorded Future,[2] Figure 1 shows the first mention of "wire transfer fraud" dating as far back as 2007, and it's reasonable to assume that these types of attacks were occurring before then. Additionally, Figure 1 shows a large cluster of mentions for this technique over the past few years, corroborating the recent rise in popularity assertion.

Figure 1



Quah6U mentioned

2007 "• In the first six months of 2008, Suspicious Activity Reports characterizing Wire Transfer Fraud increased 87%, compared to the corresponding six-month reporting period in 2007."

Source fincen.gov on Apr 20, 2012, 00:00

https://www.fincen.gov/news_room/rp/files/sar_by_numb_11.pdf •

1+ reference

So why the surge? In general, wire transfer fraud scams fall under the broader email fraud social engineering umbrella which is a threat vector that, according to Proofpoint, is not only an increasing threat but one that has risen 87 percent year-over-year. As attackers continue to be mainly motivated by financial gain, they are constantly evolving their attack techniques to optimize their return on investment (i.e., perform the least amount of work for the most amount of money).

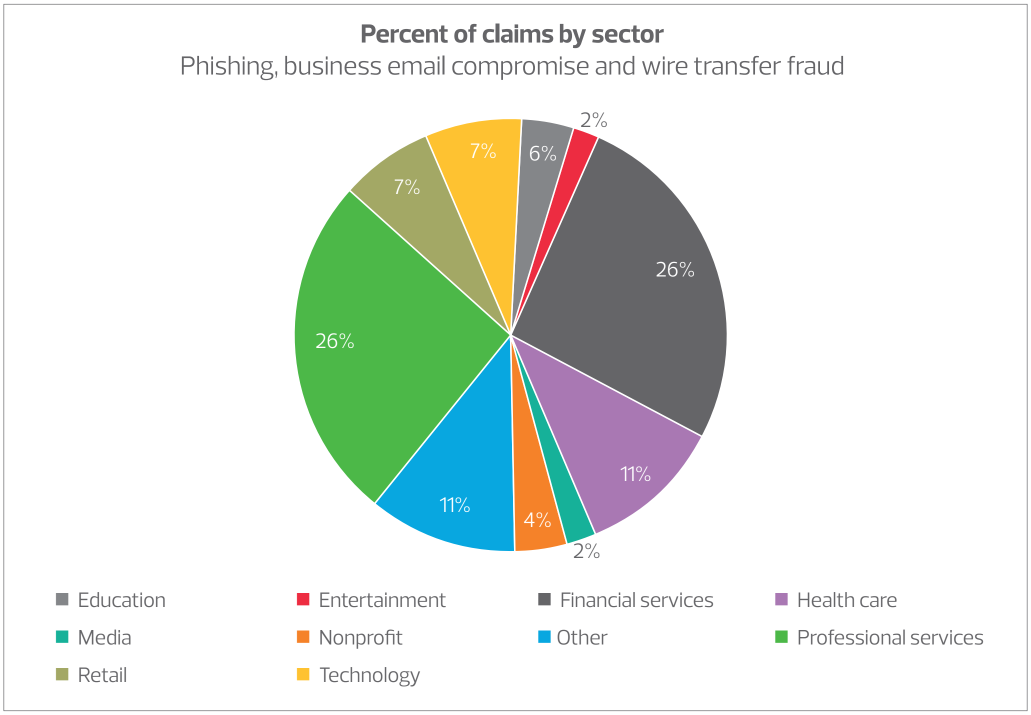
Social engineering (of which BEC is an example) illustrates the fraudsters' circumvention of systems and controls by applying pressure to an individual in a seemingly routine situation. As discussed above, an attacker pressures an honest employee (from a seemingly legitimate email address) to perform a transaction or post an entry very quickly that the employee may do quite regularly. The fraudster, posing as the CEO or a significant customer, demands immediate response or the employee will face termination or loss of business.

These types of social engineering attacks take very little time to generate and send to unsuspecting victims. And although the graphics above may seem to indicate a high victim fail rate, this is not entirely true. In fact, most email fraud scams are either detected by an organization's spam filter and blocked, or identified by the end user as being fraudulent and resulting in no action taken. Despite the majority of attacks resulting in no financial loss to an organization, it only takes one key individual in an organization to fall victim to an attack which can lead to a significant financial impact.

[2] Recorded Future is a technology company specializing in real-time cyberthreat intelligence.

In addition, social engineering attacks such as wire fraud seem to affect many industries. Based on the NetDiligence® 2018 Cyber Claims Study,[3] the top three sectors affected by wire transfer and banking fraud were professional services firms, financial services and retail. Based on the study, these events were typically caused by phishing, business email compromise and social engineering. The number of these events has been increasing during the past five years.

Figure 2: Email fraud attack trends by industry



Responding to an incident

If your company or client falls victim to a BEC or other cyberattack, having an effective incident response plan is key to understanding the breadth of the company's exposure. The plan should allow for comprehensive investigation and control remediation. These processes include:

1. Forensic review of IP addresses to identify potential origin of fraudulent emails
2. Evaluation of any potential malware on corporate servers and specified computing devices (desktops, laptops, tablets, etc.)
3. Interviews of individuals involved with the incident (senior management, controller, cash management, treasurer, etc.) as well as enterprise IT infrastructure and the global IT security officers
4. Historical evaluation of wire transfers
5. Evaluation of the vendor master file with U.S. wire transfers to assess whether vendor setup occurred prior to or after the fraudulent wire date
6. Transactional testing of manual wire transactions: Testing should be performed in the period that the transactions occurred, plus a look back to the previous three to four quarterly periods
7. IT review and documentation of current controls and control gap remediation (for each treasury locations)

[3] "The real cost of a data breach," RSM US LLP, accessed Feb. 25, 2019, https://rsmus.com/what-we-do/services/risk-advisory/security-and-privacy/the-real-cost-of-a-data-breach.html.

So what now?

While the SEC has not issued specific guidance on what companies should do, we have polled our financial and technical advisors and highlighted the following key recommendations for IT controls. The following may help organizations prevent and detect cyberfraud and ultimately mitigate potential reputational harm, financial loss and potential enforcement actions:

- Proactively monitor email activity to identify suspicious connections
- Enable multifactor authentication to minimize accounts from being compromised through phishing attacks
- Provide recurring security training program for users, especially related to email security to help prevent users from falling for suspicious emails
- Perform regular user phishing tests to further enhance awareness
- Flag all emails received from outside domains as "external" (Note: If a user account is taken over, and that account is used to perpetrate a fraud with others in the company, it would not show up as "external")
- Implement a password policy requiring a strong password and accounts that lock out after a set number of failed logon attempts; policy should be regularly audited to ensure that it is working correctly
- Actively monitor email logs to identify potentially unauthorized connections and email rules (e.g., forwarding to an external email address, moving or deleting messages based on specific terms)

By staying aware of the threats to the company, both from external sources as well as social engineering attacks on honest employees, significant impact and loss can be mitigated, or even avoided in some cases.

Help! Something bad happened

As noted throughout, there is no way to be 100 percent sure you can prevent an email account from being compromised. If the unfortunate occurs and an account becomes compromised, you can take several steps to secure the compromised account and preserve potentially relevant evidence:

- Immediately reset password(s) for the affected user(s) and reset the connection by terminating any active sessions. This will help ensure that any unauthorized users, including active connections, are disconnected.
- Put the account(s) of the affected user(s) on e-discovery litigation hold to preserve all messages going forward. This will prevent any potential data loss during the course of the investigation.
- Identify any suspicious rules in the affected user account(s). Document the rules prior to removing the suspicious rules.
- Identify any suspicious permission changes that were made to, or using, affected account(s). Document and revert identified permission changes.
- Do not disable or delete the compromised account, as this can effectively delete or otherwise clear certain log files associated with the account.
- Try to identify the phishing email, preserve one copy for analysis purposes and then purge the email from all accounts in the environment.
- If unauthorized IP addresses, phishing emails or spoofed email addresses are located, search the entire environment for other instances of those items to identify other accounts which may have been affected.

Conclusion

It's not only good business to implement effective controls and processes to limit cyberfraud, but following the recent SEC actions, failure to do so could result in significant sanctions under the Securities Exchange Act. Implementing proactive measures and utilizing the steps listed earlier can help your organization avoid threats or minimize their potential impact.

+1 800 274 3978
rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM, the RSM logo and *the power of being understood* are registered trademarks of RSM International Association.

RSM