SEPTEMBER 2015

COMMENTARY

Phishing for Corporate Dollars: The Emerging Global Threat Posed by Spear Phishing and Business Email Compromise

In August 2015, the FBI issued an alert describing the newest form of cyberattack—the Business Email Compromise ("BEC").[1] BEC is a sophisticated mutation of the now-common spear phishing data breach technique.[2] In a BEC scam, a hacker often impersonates a high-ranking corporate executive and sends a "spoofed" email[3] to a carefully selected target who generally has access and authority to transfer large sums of money on behalf of the company. Unlike traditional phishing schemes, BEC scams are well researched. Successful hackers troll the social media sites of the target employee, review corporate web pages for contact information, and read professional writings to better understand the corporate culture as well as the individual characteristics of the target employee, all with the goal of convincing that employee to part with the company's cash. Consider the following three scenarios (all based on actual cases reported to the FBI):

- 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.[4]

- A business receives a fraudulent invoice from what appears to be a longstanding supplier requesting that the next payment be sent via wire to an alternate account. The spoofed 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 supplier follows up with the business, sending an angry email expressing frustration that the funds were not timely sent. When the two business partners realize the mix-up, it is too late to recover the funds.[5]

- An employee's hacked personal email account sends fraudulent invoices to a number of vendors requesting immediate payment to phony company bank accounts. The hacker has researched the vendor relationships and knows that several of the invoices are overdue. As a result, the scheme uses social engineering—a form of manipulation and trickery based on the human tendency to obey orders—to influence the actions of the vendors by inserting a sense of urgency ("Please send payment immediately, or future deliveries will be cut off!"). Many of the vendors quickly comply for fear of having their supplies embargoed. The result is a windfall to the hacker and a loss to both the vendors and the victim company.[6]

Although the factual scenarios vary, the general BEC scheme follows a very specific pattern:

Taking the Bait: How Hackers Gain Access

In the first generation of phishing schemes, most attacks relied on a combination of fraudulent emails with links to bogus websites to obtain internet users' information.[7] In recent years, however, cybercriminals have refined their methods and increased the amount of research performed on each target so as to maximize the return on each cyber attack. Whereas a traditional phishing attack may have blanketed an entire database of email addresses, new spear phishing schemes target specific individuals within specific organizations.[8]

A BEC scam, therefore, usually begins in one of two ways: (i) by getting an unsuspecting employee to click on an email attachment that compromises the network (i.e., malware); or (ii) by spoofing an email of a high-ranking official in the company. Spear phishers, however, usually research their target and the company as a whole in order to craft highly convincing emails. The telltale signs of scam emails—poor grammar, suspicious requests, and uncharacteristic language—won't give the BEC scammer away. By mining corporate webpages and social networks, for example, the personalization and impersonations used in the spear phishing emails can be extremely accurate and compelling. Because the email appears to come from a known and trusted source, the request to release valuable data or to take urgent action appears more plausible. Thus, hackers actually employ low-tech tactics to achieve high-dollar corporate fraud.

Hook, Line and Sinker: Using Trust, Urgency, and Social Engineering to Commit Financial Fraud

The metaphoric "spear" in spear phishing is the email itself, received by a carefully selected yet unsuspecting employee. The email looks official, appears to come from a high-ranking corporate executive, and 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. But before the hacker ever spoofs the email account of the high-ranking corporate executive or drafts the text of the email, the attacker does a significant amount of legwork.

- In many cases, the hacker has gained access to the corporate email server and may have access to the high-ranking executive's calendar. As a result, the hacker knows to send the email when the executive is traveling or otherwise out of the office (and unavailable for verbal confirmation before the wire transfer is made).

- The hacker has also likely researched—perhaps extraordinarily carefully—the target employee and possibly compromised his or her email account as well as that of someone in the accounting department. The amount of money requested in the fraudulent transfer is carefully tailored to be within the expected range of the payments capable of being authorized by the target employee. The language of the request mimics past email requests; uses similar vocabulary; pertains to goods, services, or business partners with whom the company normally deals; and is requested in accordance with usual payment schedules.

- In some cases, the email will identify or even cc an employee in the accounting department to give an added sense of authenticity. Although the email address of the target employee is accurate, all others cc'd on the email chain will have slightly modified email addresses (at times the emails are modified so slightly that the change is undetectable), so that only the hackers are receiving the messages. For example, *Accounting@CompanyABDC.com* instead of *Accounting@CompanyABCD.com*.

- In another scenario, a hacker may compromise and monitor the email account of someone who receives invoices from vendors or suppliers. The hacker then modifies a legitimate invoice to reroute payment to a new bank account number or address. The hacker doesn't need to compromise the vendor's system; a spoof email from *John@Vendorcorp.com* instead of *John@Vendorco.com* including the fraudulent invoice is enough to accomplish the goal.

- Hackers often use social engineering to trick their victims into acting quickly. Thus, the hacker may insert a false sense of urgency into the text of the email to spur the target employee to wire the funds while the executive is out of the office. In other cases, the hacker may convince the target that the financial transaction relates to a secret business acquisition or a merger, thereby encouraging the target not to disclose the transfer of funds to others. Both tactics are designed to manipulate the target by portraying the orders as coming from an authority figure.

Unfortunately, the hacker's research efforts are often successful. Recent examples demonstrate that companies of all sizes in all sectors are at risk. Over the past several months, many have fallen victim to similar schemes, losing millions of dollars.[9]

Once the target wires the money, the hackers work to quickly transfer the funds from the overseas bank account before the company discovers the breach.

Removing the Hook: Conducting an Internal Investigation after a BEC Attack is Discovered

Discovering a data breach within your organization can be alarming, especially in the early hours and days when it is impossible to ascertain the full extent of the damage to corporate systems and reputation. At the outset, there are a number of operational, legal, and strategic questions the company's in-house legal team should explore:

OPERATIONAL QUESTIONS	LEGAL AND STRATEGIC QUESTIONS

• Has a breach occurred?
• When did such a breach occur?
• What is the scope of the breach?
• How can we isolate the breach and limit damage?
  ° Is it safe to use company email, or should we consider alternative methods of communication?
  ° Should we report the fraud to the relevant bank/financial institution and request that the funds in the fraudulent account be frozen?
  ° Is it possible to retrieve corporate funds improperly sent to offshore bank accounts?
  ° In the short-term, how should we interact with our customers and vendors to minimize business disruption?
	• Do we have any legal obligation to give notice of the data breach?
	• Do we have insurance coverage for this breach, and if so, do we want to submit a claim?
	• Are any third parties (e.g., business partners, vendors, service providers) liable to us for this breach?
	• Should we notify law enforcement of the breach?
	• How can we repair any damage to the corporate brand, or to the company's reputation within the industry?
	• How can we rebuild relationships with our vendors and customers who may have received spoofed emails and been victims of the BEC scam?
	• How do we quickly train employees to recognize spear phishing attacks so as not to fall victim to BEC scams in the future?

When a company is confronted with evidence of a data breach that has potentially compromised its systems, an effective corporate internal investigation protected by the attorney-client privilege can benefit the company in a number of ways:

- Revealing all of the relevant facts so that management and/or the board can make a fully informed decision regarding whether to report the breach to law enforcement or other government entities;

- Stopping the conduct to prevent further breaches; and

- Memorializing the company's good-faith response to the facts as they become known.

Each of these benefits can be achieved if the investigation is well designed with a specific work plan that addresses document collection and review, witness interviews, careful analysis, and a final report in the format that best serves the company's interests. Use of experienced outside counsel and/or a cybersecurity consultant may be helpful to focus the internal investigation and efficiently identify and contain the source of the breach.

Don't Become a Trophy Phish: Five Steps for Preventing Catastrophic Damage

Many governments now require companies to undertake reasonable security measures to avoid data breaches and other cybercrimes that potentially expose unencrypted personal information. For example, the U.S. Gramm-Leach-Bliley Act ("GLBA") Safeguards Rule and the broader European Directive 95/46/EC, Article 17, both require that companies employ reasonable or appropriate administrative and technical security measures to protect consumer information. In addition, states including California and Nevada have passed laws that impose similar responsibilities.[10] Massachusetts has gone so far as to specifically require companies to train their employees on the importance of personal information security.[11] Failure to utilize due diligence in avoiding data breaches and other cyber incidents generates exposure to both civil litigation and government enforcement actions, not to mention intangible costs such as loss of customer trust and brand damage.

The prevalence of phishing attacks, and the above-referenced legal obligations to employ "reasonable security measures" to prevent data breaches, makes it increasingly urgent that companies undertake basic precautions to prevent significant harm.

1 REVIEW WIRE TRANSFER PROTOCOLS.

Review and strengthen the controls around wire transfers and, in particular, international wire transfers. This could include:

- Requiring two forms of communication/authentication before a wire will issue (e.g., email and verbal approval). For example, use a follow-up phone call to verify significant transactions. When calling, be sure to use a known company or mobile number rather than responding to a request to "call me at XXX-XXXX with any questions." The planted phone number could be a part of the spoof. Also, limit the number of individuals authorized to approve fund transfers, vary the approvals by different dollar thresholds, and flag new individuals who have approval authorization;

- Requiring approvals from two different persons apart from the requestor to initiate a wire; and

- Authenticating the recipient party at the supposed foreign vendor before an internally authorized wire will issue.

2 TRAIN EMPLOYEES ABOUT DATA SECURITY.

- Provide regular, periodic education to all executives and employees on data security, including phishing and business email compromise. The training should be tailored to a particular employee's job description, so that he or she will understand the danger these attacks pose and be capable of spotting potential fraud. Repeat the training at regular intervals and update the training materials to account for new schemes/techniques.

- For finance or treasury employees, including those who actually process wire transfers, training should include clear direction that employees should be suspicious of requests for secrecy or pressure to act quickly.

- Encourage employees to question suspicious wires and raise red flags up the corporate chain of command, without retaliation. An employee who senses something is wrong is usually right. As a result, employees should be aware of and expected to use confidential hotlines to report questionable data security behavior.

- Revise corporate policies and procedures, as well as confidentiality agreements with employees, consultants, and third parties trusted with confidential information, with a focus on data security.

- Consider implementing strict controls on users with privileged access (e.g., Two-Person Integrity("TPI") for access to highly sensitive information).

3 TAKE PARTICULAR PRECAUTIONS WHEN USING WEB-BASED EMAIL.

- The FBI has recently issued warnings regarding web-based email accounts, because they are often more susceptible to being hacked. As a result, companies using Google Docs or Gmail should enable Google's two-step verification/two-factor authentication to prevent an outside party from logging into Google without the requisite authenticator token.

- For even greater security on web-based applications, consider using a Security Assertion Markup Language ("SAML")-based Single Sign-On ("SSO") service to control usernames, passwords, and other information used to identify users.

4 AUDIT, TEST, AND IMPROVE COMPANY TECHNOLOGY.

- Companies will benefit from keeping anti-phishing software, operating systems, and browsers up to date with the latest patches. Such programs serve as an important defense.

- If possible, register internet domains that are only slightly different from the company's legitimate domain name.

- Create a system that flags emails with extensions that are similar but not identical to company e-mail (e.g., ".co" instead of ".com" and ".ed" instead of ".edu").

- Once you have invested in the technology to protect your company from spear phishing, test it out through audits that include business email compromise scenarios (e.g., attempt to initiate a wire through direct emails to finance staff).

- If IT notices what appears to be a breach or compromise, but there is no immediate fallout, proceed as though the company's systems have been compromised. Err on the side of caution by forcing password resets.

5 KNOW YOUR CUSTOMERS.

- Make an effort to learn the frequency, amounts, details, and reasons for certain payment practices of your customers.

- Verify changes in vendor payment location and confirm requests for transfer of funds to new accounts.

Conclusion

Spear phishing in general, and BEC in particular, are increasingly prevalent because they are effective. In 2014, the average total cost of one data breach to a U.S. company was $6.5 million, up from $5.9 million in 2013.[12] Moreover, these estimates do not include intangible harms that accompany data breaches, such as damage to corporate reputation and brand, as well as dips in customer confidence. Recent case examples demonstrate that the threat posed by spear phishing and BEC scams is truly global in nature.

Unfortunately, cybercriminals will continue to use these tactics as long as they are able to infiltrate the emails and servers of corporate organizations. Although there is no way to prevent a spear phishing attack, risk mitigation measures such as employee training, two-step authentications for wire transfers, and open communication can significantly decrease the risk of losing corporate dollars and help companies avoid the phish hook. In addition, these measures make it easier to defend against civil litigation and government regulators who may, in the wake of a significant cyber incident, claim that a business failed to comply with its legal obligations to undertake reasonable measures to prevent data breaches.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Jeff Rabkin
San Francisco
+1.415.875.5850
jrabkin@jonesday.com

Neal J. Stephens
Silicon Valley
+1.650.687.4135
nstephens@jonesday.com

Shireen M. Becker
San Diego
+1.858.314.1184
sbecker@jonesday.com

Undine von Diemar
Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Jonathan Little
London
+44.20.7039.5224
jrlittle@jonesday.com

Peter J. Wang
Shanghai/Beijing
+86.21.2201.8040/+86.10.5866.1111
pjwang@jonesday.com

Sheila L. Shadmand
Dubai
+971.4.709.8408
slshadmand@jonesday.com

Jay Johnson
Dallas
+1.214.969.3788
jjohnson@jonesday.com

Rasha Gerges Shields
Los Angeles
+1.213.243.2719
rgergesshields@jonesday.com

Michael G. Morgan
Los Angeles
+1.213.243.2432
mgmorgan@jonesday.com

Gregory P. Silberman
Silicon Valley
+1.650.739.3954
gpsilberman@jonesday.com

Olivier Haas
Paris
+33.1.56.59.38.84
ohaas@jonesday.com

Alexandra A. McDonald, an associate in the San Francisco Office, assisted in the preparation of this Commentary.

Endnotes

1 Federal Bureau of Investigation, Internet Crime Complaint Center ("FBI IC3"), Alert No. I-082715a-PSA, "Business Email Compromise" (Aug. 27, 2015); *see also* FBI IC3, Alert No. I-012215-PSA, "Business Email Compromise" (Jan. 22, 2015).

2 "Phishing" refers to hackers' attempts to steal the identities of online users by gaining personal information; "Spear phishing" is a more sophisticated version of phishing that targets specific individuals that fit a certain profile, rather than mass amounts of online users.

3 *See* FBI IC3, Alert No. I-012215-PSA, *supra* note 1. A "spoofed" email is one that has the appearance of legitimacy but in reality is fraudulent. The goal of a spoofed email is to fool the recipient into thinking it came from a specific, trustworthy source. A spoof may approximate the legitimate email address, but insert an extra letter in the text, change a letter, or delete a letter. For example, *Jane@Company465.com* instead of *Jane@Company456.com*, or *Bob@CorprationXYZ.com* instead of *Bob@CorporationXYZ.com*. By using an email alias that matches the impersonated target, the spoof may be even less detectable. For example, the sender field only displays "Jane Smith," but a click into more details will expose the "*Jane@Company456.com*" address.

4 *See* Federal Bureau of Investigation, "Business E-Mail Compromise: An Emerging Global Threat," Aug. 28, 2015.

5 *See* FBI IC3, Alert No. I-012215-PSA, *supra* note 3.

6 *Id.*

7 For example, the 1995 "AOHell" scam "mail bomb[ed]" users' email accounts," and the 1996 "Samy" scam sent virus-infected links to users through their MySpace profiles. *See* Simson Garfinkel, "Illegal Program Troubles America Online," *The Boston Globe*, April 21, 1995; Daniel Bukszpan, "6 Notorious Hackers and Their Second Careers," *Fortune* (March 18, 2015, 1:06 PM EDT).

8 These emails are sent one at a time from a specific account to a specific individual. The email messages may come from outside networks using look-alike domain names and/or impersonating the domain names used by a trusted vendor/supplier. Sometimes, however, the emails are sent from within the targeted organization using a compromised account or email server. As a result, the email never crosses the network perimeter where email content filtering controls are positioned to quarantine potentially fraudulent messages and malicious attachments.

9 The FBI's August 27, 2015 Alert cautions, "[t]here has been a 270 percent increase in identified victims and exposed loss since January 2015. The scam has been reported in all 50 states and in 79 countries." FBI IC3, Alert No. I-082715a-PSA, *supra* note 1. San Jose-based tech company Ubiquiti revealed it had fallen victim to a $46.7 million spear phishing scheme in 2015. *See* Ubiquiti Networks, Inc., Form 8-K, at 1 (Aug. 4, 2015). Similarly, the Scoular Co., an 800-employee company based in Omaha, Nebraska, was conned out of $17.2 million in February 2015. *See* Russell Hubbard, "Imposters bilk Omaha's Scoular Co. out of $17.2 million," *Omaha World Herald* (Feb. 5. 2015, 1:00 AM).

10 *See* CAL. CIV. CODE § 1798.81.5 (Deering 2015); NEV. REV. STAT. ANN. § 603A.210 Lexis-Nexis 2015).

11 *See* 200 MASS. CODE REGS. 17.04(8) (LexisNexis 2015).

12 Ponemon Institute, "2015 Cost of Data Breach Study: United States," *Ponemon Institute Research Report*, May 2015, at 1 (sponsored by IBM).