BEYOND HACKING: COVERAGE FOR SOCIAL ENGINEERING SCAMS AND SCHEMES

Kathleen Crowe
AON RISK SOLUTIONS INC.
kathleen.crowe@aon.com

Jennifer O. Farina
COVINGTON & BURLING LLP
jfarina@cov.com

Laura Hanson
MEAGHER & GEER PLLP
lhanson@meagher.com

Lucy L. Thomson
LIVINGSTON PLLC
lucythomson1@mindspring.com[1]

American Bar Association Section of Litigation
Insurance Coverage Litigation Committee
Women in Insurance Conference
October 20, 2016, Washington, DC

[1] The authors' views in this paper are their own and are not intended to represent the views of their employers or clients. This paper has been a joint project with content supplied by each of the authors; the contents of a particular section of the paper do not necessarily fully reflect the views of all the authors.

I. What's the Risk? Social Engineering Fraud Schemes

Cyber risks have evolved beyond traditional hacking to include sophisticated social engineering scams that rely on unwitting insiders to effectuate the scheme. In the past two years, major companies around the world have been the victims of multi-million dollar fraud schemes that were successfully perpetrated online using social engineering.

FBI officials have warned of a dramatic increase of 1,300 percent since January 2015 in business e-mail compromise (BEC), a scheme used to defraud businesses of all types and sizes, from large corporations and technology companies to small businesses and non-profit organizations.[2] The FBI considers it a "sophisticated scam" that targets businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. Criminals carry out the fraud by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques and orchestrate the unauthorized transfers of funds.[3]

These attacks have resulted in massive financial losses in 100 countries and in all 50 states, totaling as much as $3.1 billion for U.S. and international victims. The FBI has identified more than 14,000 U.S. victims.[4]

Social engineering has been a technique used by criminals for decades to defraud unsuspecting victims.[5] US-CERT[6] describes a social engineering attack this way:

> In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility. [7]

In its *Guide to Preventing Social Engineering Fraud*, Chubb identified a number of social

[2] FBI Public Service Announcement: Business e-Mail Compromise: The 3.1 Billion Dollar Scam (Alert No. 1-061416-PSA) (June 14, 2016), *available at* https://www.ic3.gov/media/2016/160614.aspx#ref1.

[3] FBI Public Service Announcement: Business eMail Compromise (Alert No. 1-082715a-PSA) (August 27, 2015), *available at* https://www.ic3.gov/media/2015/150827-1.aspx.

[4] *Ibid.*; FBI PSA (Alert No. 1-061416-PSA), page 1.

[5] The Social Engineering Framework is a searchable resource with information on the psychological, physical and historical aspects of social engineering, *available at* http://www.social-engineer.org/framework/general-discussion/.

[6] US-CERT, the U.S. Computer Emergency Readiness Team in the Department of Homeland Security with responsibility to provide a safer, stronger Internet by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world. *See* https://www.us-cert.gov/about-us.

[7] Security Tip (ST04-014), Avoiding Social Engineering and Phishing Attacks (October 2014), *available at* https://www.us-cert.gov/ncas/tips/ST04-014.

engineering tactics[8] used by attackers, particularly to target businesses online:

- *Impersonation/pretexting*: This common form of deception may involve an attacker using a believable reason to impersonate a person in authority, a fellow employee, an IT representative, or vendor in order to gather confidential or other sensitive information.
- *Phishing/ spamming/ spear-phishing*: Phishing can take the form of a phone call or e-mail from someone claiming to be in a position of authority who asks for confidential information, such as a password. Phishing can also include sending e-mails to organizational contacts that contain malware designed to compromise computer systems or capture personal or private credentials.
- *IVR/Phone phishing* (a/k/a vishing): This telephone scam uses a technical tactic, an interactive voice response (IVR) system, to replicate a legitimate sounding message that appears to come from a bank or other financial institution and directs the recipient to respond in order to "verify" confidential information. These messages may claim to come from other seemingly "trusted" organizations such as a government agency or the police and may reference personal details obtained from social media or other sources.

The 2016 Verizon Data Breach Investigations Report has documented an increase in phishing attacks and reported that phishing has been a factor in more than two-thirds of cyber-espionage incidents for the past three years. The use of pretexting in financially motivated breaches increased in 2015.[9]

A. What types of social engineering scams have been identified?

The FBI has identified a number of scenarios by which the BEC scam is perpetrated, based on analysis of victims' complaints.[10] The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some report using checks as a common method of payment. The criminals will use the method most commonly associated with their victim's normal business practices.[11]

The FBI stated that fraudulent transfers to 100 countries have been reported, with the majority going to Asian banks located within China and Hong Kong.

1. *Business Executive Receiving or Initiating a Wire Transfer Request; also referred to as "CEO Fraud," "Business Executive Scam," "Masquerading," "Financial Industry Wire Fraud," or "Whaling Scam" (scams target the organization's top executives or 'big fish')*

   The e-mail accounts of high-level business executives (CFO, CTO, etc.) are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is

[8] Chubb *Guide to Preventing Social Engineering Fraud*, *available at* http://www.chubb.com/businesses/csi/chubb19441.pdf.

[9] Verizon 2016 Data Breach Investigations Report (Verizon DBIR), pages 17-19, 73, *available at* http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

[10] *Ibid.*; FBI PSA No. 1-061416-PSA (June 14, 2016), *available at* https://www.ic3.gov/media/2016/160614.aspx.

[11] *Id.*

normally responsible for processing these requests. In some instances a request for a wire transfer from the compromised account is sent directly to the financial institution with instructions to urgently send funds to bank "X" for reason "Y."[12]

2. *Business Executive and Attorney Impersonation; Confidential and Time-Sensitive Requests*

   Victims are contacted by fraudsters, who typically identify themselves as lawyers or representatives of law firms and claim to be handling confidential or time-sensitive matters. This contact may be made via either phone or e-mail. Victims may be pressured by the fraudster to act quickly or secretly in handling the transfer of funds. This type of BEC scam may occur at the end of the business day or work week or be timed to coincide with the close of business of international financial institutions.[13]

3. *Business Working with a Foreign Supplier; referred to as "Bogus Invoice Scheme," "Supplier Swindle," and "Invoice Modification Scheme"*

   A business, which often has a long-standing relationship with a supplier, is asked to wire funds for invoice payment to an alternate, fraudulent account. The request may be made via telephone, facsimile or e-mail. If an e-mail is received, the subject will spoof the e-mail request so it appears very similar to a legitimate account and would take very close scrutiny to determine it was fraudulent. Likewise, if a facsimile or telephone call is received, it will closely mimic a legitimate request.[14]

4. *Business Contacts Receiving Fraudulent Correspondence; Fake Invoices to Vendors*

   An employee of a business has his/her personal e-mail hacked. This personal e-mail may be used for both personal and business communications. Requests for invoice payments to fraudster-controlled bank accounts are sent from this employee's personal e-mail to multiple vendors identified from this employee's contact list. The business may not become aware of the fraudulent requests until its vendors contact company officials to follow up on the status of their invoice payments.[15]

5. *"Attorney Check Scam"*

   Attorneys are targeted to represent supposed (BEC) litigants in a payment dispute. (BEC) litigants send retainers in the form of checks to the attorney. The scam is revealed when either the checks are found to be fraudulent or the (BEC) litigants are contacted. While the payment disputes are real, the (BEC) litigants neither contacted nor retained that attorney for legal assistance.[16]

6. *Data Theft*

   Fraudulent requests are sent utilizing a business executive's compromised e-mail. The entities in the business organization responsible for W-2s or maintaining personally identifiable information (PII), such as the human resources department, bookkeeping, or

[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*

> auditing section, have frequently been identified as the targeted recipient of the fraudulent request. Some of these incidents are isolated and some occur prior to a fraudulent wire transfer request. This data theft scenario first appeared just prior to the 2016 tax season.[17]

One striking aspect of recent BEC schemes generally is that unlike the e-mail phishing attacks of past years that were designed to trick the recipient into clicking on a malicious link or opening an attachment that would download malware onto the victim's computer, many BEC attacks did not require the use of malware to be successful. More sophisticated schemes, however, have combined social engineering with the hacking and compromise of a computer, as well as phishing attacks to steal executives' credentials.[18]

Noted security researcher Brian Krebs provided some of the reasons why BEC fraud has been so successful:

> On the surface, business e-mail compromise scams may seem unsophisticated relative to moneymaking schemes that involve complex malicious software, such as Dyre and ZeuS. But in many ways, the BEC attack is more versatile and adept at sidestepping basic security strategies used by banks and their customers to minimize risks associated with account takeovers. In traditional phishing scams, the attackers interact with the victim's bank directly, but in the BEC scam the crooks trick the victim into doing that for them.[19]

B. Planning and Carrying Out Online BEC Fraud Schemes – Hacker Strategies

The 2016 Verizon Data Breach Report reported seeing breaches caused by financial pretexting, which they refer to as 'CEO Fraud.' The authors characterize the criminal operations (with some wry humor) this way:[20]

> This involves old-fashioned social engineering of employees with the authorization to move money. E-mails purportedly from the CEO or other top executive provide instruction to transfer funds to an entity, with a seemingly valid reason provided. These may also be blended with other forms of communication. "Twas not the CEO behind that email and somebody who believed they were following legitimate instructions is not having a very good day."

[17] *Id.*

[18] *See, e.g., BitPay, Inc. v. Massachusetts Bay Ins. Co.*, No. 1:15-CV-03238, 2015 WL 5446711 (N.D. Ga. filed Sept. 15, 2015). The Anti-Phishing Working Group has focused on the social engineering and technical subterfuge aspects of phishing seen in the BitPay fraud: "Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. *Social engineering schemes* use spoofed e-mails purporting to be from legitimate businesses and agencies, designed to lead consumers to counterfeit websites that trick recipients into divulging financial data such as usernames and passwords. *Technical subterfuge schemes* plant crimeware onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords – and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes)." (emphasis added). APWG Phishing Activity Trends Report Q1 2016, *available at* http://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf.

[19] Krebs on Security, FBI: $2.3 Billion Lost to CEP Email Scams (April 18, 2016), *available at* http://krebsonsecurity.com/tag/ceo-fraud/.

[20] *Ibid.*; Verizon DBIR, page 61.

BEC e-mails typically use the same format and approach. The fraud is conducted using one or more of the following methods.

- *Reconnaissance – Targeting Employees* – The perpetrators study and monitor their selected victims using social engineering prior to initiating a BEC scam. Victims may first receive "phishing" e-mails requesting details regarding the business or individual being targeted (name, travel dates, etc.).

  Thus, criminals are able to accurately identify the individuals and protocols necessary to perform wire transfers within the specific business environment of the organization.

- *Typo-squatting* – The criminal creates a "look-alike" domain name that resembles the actual domain of the targeted company (one or two letters off, *e.g.* "myydomain.com" vs "mydomain.com"; or substituting the letter "L" for the numeral 1), *e.g.* "examp1e.com" or "example.co"). These domains are often registered on the same day that the e-mail is sent, often within a matter of hours.

- *Crafting the e-mail* – Hackers spoof company e-mail or use social engineering to assume the identity of senior officials such as the CEO, a company attorney, or trusted vendor.

  Criminals will forge the sender's e-mail address displayed to the recipient, so that the e-mail will display the address of the company's domain. However, the "reply-to" address is the spoofed external domain, often a free e-mail service, ensuring that any replies are sent to the hacker. The victims often do not realize they are being duped

- *Content of e-mails tailored to the company* – Using the same techniques, "phishing" text messages can be sent purporting to be from the recipient's bank. Hackers use software that alters the sender ID so it appears with the name of the bank, potentially within an existing thread of genuine messages so the user believes the e-mail is trustworthy and is likely to respond.

  After researching employees who manage money, hackers use language specific to the company they are targeting. They request by e-mail a wire transfer using dollar amounts that would be usual and expected in the company to lend legitimacy.

- *Urgency* – The request always contains a sense of urgency or secrecy and it is followed up with a pattern of increasing urgency so the hacker can know the funds were sent.

- *Avoiding suspicion* – Criminals may plan to initiate the fraudulent e-mail wire transfer request while the executive being impersonated is away from the office.

  The e-mails may state that the CEO is traveling or is in a meeting and cannot accept phone calls. Many of the e-mails have "sent from my iPad" appended, to suggest the sender is on the road or to excuse typos in the message. They are often sent on a Friday to give the criminals more time to avoid detection.

C. Types of Attacks – Illustrative examples of social engineering scams and the resulting losses

News reports, Securities and Exchange Commission (SEC) filings, and cases in litigation provide an inside look at some of the specific techniques used to defraud high-level executives and key figures in global companies. Some of these BEC frauds contributed to the greatest reported losses since 2015.

As will be discussed in more detail below, the methodology and details of how these schemes are architected and carried out are often important in determining whether a particular fraud incident is covered under an insurance policy.

1) CEO Fraud

- **Xoom** (NASDAQ:XOOM) California, an international money transfer company (online wire-transfer provider) acquired by PayPal in mid-2015 – $30.8 million loss

Xoom reported an incident involving employee impersonation and fraudulent requests targeting the Company's finance department. As a result, $30.8 million in corporate cash was transferred to overseas accounts.[21]

Impact of the Fraud – $30.8 million in Q4 2015. The CFO resigned. The Company's audit committee authorized an independent investigation by outside advisors. The company has implemented additional internal procedures, and federal law enforcement authorities are actively pursuing a multi-agency criminal investigation. Stock for the low-cost payments company, which competes with Western Union, dipped 14%, or $31 million, after the loss was announced, but later recovered.

- **Scoular Co**., an Omaha-based commodities trader, one of Omaha, Nebraska's oldest companies (and one of the top privately held companies in the U.S.) – $17.2 million loss

The company reported an incident involving a spear-phishing wire fraud scam. According to Omaha.com, a company executive wired the money in installments last summer to a bank in China after receiving e-mails ordering him to do so.

- **Ubiquiti Networks**, a San Jose-based wireless networking technology company – $46.7 million loss

In a 2015 SEC filing,[22] Ubiquiti Networks reported an incident involving employee impersonation and fraudulent requests from an outside entity targeting the company's finance department. This fraud resulted in wire transfers of funds aggregating $46.7 million held by a company subsidiary incorporated in Hong Kong to other overseas bank accounts held by third parties, believed to be the attackers.

Impact of the Fraud – As soon as the company became aware of the 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. Furthermore, an additional $6.8 million are currently subject to legal injunction and reasonably expected to be recovered by the company in due course. 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.

In its SEC filing, Ubiquiti said the company currently believes this is an isolated event and does not believe its technology systems have been compromised. A 2015 investigation by outside

[21] Xoom SEC Form 8-K, Item 8.01 Other Events (December 30, 2014), *available at* https://www.sec.gov/Archives/edgar/data/1315657/000110465915000360/a15-1144_18k.htm.

[22] Ubiquiti Networks, Inc. Form 8-K, Item 8.01 Business Fraud (August 4, 2015); *available at* https://www.sec.gov/Archives/edgar/data/1511737/000157104915006288/t1501817_8k.htm.

advisors uncovered no evidence that company systems were penetrated or that any corporate information, including financial and account information, was accessed. The investigation found no evidence of employee criminal involvement in the fraud. The company, its Audit Committee, and advisors have concluded that the company's internal control over financial reporting is ineffective due to one or more material weaknesses. The company has implemented enhanced internal controls over financial reporting.

- **FACC** (Austria),[23] An Austrian aerospace manufacturer that designs and supplies parts to Airbus and Boeing – $54 million loss

In January 2016 FACC AG announced that it became a victim of fraudulent activities involving communication- and information technologies. To the current state of the forensic and criminal investigations, the financial accounting department of FACC Operations GmbH was the target of cyber fraud.

Impact of the Fraud – FACC's IT infrastructure, data security, and IP rights, as well as the operational business of the group were not affected by the criminal activities. The damage is an outflow of approximately EUR 50 million of liquid funds. The management board has taken immediate structural measures and is evaluating damages and insurance claims.

- **Crelan Bank** (Belgium), **Belgian Bank Crelan, Crédit Agricole's Belgian subsidiary – €70 million ($75.8 million)** loss

Crelan Bank reported that it was the victim of CEO fraud, a targeted spear-phishing wire fraud campaign.[24] The fraud was discovered during an internal audit.

Impact of the Fraud – To date, this is the largest reported loss from a targeted spear-phishing wire fraud attack.

- **Mattel**, U.S. toymaker, Barbie dolls and other toys – $3 million loss/recovered

The fraud was the result of a well-researched phishing e-mail directed to an unnamed finance executive who was on the approved sign-off list for large cash transfers. The e-mail appeared to be written by the new CEO Christopher Sinclair, one of two executives also required to sign off on cash transfers. Attackers had harvested open source information on Mattel staff, enabling them to understand its corporate hierarchy and payment patterns. Company officials wired $3 million to an account of Chinese hackers at the Bank of Wenzhou, China.[25]

Impact of the Fraud – The recovery was mostly due to luck: the cash was wired on a Chinese bank holiday so the funds were held up and later returned by fast-acting authorities. Mattel contacted the FBI and local and foreign banks; after a visit to the Bank of Wenzhou headquarters by an anti-fraud investigator with an FBI letter in hand, the funds were returned. The bank is located in a region infamous for tunneling cash stolen from CEO phishing scams.

The Barbie-company has since tracked a dozen more chief executive officer scams that have arrived since the attack.

[23] FACC AG Interim Report, Q3 2015/16, page 20, *available at* http://www.facc.com/en/Investor-Relations/Reports.

[24] http://www.crelan.be/sites/default/files/COMM/presse/pb_01-2016_nl.pdf (in Dutch).

[25] Darren Pauli, Chinese Bank Holiday Foils Near Perfect 3 Million Mattel Fleecing, The Register (April 2016), *available at* www.theregister.co.uk/2016/04/06/chinese_bank_holiday_foils_nearperfect_3_million_mattel_fleecing/

- **BitPay**, Atlanta, Georgia, Global bitcoin[26] payment processor – $1.85 million in digital currency loss

Insurance Litigation: *BitPay, Inc. v. Massachusetts Bay Ins. Co.*, No. 1:15-CV-03238, 2015 WL 5446711 (N.D. Ga. filed Sept. 15, 2015)

Multi-Pronged Nature of the Fraud: This complex fraud was launched through the use of a spear-phishing attack and successfully carried out with social engineering.[27] The perpetrator, who had previously compromised the computer and taken over the e-mail account of BTC Media CEO David Bailey, initiated the attack by sending a phony e-mail (purportedly from Bailey) to BitPay CFO Bryan Krohn, requesting a comment for an article by journalist Bailey for the publication yBitcoin. The e-mail directed Kohn to click on the link to a Google document. Bryan Krohn responded to the e-mail, and clicked on the link which directed him to a website controlled by the hacker; there Krohn entered the authentication credentials for his BitPay corporate e-mail account.

After capturing Krohn's BitPay credentials, the hacker used that information to prompt CEO Stephen Pair and executive chairman Tony Gallippi to authorize three payments totaling 5,000 BTC, including one transaction from a wallet on the bitcoin exchange Bitstamp.

This fraud was successful because after capturing Krohn's BitPay corporate e-mail, a key detail in the e-mails was now accessible to the fraudster: the fact that BitPay did not require SecondMarket to advance pay for bitcoins it received from the company.

Using this information, the individual crafted an e-mail chain showing a conversation between Krohn and SecondMarket VP Preston Blankenship regarding a purchase of 1,000 BTC. The e-mail requested that 1,000 bitcoins be transferred to SecondMarket at a specific wallet address provided. At 3:33 PM the bitcoins were sent from BitPay's hot wallet.

Less than an hour later, the criminal controlling Krohn's e-mail requested an additional 1,000 BTC be sent to the same bitcoin address. This amount was then transferred from an account held on Bitstamp by Gallippi after Pair indicated by e-mail that there were insufficient funds in BitPay's "warm" wallet following the second request.

The next day, Krohn's e-mail was used to request that Pair send an additional 3,000 BTC to another address said to be controlled by SecondMarket. Pair responded "to confirm that this request, which exceeded the usual 1000-2000 daily bitcoin amount between the companies, was valid." The assailant responded by copying an e-mail address purportedly from SecondMarket and confirming that the request was valid.

After processing the transaction, Pair confirmed the move by e-mail and copied SecondMarket employee Gina Guarnaccia. Guarnaccia wrote back "that she did not send the prior e-mail noting the 3,000 bitcoins and address for them to be sent, and that SecondMarket did not purchase the bitcoins."

[26] Bitcoin is a digital currency transferred electronically via the Internet and can be used to pay for products and services.

[27] Massachusetts Bay initial denial letter, Case 1:15-cv-03238-SCJ Document 1-1 Filed 09/15/15 Pages 34-36 of 48.

- **Long Beach Escrow Corporation,** California real estate agency – $250,000 loss

Insurance Litigation: *Maxum Indemnity Co. v. Long Beach Escrow Corp.*, No. 2:16-CV-05907, 2016 WL 4199087 (C.D. Cal. Filed Aug. 8, 2016).

Impact of the Fraud: Real estate firm Keely Partners sued Long Beach Escrow Corporation (LBEC) in April for negligence and breach of fiduciary duty after the escrow company was duped into wiring more than $250,000 to hackers who had taken control of a Keely partner's e-mail account.

- **Te Wananga o Aotearoa** *(*New Zealand), one of New Zealand's largest learning institutions – $US79,000 ($118,000) loss

The executive director of finance at Te Wananga o Aotearoa, Bronwyn Koroheke, transferred $US79,000 ($118,000) to an offshore bank account after receiving an e-mail which appeared to be from her chief executive Jim Mather telling her to send the money.

In fact, the e-mail was from Chinese-based fraudsters running the scam. They forged Mather's e-mail address to make it look like he was sending it from a mobile device.

Impact of the Fraud: The chief financial officer left her job after falling for an e-mail scam.

- **AF Global**, privately-held Houston, Texas company that provides engineering, manufacturing and aftermarket services for the oil and gas, power generation, industrial and aerospace markets – $480,000 loss

Insurance Litigation: *Ameriforge Grp. Inc. v. Fed. Ins. Co.*, No. 4:16-CV-00377, 2016 WL 67625 (S.D. Tex. filed Jan. 4, 2016).

Nature of the Fraud: On May 21, 2014, the AF Global Director of Accounting received an e-mail purporting to be from the company's CEO. The e-mail instructed the director to cooperate with a named attorney to handle a highly confidential financial operation. The e-mail instructions received advised that this was a confidential financial operation, which should take priority over other tasks. The e-mail indicated that he would receive a call purportedly from an attorney for KPMG. The Accounting Director then received follow-up telephone and e-mail communications from the purported attorney, who explained that the Director should immediately wire $480,000 to a Chinese bank account to pay the due diligence fees related to a sensitive acquisition in China that AF Global was pursuing.

A week after the director transferred the funds, he received another e-mail requesting a second transfer in the amount of $18 million. The Director became suspicious and notified his supervisors, who determined the company had been scammed. After determining that both requests were fraudulent, AF Global attempted, without success, to recall the wire from Bank of America and reported the matter to the police.

2) "Bogus Invoice Scheme," "Supplier Swindle," and "Invoice Modification Scheme"

- **Taylor and Lieberman,** California, accounting firm that issues payments and transfers funds on behalf of its clients – $100,000 loss

Insurance Litigation: Taylor and Lieberman v. Fed. Ins. Co., No. 2:14-CV-03608, 2015 WL 3824130 (C.D. Cal. June 18, 2015).

Impact of the Fraud: An imposter fraudulently took control of the e-mail account of the accounting firm's client. Purporting to be the client, the criminal sent e-mails to the accounting firm requesting that the firm wire money from the client's account, over which the firm had power of attorney, to an account in Malaysia. The Taylor employee wired several payments before discovering the fraud. By that time, it had lost almost $100,000 of its client's money.

3) Attorney Check Scam

Owens Schine & Nicola P.C., Connecticut law firm – $200,000 loss

Insurance Litigation: *Owens, Schine & Nicola, P.C. v. Travelers Cas. & Sur. Co. of Am.* (2011 WL 3200296 (Conn. Super. Ct. June 24, 2011), *vacated*, No. CV-09-5024601-S, 2012 WL 12246940 (Conn. Super Ct. Apr. 18, 2012)).

Impact of the Fraud: The policyholder was a Connecticut law firm. An imposter who purported to be an attorney from North Carolina asked the firm to help a Chinese client collect a payment in Connecticut. The potential "client" e-mailed the law firm, which accepted the representation; Owens agreed to act as an intermediary. Subsequently, the fraudster "client" e-mailed the law firm that its debtor had agreed to send the owed funds to the firm's office. When a bank check arrived, the law firm deposited it into its client IOLTA account and, pursuant to the "client's" e-mailed instructions, had its bank wire the funds, less a fee, to the "client's" account in a South Korean bank. The original check Owens received was fraudulent, and Owens's bank charged the firm for the full amount. The law firm's IOLTA account ended up with nearly a $200,000 loss.

II. How Can Social Engineering Risks be Addressed in the Underwriting Process?

Social engineering fraud directly impacts companies' balance sheets; it threatens the financial stability of organizations, and has fundamentally changed the scope of cyber-related attack coverage in the insurance market. The advent of social engineering fraud has caused the insurance market to reconsider the traditional definition of computer risk by transforming and developing new underwriting coverages to address the sophisticated techniques used by criminals to effectuate complex fraud schemes. Not only does the insurance market aim to ensure that companies are covered for sudden and accidental loss, the market is refocusing on educating policyholders in risk mitigation techniques to stifle these fraudulent activities.[28]

A. The Challenge of Evaluating Social Engineering Risk Exposure

Organizations face many challenges in their efforts to determine the breadth of their risk and quantify the probable maximum loss (PML) of a social engineering attack. The most significant challenge companies currently face is not understanding risk assessment and diagnostics. Although there is an increased emphasis on technology solutions to heighten cyber security, the examples of BEC scams described above drive home the fact that a significant proportion of cyber-related breaches still derive from human error or process issues. At-risk companies must engage with their employees to implement a framework and infrastructure that will ultimately help protect them from social engineering fraud in a way that risk transfer cannot. Employee

[28] *See, e.g.,* Chubb *Guide to Preventing Social Engineering Fraud*, Chubb Group of Insurance Companies, 14-01-1157 (ed. 10/14), *available at* http://www.chubb.com/businesses/csi/chubb19441.pdf.

engagement and process discipline will ultimately create a culture of checks and balances. It will also contribute to a better evaluation of the risk for purposes of securing insurance coverage.

To evaluate their company's risk and insurance needs, risk managers should consider three key points:

- How much unique PII does the company collect and store internally or in the cloud? For instance, a data aggregation company faces increased risks – and barriers to obtaining tailored social engineering fraud coverage – because the company's business model is based on the collection and storage of huge volumes of PII.

- What are the physical and logistical controls in place? Are employee e-mails encrypted? Are attachments encrypted? How many people must physically, verbally or in-person sign off on wire transfers?

- Finally, the company should develop a high level of expected resiliency and incident response. Underwriters evaluating these issues are not only concerned about the potential loss of data and/or funds, but also how companies are planning, practicing, and integrating business continuity plans from the top-down.

The insurance market faces many of the same challenges that companies do in evaluating the breadth of the risk and PML of a social engineering attack. These types of attacks are new to the marketplace, and quantitative data on social engineering fraud is currently unreliable as there are too many variables that make the coverage very challenging to define. As a result, the insurance markets' pricing rationale is often inconsistent. For example, as described in more detail below, endorsements directed specifically to social engineering have been available in the market for a few years, but premiums for $250,000 sublimits have varied widely, from $500-$15,000, depending on the risk exposure of the company seeking the coverage.

B. Endorsements Covering Social Engineering Fraud

No company has systems in place to catch or eliminate all possible social engineering fraud activity. So what options are available to companies to ensure that they are protected from the sudden and accidental?

The two main types of policies that exist in the insurance market today that cover facets of social engineering fraudulent activity are crime and cyber policies. As discussed in section I. above, the insurance market has seen a significant increase in both the frequency and severity of these fraudulent social engineering schemes over the past few years.[29] In addition, the hacks have become more advanced and challenging to identify. The insurance market has responded in part by creating endorsements to crime policies specifically including social engineering fraud.

For example, Chubb's *Forefront Portfolio 3.0* Crime Insurance Form now offers a Social Engineering Fraud Endorsement. The coverage highlights for this endorsement include: vendor or supplier impersonation, executive impersonation, client impersonation and a full carve back to the *voluntary parting exclusion* found on the Chubb Crime policy. The voluntary parting exclusion bars coverage when an insured voluntarily parts with property "if induced to do so by

[29] *Ibid.*; FBI Alert No. 1-061416-PSA, Business e-Mail Compromise: The 3.1 Billion Dollar Scam.

any fraudulent scheme, trick, device or false pretense." [30] The endorsement covers employees who voluntarily part with money and/or securities if s/he is acting in good faith and is unaware that the instigator is a fraud. The endorsement provides sublimits on a per-occurrence basis of $250,000, up to $500,000 for an additional premium.

Although that sublimit may seem low, Chubb's Social Engineering endorsement is on a per occurrence basis (as is the Commercial Crime policy) so there is no annual aggregate. Each time there is a fraudulent incident that would be covered under the Social Engineering endorsement, the insured has the full limit available – and that limit will keep being reinstated throughout the duration of the policy year. In contrast, an aggregated limit would erode each time a claim was paid out, until the full limit had been exhausted.

The only way to secure Chubb's Social Engineering Fraud Endorsement is to work with Chubb as the incumbent insurer for the Commercial Crime policy, or switch to Chubb upon the next renewal cycle. This endorsement is not applicable or available to policies other than the *Forefront Portfolio 3.0* Crime Insurance Form.

Travelers has been marketing a similar endorsement, which is available only through the Travelers *Wrap+* and *Executive Choice+* product suites. Therefore, in order to secure this specific endorsement for Social Engineering Fraud, the insured would have to do a package placement of Directors & Officers Liability, Employment Practices Liability, Fiduciary Liability, Errors & Omissions Liability, Crime, Kidnap & Ransom and Management Liability with Travelers. The package requirement may not be ideal for all insureds, depending on their incumbent insurance company and their risk exposure, and companies should consider whether to move their coverage to Travelers in order to secure the endorsement.[31]

The insurance company Hiscox has taken a different, more liberal approach to coverage for social engineering fraud, allowing insureds to purchase a Cyber Deception Endorsement with a standalone crime policy or with an executive risk packaged policy. This means that Hiscox *does* need to be the insurer for the commercial crime policy, but *not* all policies associated with 'wrap' coverage such as Directors & Officers, Employment Practices, and Fiduciary. The Cyber Deception Endorsement covers phishing, spear-phishing, social engineering, pretexting and confidence trick[ing]. Hiscox currently offers limits of up to $250,000, and higher limits are available at the underwriter's discretion. Depending on the company's history, industry, number of international transactions, controls in place, etc., an underwriter could consider the risk to be manageable enough to provide additional capacity for a higher limit. In addition, Hiscox provides the first $100,000 of Cyber Deception coverage without requiring additional application information, focusing on a client-friendly approach to underwriting.[32]

Note that these endorsements are available for crime policies, not cyber policies. This is a key distinction. Social engineering fraud can result not only in direct monetary losses, but also in the theft or loss of PII, credit card information, Social Security numbers, and the like. Generally

[30] *Forefront Portfolio 3.0 Crime Insurance Social Engineering Fraud Endorsement*. (June 2014), NovickGroup, *available at* http://www.novickgroup.com/forms_and_applications/cyber%20WPV%20SE/CHUBB_SE.pdf.

[31] Management and Professional Liability Insurance. (2016). Retrieved August 28, 2016, from https://www.travelers.com/business-insurance/management-professional-liability/index.aspx

[32] Hiscox *Crime-Cyber Deception Endorsement*. (October 2014), *available at* http://www.hiscoxbroker.com/shared-documents/Crime/13868_us_crime_cyber_deception.pdf

speaking, commercial crime policies respond to loss of funds, while cyber policies respond to liabilities, and in some cases expenses incurred in connection with loss of data. All companies evaluating their social engineering fraud exposure and insurance coverage should consider the differences between a cyber risk policy and a social engineering endorsement on a commercial crime policy to ensure that the policies respond as they were intended if there were to be an incident.

C. Education and Proactive Measures

Social engineering fraud is still fairly new and the insurance market will continue to evolve in response to new claims, cases, and technology advancements. However, risk transfer techniques are just one component of an overall strategy to mitigate the risk of social engineering fraud. Organizations must take proactive steps to establish appropriate policies and procedures to address the risks of social engineering fraud, and educate all employees about their role and responsibility to help prevent this rapidly growing problem.

The important recommendations of the FBI, US-CERT, and the Chubb Group of Insurance Companies are included with this article as Attachment A.

III. What Happens When There is a Dispute?

Of course, social engineering fraud existed well before insurance companies developed endorsements specifically designed to cover it. And so policyholders and insurance companies have more than once found themselves at loggerheads over coverage for social engineering fraud losses under policies without those endorsements. As the recent cases below demonstrate, the courts have not yet reached consensus.

A. A Case Finding Coverage: *Apache Corp. v. Great American Ins. Co.*[33]

On March 27, 2013, an Apache Corporation accounts payable employee received a phone call from an individual claiming to work for one of Apache's vendors. The caller asked to change the account information for future payments to the vendor. The Apache employee notified the caller that such a request must be made on the vendor's official letterhead. A few days later, Apache's accounts payable department received via e-mail a letter, on the vendor's letterhead, requesting that the account information be changed for future payments. To verify the legitimacy of the request, another Apache employee called the number on the letterhead and confirmed the information contained in the letter. Once approved by a supervisor, Apache began making payments to the vendor's "new" account. Apache ultimately discovered the fraud when, after several months, the vendor alerted Apache that it had several delinquent bills. By that time Apache had made $2.4 million in payments to the false vendor account.[34]

Apache made a claim to recover the loss under its crime policy. Its insurer, Great American, disputed coverage. The dispute centered on the policy's provision concerning "loss … resulting directly from [computer fraud]."[35]

[33] 2015 WL 7709584 (S.D. Tex. Aug. 7, 2015)

[34] *Id*. at *1.

[35] *Id*. at *2.

Apache argued that the "fraudulent email sent by the fraudsters in this case was computer fraud and directly caused the fraudulent transfer of funds. [Apache] argue[d] that despite the intervening steps – the confirmation phone call and supervisor clearance – that took place after receiving the e-mail, the fraudulent e-mail was still a 'substantial factor' in bringing about the injury."[36]

Great American argued that "because of the human intervention that took place between the fraudulent email that was received and the loss to [Apache], the language 'resulting directly from' removes the loss in this case from coverage."[37]

The U.S. District Court for the Southern District of Texas agreed with Apache, and granted its motion for summary judgment. According to the court, "[t]o adopt Defendant's reading would be to limit the scope of the policy to the point of almost non-existence. That is, if anytime some employee interaction took place between the fraud and the loss, or anytime fraud was perpetrated any way other than direct 'hacking,' the insurance company could be relieved of paying under the Policy. Such a policy or provision would be rendered almost pointless. If Defendant had intended to cover only 'hacking,' the Policy could have been written in such a way to reflect this. However, the Policy as written is not that narrow." Instead, the court held that the "quality or severity of the intervening acts" must be weighed to determine whether the loss resulted directly from the computer fraud.[38] Here, the court held that "the intervening steps of the confirmation phone call and supervisory approval do not rise to the level of negating the email as being a 'substantial factor' in bringing about the loss. The email was a cause in fact, or 'substantial factor,' and according to the Fifth Circuit's holding in First Nat. Bank of Louisville, this is sufficient to allow coverage under the "directly resulted from" policy language."[39]

But the district court will not have the last word on Apache's right to coverage: the case is currently on appeal to the Fifth Circuit, and briefing was completed earlier this spring.[40]

[36] *Id*. at *3.
[37] *Id*.
[38] *Id*.
[39] *Id.* (internal citations omitted).
[40] Other cases finding coverage for social engineering fraud claims include:

- *Owens, Schine & Nicola, P.C. v. Travelers Cas. & Sur. Co. of Am.*, 2011 WL 3200296 (Conn. Super. Ct. June 24, 2011), *vacated*, 2012 WL 12246940 (Conn. Super Ct. Apr. 18, 2012). The basic facts of this "attorney check fraud" case are laid out in section I above. Owens's crime policy defined computer fraud as the "use of any computer to fraudulently cause a transfer of Money." The trial court held that "even though the policy is ambiguous as to the amount of computer usage necessary to constitute computer fraud, this ambiguity must be resolved in favor of the plaintiff." The court concluded that the fraud had involved sufficient use of computers to fall within the policy language. Although the court vacated the judgment the following year, it did so with no explanation, and apparently by stipulation of the parties.

- *State Bank of Bellingham v. BancInsure, Inc.*, 2016 WL 2943161 (8th Cir. May 20, 2016). An employee failed to properly log off a computer at the end of the day, which enabled a hacker to make two unauthorized wire transfers from the bank's account overnight. The Eighth Circuit upheld the trial court's ruling that the malware was the efficient and proximate cause of the loss, not the employee's error in failing to properly log off. It held that "an illegal wire transfer is not a 'foreseeable and natural consequence' of the bank employees' failure to follow proper computer security policies, procedures, and protocols." "Even if the employees' negligent actions 'played an essential role' in the loss," the court further held, "and those actions created a risk of

(continued…)

B. A Case Finding No Coverage: *Aqua Star (USA) Corp. v. Travelers Casualty and Surety Co. of Am.*[41]

Aqua Star is a seafood importer that purchases shrimp from vendors. In 2013, a hacker compromised a vendor's computer. Using information gathered from e-mail communications between Aqua Star and the vendor, the hacker sent e-mails with spoofed e-mail addresses directing an Aqua Star employee to change the bank account information for future payments to the vendor. Aqua Star employees made the requested changes and Aqua Star was ultimately defrauded of $713,890.[42]

Aqua Star sought coverage for the loss under its crime policy. The policy covered computer fraud, but included an exclusion for "loss resulting directly *or indirectly* from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System.'"[43] Travelers denied coverage, citing the exclusion. Travelers argued that the loss resulted indirectly from Aqua Star's employee – an authorized user – inputting the fraudulent account data into the company's computer system.[44]

The U.S. District Court for the Western District of Washington agreed, and granted summary judgment to Travelers. According to the court, "the entry of data into the Excel spreadsheet on Aqua Star's Computer system was an indirect cause of Aqua Star's loss." This indirectly resulted in the loss because that information was later "used to prepare a packet of materials for approval of the payment by Aqua Star's management" and was "a necessary step prior to initiating any transfer." Even if the "management did not rely upon or even review the account number in the packet," the employee used the fraudulent information "to prepare and initiate the wire transfers." This qualified as "an intermediate step in the chain of events that led Aqua Star to transfer funds to the hacker's bank accounts."[45]

Unlike the *Apache* court, the *Aqua Star* court did not evaluate the "quality or severity of the intervening acts." The court expressly rejected Aqua Star's argument that saving the fraudulent bank information in a spreadsheet "was not materially different than writing the information on a sticky note or index card." The court noted that the exclusion "may not apply in such a case," but that such facts were not before the court.[46] [47]

intrusion into Bellingham's computer system by a malicious and larcenous virus, the intrusion and the ensuing loss of bank funds was not 'certain' or 'inevitable.'"

[41] 2016 WL 3655265 (W.D. Wa. July 8, 2016).

[42] *Id.* at *1–*2.

[43] *Id.* at *2 (emphasis added).

[44] *Id.*

[45] *Id.* at *3.

[46] *Id.*

[47] Other cases finding no coverage for social engineering fraud claims include:

- *Universal American Corp. v. National Union Fire Ins. Co. of Pittsburgh, P.A.*, 25 N.Y.3d 675 (2015): The New York Court of Appeals determined that Medicare fraud was not covered under a Computer Fraud Rider because although it involved fraudulent data submitted by third parties, the act of entering or changing the data was not fraudulent – it was performed by authorized individuals.
- *Taylor and Lieberman v. Fed. Ins. Co.*, 2015 WL 3824130 (C.D. Cal. June 18, 2015): The basic facts of this variation on a "supplier swindle" scheme are laid out in section I above. The court found no coverage because

(continued…)

C. A Pending Case to Watch: *Medidata Solutions, Inc. v. Federal Ins. Co*.[48]

Medidata Solutions is a New York company that provides applications, analytics and benchmarks to facilitate medical research and run clinical trials. In 2014 Medidata discovered that it had been the subject of an international wire transfer fraud.[49] E-mails that purported to come from company executives, including the CEO and an attorney, instructed mid-level employees in the Finance Department to wire money to a Chinese bank. The impostor's e-mail included the executive's picture and the CEO's forged signature, and the "From" line was altered to appear as if it had been sent from the executive's company e-mail address. The employees were instructed to contact another individual, who posed as an attorney. Through a series of e-mails and phone calls, the impostor and fake attorney convinced the employees to transfer nearly $4.8 million to a bank account in China. The company caught on – and the impostor disappeared – when the impostor requested an additional $4.8 million. The money that had already been transferred was never recovered.

Medidata submitted the loss to its insurer, Federal, and ultimately the claim ended up in litigation. Both Medidata and Federal moved for summary judgment. In March 2016 the U.S. District Court for the Southern District of New York denied the motions without prejudice, directing the parties to conduct limited expert discovery on what the court appears to consider the key factual issue: the "method in which the perpetrator sent its emails…and discussing what changes, if any, were made to plaintiff's computer systems when the emails were received." The parties recently submitted a set of undisputed facts, and short statements on the implications of those facts.

Medidata's submission[50] focused on the policy's "Computer Fraud Coverage section, which requires a Computer Violation, defined in relevant part as 'the fraudulent: (a) entry of Data into or deletion of Data from a Computer System; [or] (b) change to Data elements or program logic of a Computer System . . . ." It argued that both prongs of that definition were satisfied. First, "the perpetrator used computer code to fraudulently change the email address in the IMF 'FROM' field from the perpetrator's genuine email address to the email address of [a Medidata employee], which was then sent to, or 'entered' into Medidata's Computer System." Second, "the fraudulent use of [the Medidata employee's] e-mail address in the IMF 'FROM' field instead of the perpetrator's genuine email address caused Medidata's Computer System to change the three distinct renderings created by Gmail of each spoofed email to display [the Medidata employee's] name and picture, causing a fraudulent change to Data elements of Medidata's Computer System."

the policy required "direct loss sustained by an Insured," and the court found that the loss was "in essence" a "third-party loss" to the client. *Id*. at *3. The court found that the policy "more likely contemplates fraudulent violations against Plaintiff that result in a 'direct loss' of Plaintiff's own money—not fraudulent violations upon which Plaintiff relies that result in a loss of client's own money, which Plaintiff wants Defendant to reimburse." *Id*. at *4.

[48] No. 15-cv-00907, Dkt. No. 64 (S.D.N.Y. Mar. 9, 2016).

[49] *Medidata Solutions, Inc.,* SEC Form 8-K, Item 8.01. Other Events (September 25, 2014), *available at* https://www.sec.gov/Archives/edgar/data/1453814/000119312514353189/d795328d8k.htm.

[50] No. 15-cv-00907, Dkt. No. 71 (S.D.N.Y. June 24, 2016).

Federal's submission[51] focused on the same policy language, but argued that the language covered "involuntary transfers effected by hackers; not voluntary transfers effected by authorized signatories." It asserted that in Medidata's case, "the sender created the emails without accessing Medidata's computers or implanting them with a virus or executable code, and that the emails did not change Medidata's computers." It argued that Medidata's claim rests merely "upon the receipt of inaccurate information" – which it alleged does not qualify as "entry" of or "change to" data, and that the perpetrator "never accessed, intruded upon, manipulated or otherwise altered Medidata's computers."

As of the time of this writing, the court has not determined the merits of the parties' respective positions. Stay tuned![52]

IV. Conclusion

Advances in technology have allowed for the globalization of economies and provided companies the opportunity for international growth. With this development, new risks have emerged, including social engineering fraud. Criminals are now targeting businesses of all types and sizes, from large multi-national corporations and technology companies to small businesses and non-profit organizations, and tricking employees into making fraudulent wire transfers. The manipulation of e-mail addresses, spear-phishing attacks, and phone call follow-ups from criminals masquerading as trusted colleagues are just a small part of how social engineering schemes are carried out. No one person is immune; the cases presented here show C-Suite executives unknowingly signing off on fraudulent wire transfers. The impact of the fraud has been far-reaching, with lost funds, damages, and legal fees running into the millions of dollars, and executives resigning from their positions when the breadth of the financial damage was uncovered.

These fraudulent practices have become increasingly common, and the insurance market has responded in part by creating endorsements under commercial crime policies to help cover the financial losses from voluntary wire transfers. At the same time, organizations have developed a heightened awareness of the need to prevent fraudulent wire transfers. Employee engagement and education, as well as system controls and process discipline, when initiated with a top-down managerial approach, can be an effective first line of defense against potentially crippling social engineering fraud.

Meanwhile, disputes over coverage for social engineering fraud under policies that do not include the newly-developed endorsements continue to wind their way through the courts. The cases decided to date have had mixed results, some finding coverage and others not. Against that backdrop, each new coverage case concerning social engineering fraud should pique the interest of policyholders and insurers alike.

[51] No. 15-cv-00907, Dkt. No. 72 (S.D.N.Y. June 24, 2016).

[52] Other pending cases include *Ameriforge Group, Inc. v. Federal Insurance Co., et al.*, No. 16-cv-377 (S.D. Tex.) and *Maxum Indemnity Co. v. Long Beach Escrow Corp.*, No. 2:16-CV-05907, 2016 WL 4199087 (C.D. Cal. Filed Aug. 8, 2016).

ATTACHMENT A

FBI Public Service Announcement
June 14, 2016
Alert Number I-061416-PSA

Business E-mail Compromise: The 3.1 Billion Dollar Scam

SUGGESTIONS FOR PROTECTION AND BEST PRACTICES

Businesses with an increased awareness and understanding of the BEC scam are more likely to recognize when they have been targeted by BEC fraudsters, and are therefore more likely to avoid falling victim and sending fraudulent payments.

Businesses that deploy robust internal prevention techniques at all levels (especially targeting front line employees who may be the recipients of initial phishing attempts), have proven highly successful in recognizing and deflecting BEC attempts.

Some financial institutions reported holding their customer requests for international wire transfers for an additional period of time, to verify the legitimacy of the request.

The following is a compilation of self protection strategies provided in the BEC PSAs from 2015.

- Avoid free web-based e-mail accounts: Establish a company domain name and use it to establish company e-mail accounts in lieu of free, web-based accounts.
- Be careful what is posted to social media and company websites, especially job duties/descriptions, hierarchal information, and out of office details.
- Be suspicious of requests for secrecy or pressure to take action quickly.
- Consider additional IT and financial security procedures, including the implementation of a 2-step verification process. For example -
    - Out of Band Communication: Establish other communication channels, such as telephone calls, to verify significant transactions. Arrange this second-factor authentication early in the relationship and outside the e-mail environment to avoid interception by a hacker.
    - Digital Signatures: Both entities on each side of a transaction should utilize digital signatures. This will not work with web-based e-mail accounts. Additionally, some countries ban or limit the use of encryption.
    - Delete Spam: Immediately report and delete unsolicited e-mail (spam) from unknown parties. DO NOT open spam e-mail, click on links in the e-mail, or open attachments. These often contain malware that will give subjects access to your computer system.
    - Forward vs. Reply: Do not use the “Reply” option to respond to any business e-mails. Instead, use the “Forward” option and either type in the correct e-mail address or select it from the e-mail address book to ensure the intended recipient’s correct e-mail address is used.
    - Consider implementing Two Factor Authentication (TFA) for corporate e-mail accounts. TFA mitigates the threat of a subject gaining access to an employee’s e-mail account through a compromised password by requiring two pieces of information to login: something you know (a password) and something you have (such as a dynamic PIN or code).

  Significant Changes: Beware of sudden changes in business practices. For example, if a current business contact suddenly asks to be contacted via their personal e-mail address when all previous official correspondence has been through company e-mail, the request could be fraudulent. Always verify via other channels that you are still communicating with your legitimate business partner.

- Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail. For example, legitimate e-mail of abc_company.com would flag fraudulent e-mail of abc-company.com.
- Register all company domains that are slightly different than the actual company domain.
- Verify changes in vendor payment location by adding additional two-factor authentication such as having a secondary sign-off by company personnel.
- Confirm requests for transfers of funds. When using phone verification as part of the two-factor authentication, use previously known numbers, not the numbers provided in the e-mail request.
- Know the habits of your customers, including the details of, reasons behind, and amount of payments.
- Carefully scrutinize all e-mail requests for transfers of funds to determine if the requests are out of the ordinary.

Additional information is publicly available on the United States Department of Justice website www.justice.gov publication entitled “Best Practices for Victim Response and Reporting of Cyber Incidents”.

WHAT TO DO IF YOU ARE A VICTIM

If funds are transferred to a fraudulent account, it is important to act quickly:

- Contact your financial institution immediately upon discovering the fraudulent transfer
- Request that your financial institution contact the corresponding financial institution where the fraudulent transfer was sent
- Contact your local Federal Bureau of Investigation (FBI) office if the wire is recent. The FBI, working with the United States Department of Treasury Financial Crimes Enforcement Network, might be able to help return or freeze the funds
- File a complaint, regardless of dollar loss, at www.IC3.gov

When contacting law enforcement or filing a complaint with the IC3, it is important to identify your incident as “BEC”, provide a brief description of the incident, and consider providing the following financial information:

- Originating[4] Name:
- Originating Location:
- Originating Bank Name:
- Originating Bank Account Number:
- Recipient[5] Name:
- Recipient Bank Name:
- Recipient Bank Account Number:
- Recipient Bank Location (if available):
- Intermediary Bank Name (if available):
- SWIFT Number:
- Date:
- Amount of Transaction:
- Additional Information (if available) - including “FFC”- For Further Credit; “FAV” – In Favor Of:

Filing a complaint with IC3

Victims should always file a complaint regardless of dollar loss or timing of incident at www.IC3.gov and, in addition to the financial information, provide the following descriptors:

- IP and/or e-mail address of fraudulent e-mail
- Date and time of incidents
- Incorrectly formatted invoices or letterheads
- Requests for secrecy or immediate action
- Unusual timing, requests, or wording of the fraudulent phone calls or e-mails
- Phone numbers of the fraudulent phone calls
- Description of any phone contact to include frequency and timing of calls
- Foreign accents of the callers
- Poorly worded or grammatically incorrect e-mails
- Reports of any previous e-mail phishing activity

https://www.ic3.gov/media/2016/160614.aspx

* * * * *

US-CERT
Security Tip (ST04-014)

Avoiding Social Engineering and Phishing Attacks

How do you avoid being a victim?

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the Internet before checking a website's security (see Protecting Your Privacy for more information).
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (see Understanding Firewalls, Understanding Anti-Virus Software, and Reducing Spam for more information).
- Take advantage of any anti-phishing features offered by your email client and web browser.

US-CERT Security Tip (ST04-014), Avoiding Social Engineering and Phishing Attacks (Last Revised February 2013), *available at* https://www.us-cert.gov/ncas/tips/ST04-014.

* * * * *

Chubb Guide to Preventing Social Engineering Fraud

Counter Measures For Combating Social Engineering Fraud

The best defense for combating social engineering fraud is awareness through corporate culture, education and training. It is not enough for a workforce to simply follow a policy guideline; employees must be educated on how to recognize and respond to an attacker's methods and thus become a "human firewall."

A proper counter measure training program should include the following measures:

- Conduct a **data classification assessment**, identifying which employees have access to what types and levels of sensitive company information. Know who the primary targets of a social engineering scheme are likely to be. Remember, all employees are at risk.

- **Never release confidential or sensitive information to someone you don't know** or who doesn't have a valid reason for having it – even if the person identifies himself or herself as a co-worker, superior or IT representative. If a password must be shared, it should never be given out either over the phone or by email.

- Establish procedures to **verify incoming checks and ensure clearance prior to transferring any money by wire.**

- Reduce the reliance on email for all financial transactions. If email must be used, **establish call-back procedures to clients and vendors** for all outgoing fund transfers to a previously established phone number, or implement a customer verification system with similar dual verification properties.

- Establish procedures to **verify any changes to customer or vendor details**, independent of the requester of the change.

- **Avoid using or exploring "rogue devices"** such as unauthenticated thumb/flash drives or software on a computer or network.

- **Be suspicious of unsolicited emails** and only open ones from trusted sources. Never forward, respond to or access attachments or links in such emails; delete or quarantine them.

- **Avoid responding to any offers made over the phone or via email.** If it sounds too good to be true, then it probably is. This could include unsolicited offers to help to solve a problem such as a computer issue or other technical matter.

- **Be cautious in situations where a party refuses to provide basic contact information**, attempts to rush a conversation (act now, think later), uses intimidating language or requests confidential information.

- Physical documents and other tangible material such as computer hardware and software should **always be shredded and/or destroyed prior to disposal** in any on-site receptacles, such as dumpsters.

- **Proactively combat information security complacency** in the workplace by implementing internal awareness and training programs that are reviewed with employees on an ongoing basis. This includes developing an incident reporting and tracking program to catalog incidents of social engineering and implementing an incident-response strategy.

- **Train customer service staff to recognize psychological methods that social engineers use:** power, authority, enticement, speed and pressure. If it is important enough to move quickly on, it's important enough to verify.

- Consider **conducting a recurring, third-party penetration test** to assess your organization's vulnerabilities, including unannounced random calls or emails to employees soliciting information that should not be shared.

- **Guard against unauthorized physical access** by maintaining strict policies on displaying security badges and other credentials and making sure all guests are escorted. Politely refuse entry to anyone "tailgating." Keep sensitive areas, such as server rooms, phone closets, mail rooms and executive offices, secured at all times.

- **Monitor use of social media outlets, open sources and online commercial information** to prevent sensitive information from being posted on the Internet.

Chubb Group of Insurance Companies, 14-01-1157 (ed. 10/14), pages 6-7, *available at* http://www.chubb.com/businesses/csi/chubb19441.pdf

Authors

Kathleen (Katie) Crowe joined Aon in March 2016 and is currently a Senior Account Specialist in the Aon Risk Solutions Department. Her primary responsibility is to manage, drive and administer risk management & insurance brokerage services to a broad range of clients for the purpose of providing expert guidance and support on a worldwide basis. Aon Risk Solutions DC supports clients in and around the greater Washington, DC metropolitan area, collaborating on all lines of Property & Casualty coverage for clients both domestic and international.

Previous experience includes over three years in the international energy industry working at the AES Corporation as a Risk Analyst managing a $40M captive international property program. She received her ARM Certification in 2014 and was awarded the Rising Star of the Year Award by RIMS in 2016.

Contact: kathleen.crowe@aon.com

Jennifer O. Farina is a litigator who advises and represents policyholders seeking to maximize their coverage under a variety of insurance policies, including general liability, property, fidelity, and directors and officers policies. She also counsels clients in connection with policy renewal negotiations and the appropriate handling of insurance assets and related liabilities in corporate transactions.

Contact: jfarina@cov.com

Laura Hanson focuses her practice on commercial insurance coverage and litigation, which she has handled in the state and federal trial and appeals courts around the country, including four state supreme courts and four different federal circuit courts of appeals. Laura repeatedly has been named a Super Lawyer in the category of insurance coverage, and is the former ICLC co-chair.

Contact: lhanson@meagher.com

Lucy Thomson, CISSP, focuses her practice on cybersecurity, global data privacy, compliance and risk management. An ABA Science & Technology Law Section past chair, she served as a Justice Department white-collar crime prosecutor, senior engineer at global technology company CSC, counsel to IGOs, and Consumer Privacy Ombudsman in major bankruptcy cases.

Contact: lucythomson1@mindspring.com