SPRING 2016, ISSUE 1

INSIDE THIS ISSUE

Practice Tips
PAGE 2

FRAUD NEWS:
Executive Impersonation Fraud and Business Email Compromise
PAGE 6

FVS EYE ON FRAUD

The AICPA Forensic and Valuation Services Semi-Annual Report on Fraud Trends and Topics

EXECUTIVE IMPERSONATION: A GROWING THREAT

By David Zweighaft, CPA/CFF

The disclosure of data breaches continues to worry consumers and corporations every day. Now, a new and growing cyberattack risk exists that has gone largely unreported: business email compromise (BEC). In 2015, the FBI's Internet Crime Complaint Center (IC3) issued three public service announcements1 related to the use of a company's email system to criminally extract funds, noting that in 2014, U.S. companies lost $179 million.2 The scheme is a variation of the practice of spear phishing, in which spoof or fraudulent emails are directed at company personnel in an attempt to obtain account numbers, access codes, or other sensitive information. The newest incarnation of this scheme is more sophisticated, requires significant research and diligence on the part of the criminal hacker, and can have a huge financial impact on the victim company.

The scheme is *executive impersonation*, accomplished by the criminal creating a fake email that closely resembles the company's own email and appearing to come from a high-ranking executive. The recipient is an unsuspecting mid- or lower-level employee selected for his or her access and authority to transfer large sums of money between subsidiaries or to suppliers on behalf of the company.

BEC scams usually begin in one of two ways: by getting an unsuspecting employee to click on an email attachment that compromises the network (that is, malware), or by sending an email impersonating a high-ranking official in the company. Sophisticated hackers, however, usually research their target and the company as a whole in order to craft highly convincing emails. Using information gleaned from mining corporate websites and social networks, the impersonations used in the BEC emails can be extremely accurate and convincing. Because the email appears to come from a known and trusted source, the request to release valuable data or take urgent action appears more plausible.[3]

In order for a BEC scheme to be successful, the criminal researches social media, the business press and other company resources to get information about the corporate culture; the executive's personality, phrasing and use of language; the target employee's position and

Continued on page 2

[1] *I-012215-PSA Business Email Compromise, I-082715a-PSA Email Account Compromise, and I-082715b-PSA Business Email Compromise posted on IC3.gov.*
[2] *I-012215-PSA Business Email Compromise.*
[3] *See martindale.com/business-law/article_Jones-Day_2216506.htm.*

responsibilities; and information about other employees in the corporate accounting or treasury group. This information is then translated into a carefully crafted "look-alike" email, purportedly coming from the executive, requesting an emergency transfer, immediate payment of an urgent invoice or payment in anticipation of an undisclosed merger or secret acquisition. The request usually is characterized by a high degree of urgency ("ASAP" or "immediately").

The psychology behind BEC's success is that the employee is motivated to be responsive to the executive's request and is willing to bypass the typical controls associated with a normal wire transfer request. The more credible the appearance of the email, and the more authentic the tone and wording of the message, the more likely it will succeed. To enhance the authenticity of the scheme, the fraudulent email generally contains attachments on company letterhead directing the target employee to wire corporate funds to a particular person (usually a trusted vendor contact) at an overseas bank.

Key Characteristics

- Email requests come from a senior (C-suite) executive or a key vendor or supplier.
- The email address is substantially similar to the purported sender's address, with very minor, subtle differences. For example, if the actual address is CEO@victimco.com, the impersonator address might be CEO@vicitmco.com. Alternatively, the email display name may appear correct, but when the cursor hovers over the email address, a different underlying address is displayed.
- Requests occur when the executive is traveling and cannot be contacted.
- There is an element of urgency or secrecy regarding the disbursement.
- The amount is within the normal range of transactions so as not to arouse suspicion.
- Other employees are referred to or copied in the email, however, their email addresses are modified as noted previously.
- Requested payments are payable to a foreign bank.

The two most common variations of BEC schemes are the "urgent transaction request from the boss" and the "strong-arm vendor request."

Continued on page 3

PRACTICE TIPS

Although technology is the means by which this scheme is executed, technology is not the sole solution. As is the case for all methods of fraud, **awareness, training and repetition are key factors in the fight against these schemes.**

AWARENESS and discussion of the risks, the characteristics of these schemes and the potential consequences are necessary for all departments that may be involved in the payment of funds, including IT, treasury and purchasing. As part of your fraud prevention consulting, be sure that practitioners keep themselves apprised of the varying types of impersonation schemes and ensure that clients have adequate training of personnel in addition to appropriate internal control measures.

TRAINING should begin with the on-boarding process of new hires for the accounting and finance functions. Some or all of these people will be in positions to authorize, initiate or record wire transfers. Offering to provide periodic training on fraud risk management to a client's new hires will have a lasting impact, especially if it is endorsed by senior financial management. A two-hour continuing professional education session will give clients some necessary credits and, more importantly, peace of mind that the employees are being enlisted as the first line of defense against fraud.

REPETITION — Obviously, a one-time training session will soon fade from memory. Periodic newsletters to the client's accounting and finance staff regarding recent frauds perpetrated against companies within the client's industry will serve as reminders that the need for vigilance is constant.

Continued on page 8

In the *"urgent transaction request from the boss,"* a corporate accountant receives a spoofed email that appears to be from the CEO of the company requesting an urgent wire transfer relating to a top secret acquisition. The email contains instructions to wire corporate funds to a new bank account of a known business partner at an offshore bank. The accountant, wishing to appear responsive to her boss, drops everything and wires the funds immediately. By the time the accountant and CEO speak in person and realize the error, the money is long gone from the fraudulently opened offshore bank account.

In the *"strong-arm vendor request,"* a business receives a fraudulent invoice from what appears to be a long-standing supplier requesting that the next payment be sent via wire to an alternate account. The fraudulent email contains a PDF file of an invoice that appears to be from the trusted supplier, and the email text and header information appear to contain the hallmarks of an actual business communication from the supplier. Because the supplier is located overseas and in a different time zone, it is common practice that communication about payment of invoices be done electronically, rather than verbally. The unsuspecting business wires the funds to the new account, and the money disappears almost immediately. Weeks later, the legitimate supplier follows up with the business, sending an angry email expressing frustration that the funds were not sent timely. When the two business partners realize the mix up, it is too late to recover the funds.

The following illustrates some more examples of recent issues.

Financial Institution

On Nov. 6, 2012, a registered representative at Wells Fargo Advisors received an email from customer "GS" with an attached letter of authorization (LOA) requesting the transfer of $18,971 from the customer's brokerage account to a third-party account in Lima, Peru. As it turned out, the email was not sent by customer GS but by an imposter.

Per the regulatory proceedings, the "email address was not one known to be associated with the customer, but contained the customer's name in the email address."

Under such circumstances, it would appear that the sender's use of a previously unknown address might have alerted the representative and others to be wary — or at least make sure to follow the firm's protocols for handling such email requests. In fact, the records assert that the representative did not call the customer to confirm the wire request but merely processed the transfer. Worse, the record alleges that the representative "falsely claimed that he had spoken with GS, that he knows him personally and recognized GS's voice. [He] falsely entered 'pmt to friend for personal loan' in the service request as the intended purpose for the wire."

On Dec. 5, 2012, the representative received a second email from an imposter with attached LOA seeking a transfer of an additional $48,561 to the Lima account. It is unclear from the record whether this second email came from the same imposter as the Nov. 6 communication. The record explains that "[t]his email was a variation of the email address used in the Nov. 6, 2012, request and was also not an email address associated with the customer."

In response to this second transfer request, the representative again did not call the customer to confirm and went ahead and processed the wire and also offered the same false assurances to his firm concerning his efforts at verification.[4]

Continued on page 4

[4] *See brokeandbroker.com/2667/awc-email-/.*

Commodities Trader

Manufacturing

From May 21, 2014, to May 27, 2014, AFGlobal Corp's director of accounting received a series of emails from someone claiming to be Gean Stalcup, the CEO of AFGlobal.

> "Glen, I have assigned you to manage file T521," the phony message to the accounting director Glen Wurm allegedly read: "This is a strictly confidential financial operation, which takes priority over other tasks. Have you already been contacted by Steven Shapiro (attorney from KPMG)? This is very sensitive, so please only communicate with me through this email, in order for us not to infringe SEC regulations. Please do not speak with anyone by email or phone regarding this. Regards, Gean Stalcup."

Roughly 30 minutes later, Mr. Wurm said he was contacted via phone and email by Mr. Shapiro stating that due diligence fees associated with the China acquisition in the amount of $480,000 were needed. AFGlobal claims a Mr. Shapiro followed up via email with wiring instructions.

After wiring the funds as requested — sending the funds to an account at the Agricultural Bank of China — Mr. Wurm said he received no further correspondence from the imposter until May 27, 2014, when the imposter acknowledged receipt of the $480,000 and asked Wurm to wire an additional $18 million. Wurm said he became suspicious after that request and alerted the officers of the company to his suspicions.

According to the plaintiff, "the imposter seemed to know the normal procedures of the company and also that Gean Stalcup had a longstanding, very personal and familiar relationship with Mr. Wurm — sufficient enough that Mr. Wurm would not question a request from the CEO."

The company said it attempted to recover the $480,000 wire from its bank, but that the money was already gone by the 27th, with the imposters zeroing out and closing the recipient account shortly after the transfer was completed on May 21.[5]

Event Response

In view of the potential scope and damage that can be caused by a data breach, the initial discovery of any intrusion can be traumatic. When an attack is suspected, early mobilization and assessment of impact are crucial. Assemble the proper team, including in-house counsel, the CIO and subordinates responsible for IT security, outside counsel and, if necessary, an outside cybersecurity consultant.

Working under the direction of outside counsel under attorney-client or attorney work-product privilege will facilitate an internal investigation to gather all the relevant facts for management and the board of directors to keep them apprised of all developments and support their decision-making. Proceeding in this manner will also provide a foundation for responding to law enforcement and government investigators in the event the breach must be reported.

The principal questions the investigation must address are as follows:

- Who committed the breach, and what employees were involved?
- How did the breach occur? What internal controls were circumvented or did not operate properly?
- Scope: How much data was exposed? How much money was misdirected?
- When did the breach occur? Was it an isolated incident or a series of events?
- What needs to be done to limit the damage?
- Are the existing corporate systems (for example, email, treasury) intact and safe for continued use?

Questions for management and the board to address:

- Should we contact the financial institution to freeze the account?
- How can we recover the absconded funds?
- What are our legal obligations and responsibilities with respect to notifying various classes of stakeholders?
  - Government: Law enforcement, regulators

Continued on page 5

[5] *See krebsonsecurity.com/2016/01/firm-sues-cyber-insurer-over-480k-loss/#more-33617.*

  - Shareholders
  - Customers, business partners, vendors and service providers
- What is our cyber-insurance coverage? Do we submit a claim?
- How do we control the reputation risk arising from this breach?
- Is there any potential liability to third parties who might be at risk of identity theft, misdirected payments or other collateral damage?

Is This the New Normal?

Spear phishing in the form of BEC attacks is the newest weapon in the cyber-criminal arsenal. As noted in the IC3 data that follow, it is being used more and more frequently because it is effective and difficult to investigate and prosecute. This scheme is occurring worldwide, and there is no silver bullet to prevent these attacks.

These schemes, like others that prey on human fallibility, can be mitigated. More robust controls, including two-step authentication of transactions, enhanced employee awareness training, informed verification of transfer requests and evolving IT controls can detect BEC attempts before they result in losses. These same policies and procedures indicate a company's intent to implement reasonable safeguards to prevent data breaches, which will be questioned in the event of a lawsuit or government investigation following the material event.

NUMBER OF INCIDENTS AND RELATED DOLLAR AMOUNTS

INCIDENTS REPORTED TO THE FBI INTERNET CRIME COMPLAINT CENTER (IC3)[6]	10/1/2013 – 1/22/2015	8/27/2015
Total U.S. victims	1,198	7,066
Total U.S. actual dollar loss	$179.76	
Total U.S. exposed dollar loss ($M)		$747.66
Total non-U.S. victims	928	1,113
Total non-U.S. actual dollar loss ($M)	$35.22	
Total non-U.S. exposed dollar loss ($M)		$51.24
Combined victims	2,126	8,179
Combined dollar actual loss	$214.97	
Combined exposed dollar loss ($M)		$798.90

[6] *Ibid., IC3.gov.*

FRAUD NEWS: EXECUTIVE IMPERSONATION FRAUD AND BUSINESS EMAIL COMPROMISE

Reuters recently reported that individuals who created a false email address and posed as a legitimate vendor defrauded an unidentified American company out of almost $100 million in 2015.

As a result of the fraud, the U.S. government filed a civil forfeiture lawsuit in an attempt to recover $25 million in proceeds held in 20 banks internationally. About $74 million has been recovered. The scheme entailed creating a fake email address that was similar to a vendor in Asia. The perpetrators then posed as the vendor in dealing with the logistics of vendor payments. The American company sent almost $99 million to an account in Cyprus. While Eurobank in Cyprus restrained $74 million, the other $25 million was laundered through accounts in Latvia, Hungary, Slovakia, Hong Kong and others.

In an alert issued recently, the FBI said that global business losses from email wire transfer scams, or "business email compromise," were about $2.3 billion from October 2013 through February 2016. The FBI said it documented frauds affecting over 17,600 businesses in 79 countries. A former federal prosecutor told Reuters, "it's going to continue to get worse before it gets better."

Afognak Inc., a native corporation based in Alaska, had a subsidiary that transferred almost $4 million into an unknown account based on an email from their CEO. The email said that the transaction would be with an attorney, who then phoned shortly after. Although the transaction was real, the email was a scam from Eastern Europe and the "attorney" was a fraudster.

The Scoular Co., an employee-owned commodities trader founded 120 years ago, was taken for $17.2 million in an international email swindle, according to federal court documents.

An executive with the 800-employee company wired the money in installments last summer to a bank in China after receiving emails ordering him to do so, according to an FBI statement.

The scheme involved emails sent to a Scoular executive that purported to be from the CEO and the company's outside auditing firm. The emails directed the wire transfer of millions of dollars to a Chinese bank. But court documents say the emails were really from impostors using email addresses set up in Germany, France and Israel and computer servers in Moscow.

The first email instructed the controller to wire $780,000, which the FBI statement says he did. The next day, he was told to wire $7 million, which he also did. Three days later, another email was sent to the controller, instructing him to wire $9.4 million. The first two emails from the faux CEO contain the swindle's setup, swearing the recipient to secrecy over a blockbuster international deal: "I need you to take care of this. For the last months we have been working, in coordination and under the supervision of the SEC, on acquiring a Chinese company. ... This is very sensitive, so please only communicate with me through this email, in order for us not to infringe SEC regulations."

The second email attempted to create a further air of legitimacy by instructing the controller to contact a certain employee of the company's accounting firm for details on where to wire the money. He later received an email purported to be from the real employee of the real accounting firm, instructing him to wire the money to a bank in China with many branch offices and international clients.[7]

Continued on page 7

[7] *See omaha.com/money/impostors-bilk-omaha-s-scoular-co-out-of-million/article_25af3da5-d475-5f9d-92db-52493258d23d.html.*

FRAUD NEWS: EXECUTIVE IMPERSONATION FRAUD AND BUSINESS EMAIL COMPROMISE *(CONTINUED)*

Networking firm Ubiquiti Networks Inc. disclosed recently that cyber thieves stole $46.7 million using an increasingly common scam in which crooks spoof communications from executives at the victim firm in a bid to initiate unauthorized international wire transfers.

Ubiquiti, a San Jose-based maker of networking technology for service providers and enterprises, disclosed the attack in a quarterly financial report filed with the SEC. The company said it discovered the fraud June 5, 2015, and that the incident involved employee impersonation and fraudulent requests from an outside entity targeting the company's finance department.

> "This fraud resulted in transfers of funds aggregating $46.7 million held by a company subsidiary incorporated in Hong Kong to other overseas accounts held by third parties," Ubiquiti wrote. "As soon as the company became aware of this fraudulent activity, it initiated contact with its Hong Kong subsidiary's bank and promptly initiated legal proceedings in various foreign jurisdictions. As a result of these efforts, the company has recovered $8.1 million of the amounts transferred."

Ubiquiti said in addition to the $8.1 million it already recovered, some $6.8 million of the amounts transferred are currently subject to legal injunction and reasonably expected to be recovered. It added that an internal investigation completed last month uncovered no evidence that its systems were penetrated or that any corporate information, including our financial and account information, was accessed. Likewise, the investigation reported no evidence of employee criminal involvement in the fraud.

"The company is continuing to pursue the recovery of the remaining $31.8 million and is cooperating with U.S. federal and numerous overseas law enforcement authorities who are actively pursuing a multi-agency criminal investigation," the 10-K filing reads. "The company may be limited in what information it can disclose due to the ongoing investigation. The company currently believes this is an isolated event and does not believe its technology systems have been compromised or that company data has been exposed."

Ubiquiti noted that as a result of its investigation, the company and its audit committee and advisers concluded that its internal control over financial reporting were ineffective due to one or more material weaknesses, though it didn't disclose what measures it took to close those security gaps. "The company has implemented enhanced internal controls over financial reporting since June 5, 2015, and is in the process of implementing additional procedures and controls pursuant to recommendations from the investigation," it said.[8]

Several industry professionals have been advising companies to look for the warning signs of such frauds. Red flags, such as the domain being off by one letter, a change in writing style and payments to countries where the company has never done business are just a few that have been noted.

[8] *See krebsonsecurity.com/tag/business-email-compromise/.*

PRACTICE TIPS *(CONTINUED)*

Specific Procedural Controls

Depending on the size and sophistication of the client, the controls relating to how emails can be used to initiate wire transfers should be documented and included in the Internal Control Over Financial Reporting for Sarbanes-Oxley Act of 2002 compliance. These will then be included as part of the annual controls testing in connection with the audit.

For each of your client organizations, those involved in the payment of funds will vary. Essentially, any employee who has the authority to request, approve, or execute wire transfers must be properly trained on the varied impersonation schemes as well as the protocols established internally. Additional controls may be suggested that include a secondary level of verification. Many companies have limited the number of personnel authorized to execute wire transfers and instituted a requirement for a verbal confirmation from a known phone number before any wire transfer may be executed. The client should have a secondary verification process in place, such as follow up via phone call using a verbal authorization code, before any action is taken.

Client companies should communicate with their financial institutions to determine best practices and ensure all parties understand the risks and methods to apply when a potential situation arises.

A review of the company's social media policy is also appropriate. Determine whether employees are over-sharing details about key executive locations and travel. In such instances, a general guide might be provided to employees directing them to limit details about travel by, and locations of, key executives. Remember, when sharing on social media, less is often more.

Other technological controls involving guarding against malware, email header data, local encryption for emails designed to initiate wire transfers and domain blocking are appropriate preventative solutions that a security consultant may evaluate and recommend.

Finally, recommend that the client's risk management team examine the company's insurance policies and consider cyber-risk coverage, including fraud, data breach, ransomware and losses arising from denial of service attacks.

To summarize:

- **Train employees responsible for wire transfers, placing a focus on BEC schemes and data security.** Increase the frequency of training from annual to semi-annual or quarterly and provide updated information describing the latest schemes and trends in phishing and social engineering. Encourage a healthy level of skepticism in finance and treasury employees, and establish procedures to verify the origin of all wire requests. Remind all employees to use the company fraud hotline to anonymously report suspicious activity without fear of retaliation.
- **Engage cyber-risk security consultants to identify, monitor and mediate spear-phishing threats**, including identifying employee-targeted attacks on social networks; finding and taking down fraudulent and impersonating accounts; continuously monitoring key employee and company accounts for compromise; and investigating attacks being planned against your organization.
- **Review policies and procedures for requesting, initiating and approving wire transfers.** Email requests should be verified by phone calls to company-registered phones. Require two employees to approve wire requests and authenticate the recipient's identity before the wire is released.
- **Conduct a risk assessment of the wire transfer process to identify weaknesses that could be exploited.** Engage a cybersecurity firm to perform a penetration test of the company's firewalls, email, security software, operating systems and browsers. Flag incoming emails with domains that are similar, but not identical, to those of the company. Identify "look-alike" domains and register them in the name of the company to prevent hackers from attempting BEC attacks.

RESOURCES

AICPA – **aicpa.org**
FBI's Internet Crime Complaint Center (IC3) – **ic3.gov**
FBI Alert – **fbi.gov**
FBI Stories – **fbi.gov/news**
Consumer Affairs – **consumeraffairs.com**
Office of the Comptroller of the Currency – **occ.gov**
Federal Trade Commission – **ftc.gov**
Federal Trade Commission — Identity Theft – **consumer.ftc.gov**

20280-378