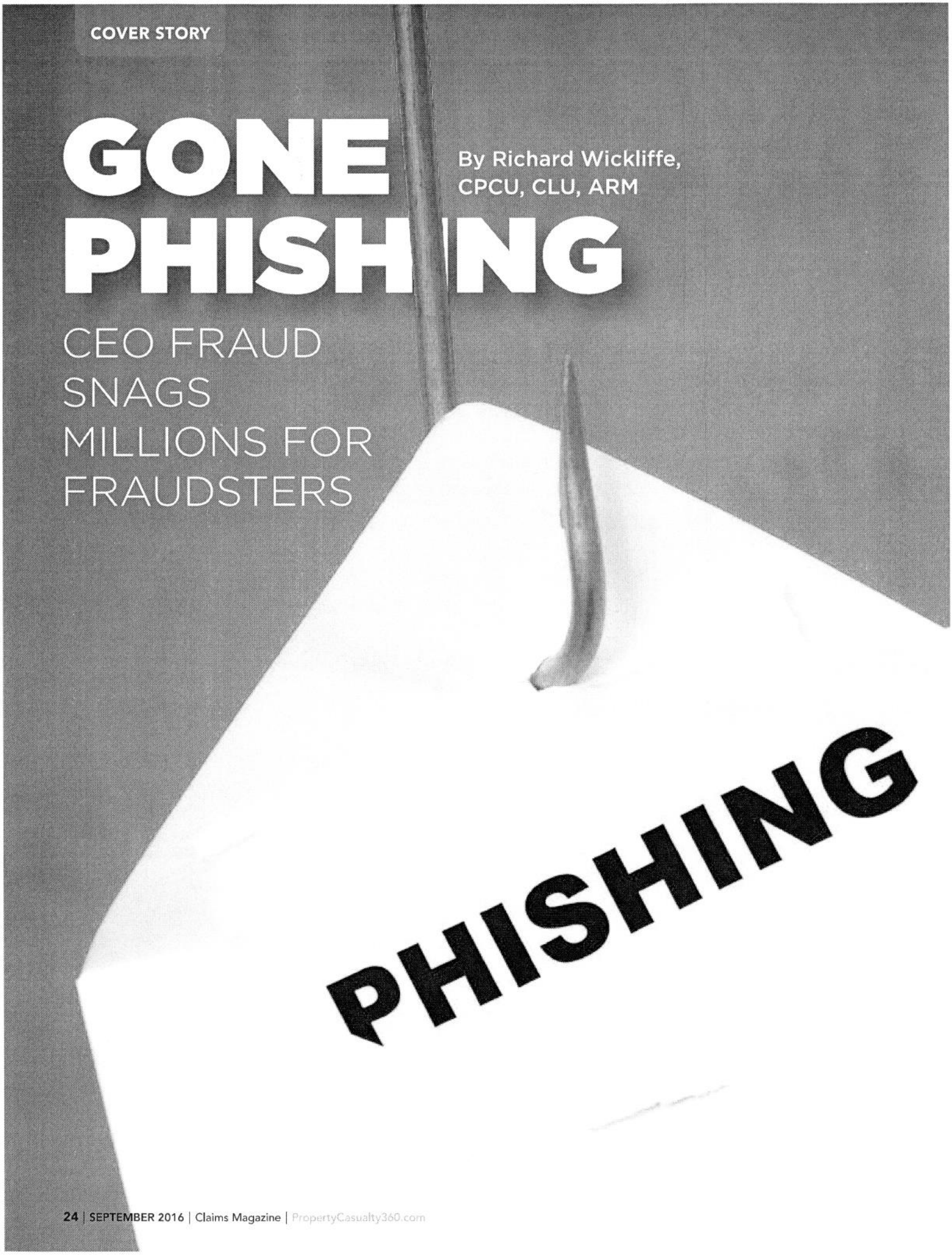
GONE PHISHING

CEO FRAUD SNAGS MILLIONS FOR FRAUDSTERS

By Richard Wickliffe, CPCU, CLU, ARM



A young man sits in a café by the Volga River in the western Ukraine. Using his laptop, he just robbed your company in the U.S. of $11 million and your employee was his accomplice.

The latest cyber fraud, according to the FBI and countless corporate victims, is known as Business Email Compromise (BEC) fraud or "CEO fraud." And employees are being conned into enabling the thefts — which creates an exclusion under many insurance policies.

CEO fraud involves phishing attacks that cleverly mimic an email from someone in management at an employee's company or an executive demanding financial transfers. Phishing for high-profile targets has even been called "whaling."

In April 2016, an FBI press release warned of these schemes to transfer funds by compromising legitimate business email accounts through social engineering and computer invasion methods.

According to the FBI, the crimes have been reported in every state across the U.S. From October 2013 through February 2016, law enforcement received reports from 17,642 victims, totaling over $2.3 billion in losses and reflecting a 270 percent increase in victims. Fraudulent transfers have been sent to 79 countries, with the majority going to China, Russia and the Ukraine.

How it's done

The intrusions are initiated by a phishing scheme in which a victim receives an email from a seemingly authentic source that contains a malicious link. Similar to other fraud trends, the scam may occur at the end of the business day or work week.

Pay requests allegedly authorized by a high-ranking individual in management are unlikely to be questioned by junior employees. Criminals create a plausible looking email, purportedly from another employee or vendor, to deceive them into transferring funds into accounts controlled by the thieves, which are usually offshore.

The thieves will conduct exhaustive research. They will exploit open-source intelligence (meaning anywhere online where an executive's business email or title can be found). They'll study what the company is working on, learn jargon and product names, and send phishing emails to get feelers in the door. Some go so far as to create phony company websites to lend credibility to their emails.

A public service announcement from the FBI explains how thieves go to great lengths to spoof a company's email or assume the identity of the CEO or a trusted vendor. They research employees who manage money and use language specific to the target company.

They will take a company's legitimate email such as "abc-company.com" and create a fraudulent phishing email that closely resembles the company's address like "abc_company.com."

The FBI warns businesses to be wary of any wire transfer requests made by email only or having a sense of urgency. Anyone who receives such a request should contact the individual by phone to verify the transfer and companies should practice multi-level verification for large transfers.

Noteworthy cases

Imagine being a shareholder of Ubiquiti Networks, reading their Q4 Fiscal 2015 Earnings Report. It admitted that cyber thieves stole $46.7 million through spoof emails purportedly from executives of their company to initiate unapproved international wire transfers.

The San Jose-based company stated the incident involved requests from an outside entity targeting their finance department. The funds were transferred to "overseas accounts held by third parties." The company disclosed to its shareholders that it may not be successful in obtaining insurance coverage for the loss.

The popular app company Snapchat was a victim of a similar scheme in February 2016. An email intruder pretended to

be their CEO, Evan Spiegel, and asked for employees' payroll information. The employee who received the email did not realize it was a con and responded with the information. The hacker then exposed the data to the outside world. Snapchat has not revealed what information was compromised or how many employees were impacted.

Why insurance might not provide coverage

The only thing conceivably worse than being a victim of CEO fraud is wondering if the company's policy will cover any portion of the loss.

Insurance alone cannot combat the threat of cyber crime. Cyber liability insurance can protect specific financial losses, however many policies have exclusions if an employee was deceived into participating in the loss. Since the funds are ostensibly wired *voluntarily*, most commercial policies won't cover the loss.

According to *The Betterley Report's* "Cyber/Privacy Insurance Market Survey," published by Betterley Risk Consultants, out of 31 leading cyber insurance carriers, only eight cover fraudulent wire transfers. Out of those eight, most have exclusions if an employee is involved in the fraud. With schemes such as CEO fraud, employees are almost always implicated whether they realize it or not.

Insurers are now taking advantage of these gaps by offering specialized coverage. Beazley Group, a syndicate of Lloyd's of London, has begun offering "Fraudulent Instruction Insurance," to cover financial losses due to "fraudulent instructions from a person purporting to be a vendor, client or authorized employee." What is *not* covered is the fraudulent transfer of anything nonfinancial, such as goods or merchandise.

Is the tide turning?

In May 2016, the United States Court of Appeals for the Eighth Circuit (Minnesota) ruled in favor of a bank that sued its insurer after it denied a claim for a fraudulent wire transfer. In State Bank of Bellingham v. BancInsure, Inc., the court upheld a ruling that losses suffered by the bank should be covered by their insurance provider. The court awarded State Bank $620,187 plus attorney's fees.

In that case, a bank employee's actions after a valid wire transfer allowed their computer to become infected. The bank's policy provided coverage for losses such as employee dishonesty and computer-system fraud. The carrier denied the claim because the loss resulted from an employee's error and not because of the theft of data. The court disagreed, noting, "The computer system's fraud was the efficient and proximate cause of loss…"

Can you lose your job due to poor security?

In May 2016, the CEO of Austrian aerospace company FACC was fired by its board after a hacker sent a fraudulent email pretending to be the CEO, stealing 42 million euros ($47 million.) An unaware employee inadvertently helped wire the funds offshore for a fictitious project.

FACC's board, whose customers include Airbus and Boeing, concluded their CEO had "severely violated his duties in relation to the fake president incident." Although an employee was fooled by a sham email, the board evidently believed it should not have been that easy.

When retailer Target suffered one of the largest cyber breaches on record in 2013, resulting in a $40 million loss, their CEO was fired after 35 years with the company. Executives are being held responsible for their cybersecurity measures or lack thereof.

Bigger than we thought?

Russian cyber security firm *Kaspersky Labs* claims a hacker gang called *Carbanak* has stolen over $1 billion since 2013 from 100 financial service businesses in more than 30 countries. If these breaches don't sound familiar, it could be because few companies wish to publicize any failures or weaknesses within their own systems.

According to a Kaspersky Lab press release, INTERPOL, Europol and authorities from numerous countries have collaborated to investigate these unparalleled cyber robberies. The *Carbenek* multinational gang includes cybercriminals from Russia, Ukraine and parts of Europe and China.

The thieves reportedly gain entry into employees' computers through spear phishing, infecting victims with the *Carbanak* malware. They were then able to navigate into the companies' internal networks, concealing their presence behind legitimate transactions. Though most crimes are targeted within Russia and Eastern Europe, new cyber gangs are modeling their techniques, according to Kaspersky.

How to combat wire fraud

By being proactive, companies can reduce the likelihood of being impacted by BEC fraud. While executives debate the minutiae of cyber insurance policies, IT and accounting departments should take steps now to lessen the risk of schemes that lead to wire fraud. When it comes to financial transfers, have policies in place for any transfers larger than a specific amount, and have multiple employees sign off on the transfers. Uninformed employees only make it easier for the thieves.

Companies should consider these factors when creating their cyber response plans:

- Cyber security awareness training is imperative.
- Businesses are being tricked by deceptive email messages into diverting funds to cyber thieves.
- Employees are the weakest link due to phishing and social engineering schemes.
- Consider multiple levels of authorizations, especially over certain dollar amounts.
- Keep all software up to date to minimize flaws for criminals to exploit.

Prevention is far less expensive than losing money to cyber thieves.

Richard Wickliffe, CPCU, ARM, CLU, (RLWickliffe@yahoo.com) is a 26-year insurance professional in leadership at one of the nation's largest insurance carriers. He enjoys writing and speaking about unique insurance and fraud trends. His articles have appeared in National Underwriter and SIU Today, in addition to published fiction novels.