How to combat fraud in an increasingly digital world

Cybersecurity and employee training are key solutions

By Phillip M. Perry

Businesses face a growing risk of financial loss from fraudulent internet transactions. The right internal operating procedures can reduce an organization's vulnerability to social engineering techniques designed to access company funds and data. When breaches do occur, cybersecurity solutions and dedicated insurance policies will mitigate the damages.

A scary hypothetical

A controller of a California business receives an email from the CEO requesting an immediate wire transfer for a vendor. The request and transaction seem routine. Unfortunately, after the money was sent, they discover no payment was owed to that vendor. Even worse, the funds were never received.

After further investigation, it is determined that the request is from a thief using an email address misleadingly similar to the targeted company's top executive. The supplied banking credentials actually belong to the crook's account in China.

The controller calls the overseas bank to see if the payment could be canceled. Fortunately, the funds had arrived on a Chinese bank holiday and couldn't be credited to the thief's account. The company was able to recover its funds.

BEC fraud rampant

While our opening story has a happy ending, most businesses targeted by so-called Business Email Compromise (BEC) fraud are not so lucky. In a recent survey from consulting firm AP Now, 11% of respondents reported losing money to BEC fraud, and only 3.2% of respondents recovered all the stolen funds.

BEC fraud is increasing rapidly as thieves have learned to cleverly disguise C-level executives' identities. "Crooks know it's very, very easy for people to miss slight changes in email addresses," said Mary S. Schaeffer, AP Now's president.

DASMA Executive Director Chris Johnson knows far too well how employees can be misled by BEC fraud. During the January 2019 Annual Meeting, several DASMA staff members were targeted.

Using a common BEC scam technique, an online criminal used the email of an executive to gain trust and request money from other staff members. In total, five employees were contacted; somewhat fortunately, only two were successfully scammed. While the financial losses were minimal, it demonstrates the potential risk of processing any financial request made via email.

Watch for suspicious alerts

There are several suspicious terms commonly used in the subject lines of fraudulent emails, including "*request, payment, transfer,* and *urgent,* among others." (trendmicro.com, "Business Email Compromise")

"We continue to receive suspicious emails regularly, and they are becoming more and more sophisticated. The key is to educate your employees to know what to watch out for and to have proper controls and processes in place," said Johnson. "We emphasize to our employees that it is better to talk directly to IT staff if there is any question whatsoever regarding the validity of an email message."

Reports from the FBI, the IRS, and other agencies show that cyber fraud poses a growing threat to businesses. While many thieves want money, others want data, such as company marketing plans or customer information for identity theft. Losing control of the latter can be especially costly.

"The extent of liability for customer data loss depends on the severity of the incident," said Diane D. Reynolds, partner at McElroy Deutsch. "Not only may a breach require notification under state and possibly federal regulations, but there are also costs involved with the ongoing need to monitor the results of the breach, cleanup of the system, and dealing with negative public relations."

No one is safe

Large companies are not the only businesses at risk. "Criminals often target smaller businesses because their protections are typically not as strong," said Schaeffer. "They are likely to have older, unsafe technology and lack the security personnel to keep software updated."

The growing digitalization of business transactions is fueling the rise of cyber fraud. A greater reliance on electronic

Editor's Note:
I have been a victim of cyber fraud twice in my life, and I'm still recovering from the trauma. The first time, I was hit with ransomware. After refusing to pay the sum requested, I lost years of work files and too many personal images to count. During the second incident, a person posing as my supervisor used business email fraud to swindle me for $600 in gift cards.

I am sharing these experiences to demonstrate that any person or company can experience cyber fraud firsthand. The information included in this article from Philip Perry will further ensure that you are not their next target.

communications during the COVID-19 pandemic is exasperating the problem.

"Flaws in firewalls and Virtual Private Networks (VPNs), as well as in videoconferencing systems, have exposed more businesses to incursions," said Robert M. Travisano, an attorney at Epstein Becker Green. Additionally, the expansion of devices on the typical employer's computer network has given cyber criminals more opportunities.

The pandemic has increased risk in another way: "More people are working at home, sharing business computers with family members," said Cybersecurity consultant Eric Jackson. "This has created some serious security breaches."

Not only can users log onto malware-infested sites they would not access at work, but family members may accidentally open email attachments that install damaging programs.

Risky payments

Wire transfers and Automated Clearing House (ACH) transactions are juicy targets for cyber thieves as the business world moves away from paper checks. "The right procedures can help spot electronic payment fraud before the money goes out the door," said Schaeffer. "That's much better than trying to recover what's been lost."

Security experts say most business fraud stems from social engineering — a thief's skillful engagement with a company employee. "Social engineering is responsible for 70% to 90% of all successful digital breaches," said Roger Grimes, a consultant at Knowbe4. "Yet the average company spends less than 5% of its cybersecurity budget to fight it."

Proper verification is key

Training employees in preventive procedures is critical. To eliminate BEC fraud, businesses should require that wire transfers be validated by a means other than email. "Validation should be done by either picking up the phone and calling the executive using a known number, or if feasible by walking over to that individual's office," said Schaeffer.

The pandemic has made verification more difficult. "Calling and verifying sounds easy in the abstract, but it can be exponentially more difficult when people work from home," said Schaeffer. "Sometimes the right person is not readily available because of their schedule."

Don't fall for the tricks!

Often, security breaches occur when targeted employees are pressured into quick action. "Thieves will often request transactions when they know people are more likely to be overworked or harried," said Schaeffer.

Beware of requests that come in late on a Friday afternoon, at the end of the month, or anytime when thieves think they can trick somebody into failing to properly verify a transaction, she added.

Implementing sound procedures can protect your business if a caller, pretending to be a customer, requests bank routing numbers to pay an invoice. "People are often only too happy to give out such information because they want to receive money," said Schaeffer.

continued on page 46

Five types of BEC scams recognized by the FBI

Source: trendmicro.com, Definition of Business Email Compromise (BEC)

1. The Bogus Invoice Scheme – Attackers pretend to be a supplier and request fund transfers for payments to an account owned by fraudsters.
2. CEO Fraud – Attackers pose as an executive or the CEO and send an email to employees requesting them to transfer money to an account they control.
3. Account Compromise – An executive or employee's email account is hacked and used to request invoice payments to vendors listed in their email contacts. Payments are then sent to fraudulent bank accounts.
4. Attorney Impersonation – Attackers pretend to be someone from a law firm supposedly in charge of crucial and confidential matters. Normally, such bogus requests are done through email or phone during the end of a business day.
5. Data Theft – Human Resources or bookkeeping employees are asked to obtain personally identifiable information or tax statements of employees and executives. Such data can be used for future attacks.

continued from page 45

"However, rather than using the provided information to wire funds into the account, the thief wires funds out." Businesses can prevent such wire fraud by requiring that account information be communicated only by designated individuals who directly dial the paying company using known telephone numbers.

"Another solution is to establish one bank account dedicated to wire transfers, and use it only for inbound transactions," said Schaeffer.

Another example of fraud to be aware of is when a thief, pretending to be a vendor, sends an email providing routing numbers for a new bank account where all future payments are to be made. The account, of course, belongs to the thief.

"This type of fraud is exploding, and I cannot caution you enough to be careful," said Schaeffer. "You need to get to the right person to verify that the request is legitimate." Again, verification should be done over a voice line using a known telephone number.

Schaeffer cautions that calling to verify changes in bank accounts or email addresses will only work if a company's records are accurate. "It's more important than ever to enter valid contact information in the master vendor file when it's first set up, and then update it regularly."

Tools to protect your ACH numbers

Thieves can also use stolen ACH numbers to steal company funds. Banks offer a number of services to stem losses. An ACH block will prohibit all ACH transactions for a specified account.

An ACH debit block prohibits only transactions initiated by payees. An ACH filter allows ACH debits only to those on a designated list of names. An ACH alert triggers a notification when an ACH debit arrives, enabling a staff member to accept or reject.

"I suggest putting ACH debit blocks on all accounts where debit activity is not needed," said Schaeffer. "Limit ACH debit activity to one or two accounts and check those accounts each day. Businesses have 48 hours' time to notify the bank of any unauthorized transaction." (Consumers enjoy a 60-day notification window.)

Damaging malware

Ransomware is a form of malware that requires targeted businesses to make costly payouts to either regain access to encrypted data or prevent the release of business information to competitors.

Measures to help reduce the chances of being hit with ransomware:

1. Train employees to handle all emails with suspicion.
2. Replace old equipment with new models.
3. Regularly update operating systems and office applications to their latest versions.

"Unpatched software is involved in 20% to 40% of all digital breaches," said Grimes.

continued on page 48

Reducing risk with cyber insurance

While no business can eliminate the risk of cyber fraud, insurance can save the day when a breach occurs. Many common commercial general liability (CGL) policies already address some areas related to digital transactions. Security experts, though, advise seeking better protection.

Determining the right coverage

"Cyber coverage in existing property polices is often limited," said Travisano. The typical cyber policy will cover money lost to cyber thieves. In the event of customer data loss, policies may cover breach notification, credit and fraud monitoring services, and the costs associated with restoring and recreating data as well as with hiring a PR firm. Especially important is coverage for business interruption.

"Statistics show that most businesses are not back to normal operations for at least one month after an attack," said Reynolds. Even the best dedicated cyber policies may have potentially costly coverage omissions.

"Insurance companies, God bless them, are really good at writing policies that are very precise and cover you for exact things," said Schaeffer. "If you haven't checked your policy closely, you may not have the coverage that you think you do."

Update your policies regularly

What seems like good coverage today may not look so attractive down the road. "As cyberattacks evolve, so will insurance," said Jessica Averitt, a partner at Baker McKenzie. "For example, a few years ago provisions related to ransomware were rare. But after some recent high-profile attacks, such coverage is more common."

Reap the benefits

Cyber policies can carry benefits that go beyond coverage categories. "The insurance agency will get you in touch with expert incident response brokers who will get you back up and running as quickly and cheaply as possible after an attack," said Grimes.

The good news is that more carriers are entering the field of cyber insurance, increasing the competition for customers and helping improve terms and premiums. With a decade or more of loss history to analyze, carriers are fine-tuning their premiums to make policies more attractive and more reasonably priced.

An important caveat

The terms of a cyber policy will be invalid if the covered business cannot illustrate compliance with a good security plan. Insurance companies are tightening the screws in this area.

"We are seeing more carriers who will not even issue policies unless a business has security controls validated by a third party," said Jackson. "And when an incident occurs, carriers will often send inspectors to investigate the insured's security posture before paying a claim."

continued from page 46

Insurance policies

The right insurance can lessen the blow of cyber fraud when a breach occurs. "Insurance can protect businesses from so-called 'first party risk' of their own losses," said Reynolds.

"Policies can also protect against losses to third parties such as customers and vendors, obviating lawsuits against the insured company." (For more details, see "Reducing risk with cyber insurance.")

Even the best insurance policy is no substitute for operating procedures that help stop cyber theft in its tracks.

"The one piece of advice I have is to be suspicious," said Schaeffer. "Make sure everyone knows that if something looks a little odd, or if someone asks for something out of the ordinary, speak up. It's better to go overboard on security than to go the other way." ■

Cyber Defense Quiz

How solid is your cybersecurity program?

Find out by taking this quiz. Score 10 points for each "yes," then total your score and check your rating at the bottom of the chart.

1. Have all personnel been trained on security protocols, including correct handling of suspicious emails?
2. Do changes in a vendor's or customer's bank account information for e-payments require verification by voice telephone call to a known number?
3. Do you require non-email validation of wire transfer or ACH requests?
4. Have you established one bank account dedicated to wire transfers and blocked such transfers on all other accounts?
5. Have you limited ACH debit activity to one designated account?
6. Have you established ACH filters, blocks, and alerts where appropriate?
7. Do you regularly update vendor master files?
8. Have you replaced hardware older than 15 years?
9. Do you regularly update software programs?
10. Have you taken out a comprehensive cyber insurance policy?

What's your score?

80 or more: Congratulations! You have gone a long way toward securing your company funds and data.

Between 60 and 80: It's time to fine tune your security procedures.

Below 60: Your business is at risk. Take action applying the suggestions provided in this story.