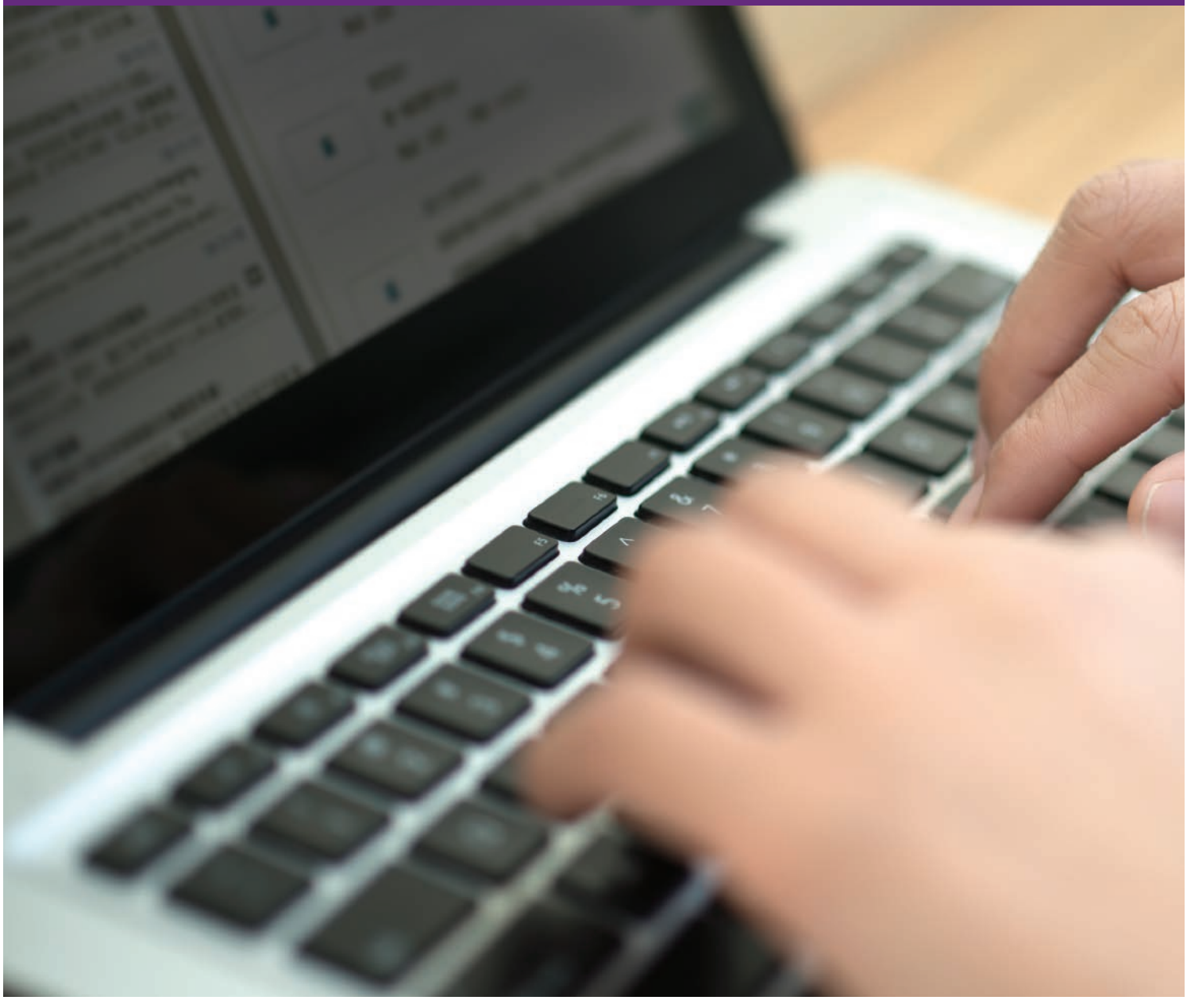
ASSOCIATION FOR FINANCIAL PROFESSIONALS

AFP Payments Security Guide

Trust, But Verify: How to Stop Business Email Compromise Attacks

Underwritten by

MUFG UnionBank



Payments fraud and cyber security are a real challenge facing businesses of all sizes when managing their working capital. For this reason, MUFG Union Bank, N.A., is pleased to sponsor AFP's second *Payments Security Guide*. This guide complements our organization's investment in fraud prevention education programs and products.

Even with advancements in fraud prevention and detection, the national statistics are high. According to *AFP's 2016 Payments Fraud and Control Survey*, 73 percent of finance professionals report that their organizations were targets of payment fraud in 2015, and of those 71 percent were victims of check fraud.

This reality for financial professionals supports the importance of this informative and actionable *AFP Payments Security Guide*. The data, examples, and prevention strategies in this booklet will enable treasury professionals to better identify and combat fraud.

Payment breaches are not entirely preventable; however, the services available from banks coupled, with the helpful information outlined in this guide, can help decrease incidents. We commend AFP's commitment to educating readers of this guide on potential fraud risks and we plan to share this booklet with our clients. We look forward to discussing with customers, strategies to mitigate potential risks to their businesses.

Best regards,

Ranjana B. Clark
Head of Transaction Banking
MUFG Union Bank, N.A.

Trove of Internet Data Makes BEC (Business Email Compromise) Attacks More Sophisticated—and Believable

Defense Tech is Necessary but Humans are the Final Defense

The corporate world was unpleasantly surprised five years ago when EMC's RSA security division was hacked, and data related to its SecurID security product—used by thousands of companies to secure critical information—was stolen. Ultimately, no customer networks were breached, but the attack ended up costing EMC more than $60 million to rectify. The incident highlighted how sophisticated cyberattacks have become, as well as the fact that the weakest of a company's cyber defenses is its own employees.

The first step of the three-part attack, as described by RSA in a blog post, was a phishing email titled "2011 Recruitment Plan" that was sent to the members of two small groups. It was crafted authentically enough to trick an employee into retrieving it from spam and opening the attached Excel file, releasing malware that allowed the hacker to control the computer remotely. Armed with the employee's passwords, the hacker infiltrated systems and entered the accounts of other employees who had access to sensitive data. Finally, the hacker sent the data to a hacked server at a hosting provider and then on to the hacker, believed to have been a state-sponsored entity.

"Whaling" attacks—attacks that target executives holding the power of the corporate purse—often rely solely on the email message to trick targeted executives into sending funds, without any malware component.

Most basic cyberattack strategies have changed little over the last decade, but they have become much more detailed, authentic-looking, and thus believable. So much so that "whaling" attacks—attacks that target executives holding the power of the corporate purse—often rely solely on the email message to trick targeted executives into sending funds, without any malware component.

Edward Mundt, CTP, director of treasury at Hard Rock Café International, recently received an almost perfect facsimile of the company's internal email from the company's longtime president and CEO. It even had the telltale photo marking all of the CEO's Microsoft Outlook emails. The message said that the company was about to ink an acquisition, secrecy was imperative, and payments should be made strictly through him. Similar emails were sent to Mundt's predecessor and a vice president of accounting.

"The chink in the armor was the request to bypass the CFO, and then when I hit 'reply' I could see it wasn't his email address," Mundt said.

Fortunately, the vice president of accounting was also suspicious. Nevertheless, said Mundt, the email was a nearly perfect replica of an internal email message, and a less experienced treasury executive, eager to please superiors, could very well have been duped.

In fact, more executives are being duped by business email compromise (BEC) schemes. The FBI reported in late August 2015 that there had been a 270 percent increase in BEC victims since the start of the year, and its Internet Crime Complaint Center (IC3) had compiled statistics on more than 7,000 U.S. victimized companies—with total dollar losses exceeding $740 million—since it started tracking the email scams in late 2013. According to the 2016 AFP Payments Fraud & Control Survey, fifty percent of the respondents reported having been subjected to attempted and/or actual BEC fraud.

The FBI is likely recording only a small fraction of the scams taking place. The BEC increase appears to stem from more whaling attacks. Alastair Paterson, CEO and co-founder of Digital Shadows, which analyzes clients' digital footprints to determine vulnerabilities, reports a "tremendous rise of whaling attacks in very recent time," including one trying to impersonate him. The increase in BEC attacks is partly the result of better malware defenses. More importantly, fraudsters have ever more data at their disposal, much of it freely available over the Internet and some for sale through the ominous sounding "dark web." Fraudsters can monitor where executives are, what they're doing in their business and personal lives, their health and other records—enough to persuade targeted underlings to send funds, despite company procedures and their better judgment.

This report will focus on whaling attacks, examining first how fraudsters develop detailed profiles of corporations and

their executives. It will then explore how cybercriminals go about constructing persuasive messages, including those harboring malware that can help fraudsters create even more convincing emails. Finally, it will examine the basic steps companies can take today to minimize—if never completely eliminate—cyberthreats.

"Know your enemy" has been longtime truism, and understanding the different types of cyberperpetrators and what they are looking for is essential for companies to set up viable defenses.

Building Profiles

Different Cyberperps Seek Different Corporate Data

"Know your enemy" has been longtime truism, and understanding the different types of cyberperpetrators and what they are looking for is essential for companies to set up viable defenses. The first and most populous rung is comprised of individuals playing the odds by sending out scam emails to a broad swathe of recipients, in anticipation of a few bites. Those emails have become more sophisticated than the proverbial Nigerian-businessman-seeking-a-short-term-loan scams, but they are typically detected by attentive employees and off-the-shelf technology defenses. Any accompanying malware tends to be a seasoned variety that's quickly spotted.

Nevertheless, a small percentage of scam email attacks are successful. And their goal usually isn't to extract money but rather data and information that can be sold over the internet, providing more sophisticated BEC attackers with a critical layer of information about companies and the executives who work for them.

Next are crime syndicates, which use the information generated by the first rung. According to Dan Hushon, CTO of Computer Sciences Corp., crime syndicates are flush with cash and talent. They tend to scour the dark web for exploitation tools, which they proceed to modify and improve upon in order to pursue their schemes. This rung also tends to target a wide range of organizations.

The top rung is comprised of state intelligence services, which Hushon described as "incredibly well funded and staffed, with an infinite level of patience and resources." Employing techniques including advanced persistent threats (APTs), they tend to go after organizations with highly sensitive information, including those in the defense and infrastructure sectors, and they have the wherewithal to devise multi-faceted and often patient strategies to compromise and then exploit a target. RSA's 2011 attacker neatly fits that description.

Cybercriminals Build Profiles from Public to Dark Web Data

Companies are faced with a variety of cyberthreats these days, from data theft to denial-of-service attacks that may or may not seek ransoms to get systems up and running again. To be successful, all attacks require some level of target profiling, and that requires the gathering of data. BEC attacks aimed at a specific executive or corporate group of executives in treasury, or another department entrusted to make payments, require lots of accurate and current details to persuade highly educated and savvy targets. Often they present a realistic scenario that creates a sense of urgency and prompts the executive to send funds, perhaps skirting established procedures. Or the goal may be to persuade the target to click a link in the email, releasing malicious software that can hide from the computer's defenses for days or weeks, waiting for remote commands from the fraudster.

Unfortunately, the internet provides a treasure trove of free information. Top executives are often listed on company websites or in SEC filings, and Google searches can fill in many of the blanks. Todd Waskelis, executive director at AT&T Security Consulting, notes that www.pastebin.com and similar websites can be used as repositories for documents or data such as password files or telephone numbers stolen in prior breaches of corporate networks. The data may be dated, but more current and detailed data can be purchased over the dark web—networks that use the public internet but require credentials to enter.

"Then there are underground sites in the dark web with high-value data from recent breaches," Waskelis said, such as Sony Pictures Entertainment's in November 2014, in which stolen data ranged from employees' personal information to sensitive emails between employees to even executive salaries.

Tracking Executives' Movements—The Downside of Social Media

Crime syndicates scour the dark web for data to build accurate and detailed profiles and create scenarios that are believable enough to elicit payments from treasury or another department endowed with payment powers. For such scams to work, however, they must coincide with current reality. An urgent request for a wire transfer from the CFO or CEO is more effective when that top executive is away from the office and difficult to communicate with.

Social media websites such as LinkedIn, Facebook, Instagram and Twitter can provide those final touches, including the executives' whereabouts, schedule, and who he or she is meeting with. Even seemingly innocuous information, like the great meal he or she ate in one of Bangkok's top restaurants, can be the missing piece that completes a fraudster's pitch.

When BEC Emails are Turbo-charged with Malware

Fraudulent emails may be carefully crafted to persuade the targeted victim to click on a link, releasing malicious malware into his or her computer. Craig Williams, who runs the teams investigating cyberthreats at Cisco Talos, said eight percent of the 500 billion spam messages passing through its technology daily carry malware attachments. In some cases, he adds, the malware will link users to phishing sites designed to replicate his or her corporate email login page, corporate credit card or bank portals, in order to capture credentials. Sophisticated man-in-the-middle malware can even send the user on to the actual site, so the credential theft goes unnoticed.

If an executive's email account is compromised, the cybertransgressor can heighten the authenticity of the fraudulent emails, for example, by copying the telltale photo of the email's sender, such as the company's CEO. In addition, said Mary Ann Miller, a senior director and authority on enterprise fraud and risk management at NICE Actimize, some malware logs keystrokes, captures credentials, and enters the email account.

"The fraudster can then monitor the email traffic to understand the relationship between the company and its suppliers, and who the company needs to pay," Miller explained. "The fraudster could then spoof the supplier's CFO or top accountant, saying the organization has changed banks and instead send the payment to a different bank account: the fraudster's."

Constructing the Message

Watch Out for Reasonable Requests

Unreasonable requests for fund transfers raise red flags, so fraudsters—no dummies—design their fraudulent emails to be as reasonable as possible. The more reasonable the request, Hushon said, the less likely the target executive will question it. For example, a fraudster impersonating a CFO emails the treasurer to say she just discovered that the company she is negotiating to acquire—a report the fraudster read about in *The Wall Street Journal*—has a critical subcontractor that must also be acquired.

"The assistant treasurer knows about the acquisition, and it is only logical that the acquired company could have an auxiliary firm that's closely tied to it, and he can see the payment as a reasonable way to sew some additional value into the deal," Hushon said.

Perhaps the email is followed up by a phone call from a name the assistant treasurer doesn't recognize but who identifies himself as an attorney representing the acquiring company. Thanks to Google Voice, his name and a U.S. telephone number appear on the assistant treasurer's office phone, a validating indication. The fraudulent attorney also drops names of others working on the deal, unearthed from news articles and social media references.

"Now all of a sudden the criminal might know a lot more about the deal than the employee, and that's when things start to happen," Hushon said.

Misspellings and other dead giveaways of fraud are rare these days, and oftentimes the emails not only look realistic but the senders clearly understand the company's business and how finance departments work.

Misspellings and other dead giveaways of fraud are rare these days, and oftentimes the emails not only look realistic but the senders clearly understand the company's business and how finance departments work.

"APTs actually hire people with accounting backgrounds so they can emulate accounts payable or accounts receivable (A/R) staff. When they successfully infiltrate a network, they can create fake user accounts or companies that seem

legitimate and get past payroll, processing and A/R," said Kalani Enos, who heads up security, risk and compliance at Hard Rock, and does cybersecurity-related work on a contractual basis for the federal government.

... And Other Subtle Tells

Hushon's example brings up other key elements that often accompany BEC attacks. For one, the top executive supposedly seeking the funding is unavailable and has supposedly directed a surrogate to carry out the request. And two, the request is urgent.

In a recent attack directed at CSC, Hushon says, the fraudster emailed a junior finance executive and, representing himself as a key deal participant, said CEO John Lawrie was close to closing a secretive acquisition. In the email the fraudster also noted contacting CFO Paul Saleh by referencing an email supposedly from Saleh that was pasted below.

"They actually understood the organizational chart and who would be contacting who on such a transaction, and the fraudster brought those people a priori into the conversation, to try to dissuade any secondary validation," Hushon said. Fortunately, the targeted executive grew suspicious and reported it.

Such a hush-hush acquisition also implies a sense of urgency, which is typical in BEC attacks. Other tactics can also prompt more junior executives to bypass security measures and pull the payment trigger. Mike Spanbauer, vice president of security test and advisory at NSS Labs, points to "rage notes" that may entail the fraudster posing as a top executive and complaining about the poor performance of an underling's department before threatening the lower-level executive with termination.

"Taking a hostile stance and instilling fear could prompt the subordinate to send the funds without completing the typical due diligence. The psychology fraudsters use is a variable that's hard to predict," Spanbauer said.

On the other end of the spectrum, fraudsters phishing for sensitive personally identifiable information (PII) may impersonate a firm that company XTZ regularly does business with and request information to facilitate their business relationship, such as a list of employee contacts. Or a treasury executive could receive a realistic but fake fraud alert from the company's bank complaining of a breach and seeking to update security information.

"Fraudsters prey on people's good intentions to do the right thing," Miller said.

Trim the Digital Footprint of PII

The Obvious Steps Too Often Overlooked

Given that building detailed profiles of executives and their companies is essential to conducting a successful BEC scam, it follows that the first step in defense is to limit one's digital footprint. That means reviewing their websites to remove key information, such as email addresses, phone numbers and other potentially problematic details. Much of the information in securities and regulatory filings, available online, may be required and unavoidable. However, marketing materials, conference brochures discussing upcoming speaking events of a company's executives, and other publicly available materials should be scoured for PII and other sensitive information.

Top executives should be careful of what they post on social media sites, especially if they provide their timely whereabouts, and should be skeptical of requests from strangers to join their LinkedIn network.

Top executives should be careful of what they post on social media sites, especially if they provide their timely whereabouts, and should be skeptical of requests from strangers to join their LinkedIn network.

"Anyone with an important position in a company should ensure their security and privacy settings are appropriate on social media websites, such as Facebook," Miller said, adding out-of-office email replies and voice messages should not include specific details.

Companies should establish clear guidelines about the type of information employees should be providing in their communications, Miller said.

Although little can be done about information sold over the dark web, above-board websites such as pastebin.com have procedures to take down sensitive information appearing there, Waskelis said.

Spotting Bad Mail

In terms of incoming emails, modern operating systems have much richer security controls built in, whereas older

"If you keep systems patched, upgraded and certified, you're at substantially lower risk. But also important is cyberawareness training for employees."

systems bolt on that security, making it easier to circumvent, Hushon said, "If you keep systems patched, upgraded and certified, you're at substantially lower risk. But also important is cyberawareness training for employees."

In addition, there's plenty of supplemental technology out there to check for problematic domains and other indications of BEC scams. Paterson at Digital Shadows said another basic step is creating a sender policy framework (SPF) record to check domains to verify that emails are coming from the correct emails servers, flagging those that aren't and may be malicious.

"At a lot of companies, SPF tends not to be on because it can block some third-party tools the company employees might be using," Paterson said. "It's a bit complicated to configure it to prevent that from happening, but it's something we do at Digital Shadows and it has protected us from these types of incidents."

Waskelis notes that AT&T offers services to protect organizations by filtering all inbound emails for spam and malicious links and preventing employees from connecting to known bad websites from their systems. In 2014, IBM spent more than $1 billion to acquire Trusteer, a cybersecurity firm specializing in software that can identify cyberthreats that traditional defenses may miss.

Precautions should be taken to control personal laptops or other personal devices that might be plugged into the network (Bring Your Own Device). And cyber defense experts such as CSC can analyze a company's network and systems for vulnerabilities, identify where valuable information rests in the information systems, and establish additional security perimeters around that information.

"The fortress styled cyberdefense… moats, walls and gates aren't effective in keeping people out, much less controlling them once they are inside. In most cases, we are recommending that secure enclaves be built around critical systems to add an additional layer of defense," Hushon said.

He added that sophisticated digital systems can turn a company's information network from a stadium, in which everyone can mingle, to more like a hotel, where critical systems have their own access keys and door locks.

"A lot of clients are moving toward cloud-like architecture, where hard walls are set up between rooms, so instead of having to breach application A to get access to application B, access to B has to be gained on its own through the heavily guarded front door," Hushon said.

The Last Line of Defense: Humans

Alas, no technology is perfect. As long as fraudsters see BEC scams to steal funds or valuable information outweighing the risks, they are likely to continue developing ever cleverer schemes.

Besides ever craftier BEC messages that closely replicate actual communications to a target executive, so-called zero-day attacks can deliver malware payloads undetected by most anti-malware defenses. The software may be designed to hide in a desktop computer, browser or application such as Dropbox for weeks and even months at a time before the fraudster directs it remotely toward a malicious goal. Enos said that tools to detect zero-day attacks are still so new that their success remains unclear.

So that leaves humans as the last resort. The clear solution to prevent executives from rashly rushing payments is to institute procedures that must be followed by everyone, including the CEO. Forbid one-person fund transfer decisions and require at least one other set of eyes to approve every payment request.

"We have dual controls for all transfers of money," said James Gilligan, CTP, FP&A, assistant treasurer at Great Plains Energy.

One approach might require phone confirmation with the executive requesting the payment. Procedures vary by a particular company's business needs and whether it has a centralized or decentralized treasury. Decentralized treasuries tend to be more vulnerable to BEC attempts and could therefore require central-office approval, at least for payments over an amount specified by the central office.

Best practices, according to Howard Forman, product group manager, corporate online and mobile services at PNC Bank, N.A., can range from physical sign-offs on actual paper to digital signatures, as long as the hardcopy or electronic documents pass through the correct workflow. Some companies, Forman said, route payment requests through

their enterprise resource planning (ERP) systems, and approval must be obtained from a hierarchy of individuals before treasury can push the pay button.

"There's no one-size-fits-all process. What's important is that it works for the particular business, it's repeatable, and the process is consistently followed—even by the company's executives—so that employees can easily detect requests that are outside of the company's typical payment patterns."

Essential Training

Not all payment requests are for millions of dollars to pursue acquisitions, and strictly following procedures for each request could severely burden treasury staff. For that reason, fraudulent payment requests often seek amounts below the threshold at which a company has more stringent procedures in place—an amount typically between $10,000 and $100,000, depending on the size of the company.

It is essential to train employees to recognize BEC attacks, and to offer more frequent training to those executives who are the likeliest targets, such as treasurers and CFOs.

Consequently, it is essential to train employees to recognize BEC attacks, and to offer more frequent training to those executives who are the likeliest targets, such as treasurers and CFOs. A basic step for any employee to make before clicking a link in an email is to press the "reply" button and examine the email domain for discrepancies, since fraudsters can buy nearly identical domains.

The same holds true for links in the email. Instead of immediately clicking on a questionable link, "Teach employees to cut and paste the link out of the email and into a text editor and make sure it's pointing to where it should be pointing," Williams said.

Sophisticated cybercriminals may successfully insert malware somewhere in a company's information network, or the network of a firm the company communicates with, and hijack the company's email domain. Even then, discrepancies usually appear to employees who have been trained to be aware of fraudulent attempts. Forman said one bank customer caught on to a BEC scheme requesting a large payment because the signatory usually signed his emails "Dick" but this one was signed "Richard."

Several cyberdefense providers offer services that test employees by delivering messages via email and even phone calls that are carefully crafted to persuade them to click on a link. If they miss the subtle clues and click, it subjects them to a brief training course.

Williams said companies must determine who has "keys to the kingdom" and can inadvertently provide damaging access to the company's information system.

"Make sure those users understand how sophisticated these attacks can be, so whenever they receive emails they view them with a bit of skepticism," he said.

Combatting Cyberfraud on Multiple Levels

Cybertransgressors, especially at the well-resourced APT level, have so far proven themselves to be one step ahead of their victims, and that is likely to continue while the benefits of theft continue to outweigh the risks. No defense technology will remain 100 percent effective, and given the increasing volume of detailed data available to profile targets, fraudsters will almost certainly construct scams that will catch executives off-guard at some point.

Thus, recommend cyberexperts, organizations should pursue a multi-faceted approach to defending themselves against BEC attacks. "There's no silver bullet," said Paterson. "It's got to be a combination of defenses."

Magnus Carlsson is the manager for treasury and payments at the Association for Financial Professionals (AFP). Previously, Carlsson worked as the project manager for the SEPA project at AB Volvo and was the arbitrage manager for the Arlington County Treasurer's Office, managing all arbitrage issues, debt service payments and investment management. He was with the Federal Home Loan Banks (FHLB) Office of Finance for seven years in positions of increasing responsibility and scope including credit analysis, short-term debt issuance and investor relations.

AFP® ASSOCIATION FOR FINANCIAL PROFESSIONALS

About the Association for Financial Professionals

Headquartered outside Washington, D.C., the Association for Financial Professionals (AFP) is the professional society that represents finance executives globally. AFP established and administers the Certified Treasury Professional™ and Certified Corporate FP&A Professional™ credentials, which set standards of excellence in finance. The quarterly AFP Corporate Cash Indicators® serve as a bellwether of economic growth. The AFP Annual Conference is the largest networking event for corporate finance professionals in the world.

General Inquiries	AFP@AFPonline.org
Web Site	www.AFPonline.org
Phone	301.907.2862

In the business of knowing your business

COUNT ON THE EXPERTISE YOU DESERVE.

At MUFG Union Bank, N.A., we believe a strong relationship starts with a solid understanding of your unique needs and goals.

With a world of resources—$2.5 trillion[1] in assets, over 140,000 professionals, and 350 years of experience—it's no wonder we were named the 2015 Best Global Corporate Bank by *Global Finance*.[2]

Contact us today to discuss how we can help your business thrive.

Chaz Present
Division Manager
404-464-4949
cpresent@us.mufg.jp

Christine Foley
Managing Director
312-601-3956
cfoley@us.mufg.jp

MUFG Union Bank, N.A.
A member of MUFG, a global financial group

MUFG

[1] Exchange rate of USD 1 = ¥ 120.6 (J-GAAP) as of December 30, 2015.
[2] Source: *Global Finance*, October 2015.