NEW EDITION

Whittlesey
Forward Advising™

KnowBe4
Human error. Conquered.

CEO FRAUD
Prevention Manual

> "The adage is true that the security systems have to win every time, the attacker only has to win once."
>
> — Dustin Dykes

Introduction

It has ruined the careers of many executives and loyal employees. Successful CEOs have been fired because of it. Stock prices have collapsed. IPOs and mergers have been taken off the table. Known as CEO fraud or Business Email Compromise (BEC), the FBI reports that this type of cyber crime generated more than 23,000 complaints that were responsible for losses of more than $1.7 billion in 2019 alone. Between June 2016 and July 2019, the FBI reported that the total domestic and international exposed dollar loss was over $26 billion. (ref: https://www.ic3.gov/media/2019/190910.aspx#fn1 and https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120)

Despite these statistics, cyber-risk management remains a blind spot for most C-level executives. Therefore any organization led by its CEO must quickly learn to integrate these skills and technologies into day-to-day operations – or face the consequences.

This CEO Fraud Prevention Manual provides a thorough overview of how to deal with this exponentially growing wave of preventable cyber crime. Part I explains how top executives in finance are hoodwinked, how organizations are compromised, how millions are siphoned off by criminals, and how fiduciary responsibilities play a role. Part II covers how to prevent such an attack as well as what to do if you become the latest victim. This includes checklists of the key steps.

Part I: Understanding CEO Fraud

What is CEO Fraud?

The FBI calls it Business Email Compromise (BEC) or Email Account Compromise (EAC) and defines it as "a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests. The scam is frequently carried out when a subject compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds." (ref: https://www.ic3.gov/media/2019/190910.aspx#fn1)

CEO fraud is another name for this type of scam and it usually involves tricking someone into making a large wire transfer into what turns out to be a bogus account, redirecting paycheck deposits or even requesting employees' Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms. On a few occasions, however, checks are used instead of wire transfers. Between May 2018 and July 2019, the FBI reported a 100% increase in identified global exposed losses. Most victims are in the U.S. (all 50 states), but organizations in 177 other countries have also reported incidents. While the fraudulent transfers have been sent to at least 140 countries, most end up in China and Hong Kong. Unless the fraud is spotted within 24 hours, the chances of recovery are small. (ref: https://www.ic3.gov/media/2019/190910.aspx#fn1)

Certainly, large enterprises are a lucrative target. But small businesses are just as likely to be the mark. Other than being a business that engages in wire transfers, there is no discernible pattern in terms of a focus on a particular sector or type of business. The bad guys don't discriminate.

Fortunately, organizations can learn/familiarize themselves with the methods in which these attacks are initiated.

Phishing: Phishing emails are sent to large numbers of users simultaneously in an attempt to "fish" sensitive information by posing as reputable sources—often with legitimate-looking logos attached. Banks, credit card providers, delivery firms, law enforcement, and the IRS are a few of the common ones. A phishing campaign typically shoots out emails to huge numbers of users. Most of them are sent to people who don't use that bank, for example, but by sheer weight of numbers, these emails make their way to a certain percentage of likely candidates.

Spear Phishing: This is a much more focused form of phishing. The cyber criminal has either studied up on the group or has gleaned data from social media sites to con users to help them formulate a more personalized attack. The email generally goes to one person or a small group of people who use that bank or service. Some form of personalization is included – perhaps the person's name, or the name of a client.

Executive "Whaling": Here, the bad guys target top executives and administrators, typically to siphon off money from accounts or steal confidential data. Personalization and detailed knowledge of the executive and the business are the hallmarks of this type of fraud.

Social Engineering: All of these techniques fall under the broader category of social engineering. This innocuous sounding label was originally defined as the application of sociological principles to specific social problems. But within a security context, it has come to signify the use of psychological manipulation to trick people into divulging confidential information or providing access to funds.

The art of social engineering often includes mining information from social media sites that are collecting something called Open Source Intelligence (OSINT). LinkedIn, Facebook and other venues provide a wealth of information about organizational personnel that can be used to craft attacks. This can include their contact information, connections, friends, ongoing business deals and more.

Unfortunately, these scams have a high rate of success. The Verizon 2020 Data Breach Investigations Report (DBIR) revealed that phishing unsurprisingly topped the list for top threat actions in breaches. Many of these breaches happen within two minutes of receipt, meaning that IT has little chance of catching this malicious traffic before it hits inboxes. (ref: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf)

While phishing emails may not directly lead to CEO fraud, they are the top avenue of entry for malware and spyware into the enterprise. Once inside, cyber criminals can bide their time finding the financial connections and interactions within the organization. They eventually learn enough to spring a convincing BEC attack, usually posing as an organization executive or an accounts personnel. They can sit unobserved for months while they study the key individuals, processes, procedures and protocols necessary to perform wire transfers or other financial redirection within that business environment.

The FBI identifies five main scenarios by which this scam is perpetrated:

1. Business working with a foreign supplier: This scam takes advantage of a long-standing wire-transfer relationship with a supplier, but asks for the funds to be sent to a different account.
2. Business receiving or initiating a wire transfer request: By compromising the email accounts of top executives, another employee receives a message to transfer funds somewhere, or a financial institution receives a request from the organization to send funds to another account. These requests appear genuine because they come from the correct email address.
3. Business contacts receiving fraudulent correspondence: By taking over an employee's email account and sending invoices out to organization suppliers, money is transferred to bogus accounts.
4. Executive and attorney impersonation: The fraudsters pretend to be lawyers or executives dealing with confidential and time-sensitive matters.
5. Data theft: Fraudulent e-mails request either all wage or tax statement (W-2) forms or a organization list of personally identifiable information (PII). These come from compromised and/or spoofed executive email accounts and are sent to the HR department, auditing departments or accounts.

Who is at Risk?

Such attacks are anything but rare. In fact, they are so successful that billions are being plundered through corporate accounts. Here are some examples of recent attacks:

Israeli Startup and a VC Company: Bad actors managed to compromise the email accounts of an Israeli startup company, then redirected email messages to look-alike domains for both the Venture Capital company and the startup, and walked away with $1 million in startup seed money.

This was a brilliant man-in-the-middle attack that was successful because the attackers created fake domains with an extra "s" on the end and tricked both sides into routing emails through the attackers' servers.

Two B.C. law firms: Two B.C. law firms lost almost $2 million to attackers who sent emails to the firms asking that funds transfers go to different accounts. These were done through spoofed email addresses that were either the same as the sender or only off by one letter.

Two defense contractors and a university: Two defense contractors and a university lost approximately $170,000 in three incidents where an attacker impersonated employees at a university. The attacker ordered expensive electronic measurement instruments and billed the university. It was a simple scam. They used spoofed email addresses pretending to be the university and obtained fraudulent lines of credit to easily make the purchases.

In many of the publicly disclosed cases, funds are recovered due to quick identification and reporting by employees. However, this insight might give a false impression given that the FBI states that overall losses are well into the billions. Beyond the immediate funds looted, the indirect damage caused by CEO fraud is additionally substantial. C-level executives are fired, reputations are damaged and stocks can take a hammering.

Risk or Reputation - Who is a Target?

The label of this category of cyber crime may be CEO fraud, but that doesn't mean the CEO is the only one in the criminal's crosshairs. In addition, the HR team, IT manager, C-level positions, other senior executives and anyone with finance approval is likely to be on the receiving end of one of these attacks, using the authority of the CEO as leverage.

Finance: The finance department is especially vulnerable in organizations that regularly engage in large wire transfers. All too often, sloppy internal policies only demand an email from the CEO or other senior person to initiate the transfer. Cyber criminals usually gain entry via phishing and then spend a few months doing recon and formulating a plan. They mirror the usual wire transfer authorization protocols, hijack a relevant email account and send the request to the appropriate person in finance to transmit the funds. As well as the CFO, this might be done through the identity of anyone in accounts that is authorized to transfer funds.

HR: Human Resources represents a wonderfully open highway into the modern enterprise. After all, this departmen has access to every person in the organization, manages the employee database and is in charge of recruitment. As such, a major function of HR is to open résumés from thousands of potential applicants. All the cyber criminals need to do is include spyware inside a résumé and they can surreptitiously begin their early data gathering activities. In addition, W-2 and PII scams have become more commonplace. HR receives requests from spoofed emails and ends up sending employee information such as social security numbers and employee email addresses to criminal organizations.

Executive Team: Every member of the executive team can be considered a high-value target. Many possess some kind of financial authority. If their email accounts are hacked, it generally provides cyber criminals access to all kinds of confidential information, not to mention intelligence about types of potential ongoing deals. Thus executive accounts must receive particular attention from a security perspective.

IT: The IT manager and IT personnel with authority over access controls, password management and email accounts are even further high-value targets. If their credentials can be hacked or phished, hackers gain entry to every part of the organization.

From the perspective of the individual executive, the risk of losing one's job should be enough incentive to pay attention to the potential for fraudulent email. CEOs and CFOs have lost their job over a breach. Ignorance of the techniques and surprise at the outcome are no excuse. It is up to C-level executives to inform themselves on the subject and take the necessary steps to minimize risk.

Board members, too, have a fiduciary responsibility with regard to cybersecurity risk. With the number of incidents very much on the rise, the record should reflect strong interest by the board and a specific address to risk mitigation. Steps should be taken to identify threat vectors, ascertain what information is most in need of protection, institution of preventive measures and protocols put in place in the event of a breach. It may also be prudent to bring in outside bodies to audit cybersecurity safeguards.

Board Oversight and Fiduciary Duty

Virus and malware defense has long been viewed as purely an IT responsibility. Even though some organizations appoint Chief Information Security Officers (CISO), the fact remains that information security is often viewed as a challenge that lies well below board or C-level attention.

However, the events of recent years have highlighted the danger of this viewpoint. With the FBI warning corporations that they are at risk and so many high-profile victims in the news, organizations, led by their CEO, must integrate cyber-risk management into day-to-day operations. Additionally, organizations must take reasonable measures to prevent cyber-incidents and mitigate the impact of inevitable breaches.

Many state and federal laws in the United States, Australia and other countries use the concept of acting "reasonably."

Blaming something on IT or a member of staff is no defense. CEOs are responsible for restoring normal operations after a data breach and ensuring an organization's assets and organization's reputation are both protected. Failure to do so can open the door to legal action.

Let's put it in these terms. A cyber breach could potentially cause the loss of a bid on a large contract, could compromise intellectual property (IP) and loss of revenue, to name just a few of the repercussions. These challenges place cybersecurity firmly at the top of the organizational chart, similar to all other forms of corporate risk.

"People are used to having a technology solution, [but] social engineering bypasses all technologies, including firewalls. Technology is critical, but we have to look at people and processes. Social engineering is a form of hacking that uses influence tactics." – Kevin Mitnick

Technology vs. The Human Firewall

Most efforts towards risk mitigation concentrate on technology. Certainly, antivirus, antimalware, intrusion detection/protection, firewalls, email filters, two-factor authentication and other technology solutions are vital. Similarly, appropriate backup and disaster recovery (DR) processes must be in place. For example, a 3-2-1 backup strategy (three copies of the data, on two different types of media, with one off site) is a recommended best practice along with testing of the restore function on a regular basis.

However, these technology safeguards must be supported by what is known as the human firewall – an internal staff that is educated on cyber threats that can spot a phishing email a mile away, quickly report it and won't fall prey to CEO fraud.

The way to manage this problem is new-school security awareness training. Thousands of organizations are doing this with great results. Stepping users through this training educates them against falling for social engineering attacks. Establishing a human firewall won't eliminate breaches entirely, but it will reduce them.

Part II Prevention, Resolution and Restitution

1. Prevention

Many steps must dovetail closely together as part of an effective prevention program.

Identifying High-Risk Users

High-risk users include C-level executives, HR, Accounting and IT staff. Impose more controls and safeguards in these areas. For example, on finance approvals for wire transfers, stipulate several points of authorization and a time period that has to elapse before the transfer is executed.

It is wise to conduct a search of all high-risk users to see how exposed they are. For example, LinkedIn and Facebook profiles often provide detailed personal information or even what could be considered sensitive corporate data such as the person having wire transfer authority, as well as email addresses and lists of connections.

Technical Controls

Various technical controls should be instituted to prevent the success of phishing attacks. Email filtering is the first level of this, but it is far from foolproof. Authentication measures should be stepped up. Instead of a simple username and password, which the bad guys have a good success rate of getting past, two factor authentication also requires something that only the user possesses, such as a physical token. This makes it much harder for potential intruders to gain access and steal that person's personal data or identity. Key fobs, access cards and sending a code to a registered mobile phone are some of the possible prevention methods, but we prefer the Google authentication app.

Automated password and user ID policy enforcement is another wise defense. Comprehensive access and password management can also minimize malware and ransomware outbreaks and successful email account takeovers. Review existing technical controls and take action to plug any gaps.

Policy

Every organization should set security policy, review it regularly for gaps, publish it and make sure employees follow it. It should include such things as users not opening attachments or clicking on links from an unknown source, not using USB drives on office computers, password management policy (not reusing work passwords on other sites or machines, no Post-it notes on screens as password reminders), completing specific types of security training, including training on security policy, and the many other details of employee and overall security diligence. Policy on Wi-Fi access, for example, should be reviewed. Include contractors and partners as part of this if they need wireless access when on site.

Policy should also exist on wire transfers and on the handling of confidential information. It should never be possible for a cyber criminal to hijack a corporate email account and convince someone to transfer a large sum immediately. Policy should limit such transactions to relatively small amounts. Anything beyond a predetermined threshold must require further authorizations.

Similarly, with confidential information such as IP or employee records, policy should determine a chain of approvals before such information is released.

Procedures
IT should have measures in place to block sites known to spread ransomware, keep software patches and virus signature files up to date, carry out vulnerability scanning and self-assessment using best practice frameworks such as US-CERT or SANS Institute guidelines, and conduct regular penetration tests on Wi-Fi and other networks to see just how easy it is to gain entry. These and many other security procedures will go a long way toward protecting your organization.

Procedures must also be developed to prevent CEO fraud and BEC. Wire transfer authorization is one scenario demanding careful attention. Set it up in a way that any wire transfer requires more than one authorization, as well as a confirmation beyond email. Phone, or ideally face-to-face confirmation, should be included. That way, a spoofed email attack is thwarted because confirmation is done on a different channel. If by phone, only use a pre-existing number for your contact, not one given to you in an email.

The subject of time should also be part of procedure. To guard against urgency injected by a cyber criminal into an email, standard procedure should call for a 24-hour waiting period before funds are transferred. This gives ample time for the necessary authorizations and side-checks for authenticity to be completed.

Cyber-Risk Planning
Cybersecurity has historically been treated as a technology issue. However, cyber risk must be managed at the most senior level in the same manner as other major corporate risks. The CEO must fully understand the organization's cyber risks, its plan to manage those risks, and the response plan for when the inevitable breach occurs. CEOs also must consider the risk to the organization's reputation and the legal exposure that could result from a cyber incident. CEO fraud must be part of the risk management assessment.

While this assessment is of a technical nature, it is more about organizational procedures. Executive leadership must be well-informed about the current level of risk and its potential business impact. This is rarely the case within organizations inflicted with phishing and CEO fraud. Management must know the volume of cyber incidents detected each week and of what type. Policy should be established that outlines thresholds and types of incidents that require reporting to management.

In the event of an outbreak, a plan must be in place to address identified risks. This is another weak point in many organizations, yet it is an essential element of preserving the integrity of data on the network.

Best practices and industry standards should be gathered and used to review the existing cybersecurity program. Revise the program based on a thorough evaluation. One aspect of this is regular testing of the cyber-incident response plan. Run a test of a simulated breach to see how well the organization performs. Augment the plan based on results.

Lastly, call your insurance company and go over the fine print regarding your coverage. If no cyber insurance exists, acquire it rapidly. Go over the details of cybersecurity insurance to ensure it covers the various types of data breaches and includes the various types of CEO fraud and BEC attacks.*

Training
No matter how good your prevention steps are, breaches are inevitable. But user education plays a big part in minimizing the danger. Make it a key aspect of your prevention strategy.

Start by training staff on security policy. Augment this by creating a simple handbook on the basics of security. This should include reminders never to insert USB drives from outside devices into work machines. It should also review password management, such as not reusing work passwords on other sites or machines.

**Note: Normally human error like CEO fraud is NOT covered by cybersecurity insurance.*

Phishing demands its own training and instruction, as it represents one of the biggest dangers. Let users know that hovering over email addresses and links in messages shows the actual email address or destination URL. Just because it says "Bank of America," or "IT department" with all the right logos doesn't mean it's from that source. Add further instruction not to open unknown file types, click on links, or open attachments from unknown people or entities. Coach them into a suspicious frame of mind regarding requests to send in their passwords or account details. If, for instance, educating a student body in this manner isn't feasible, put them on a separate network and severely restrict their access to sensitive data.

Security awareness training is strongly recommended. The best programs baseline click rates on phishing emails and harness user education to bring that number down. But again, don't expect 100% success. Good employee education can reduce phishing success significantly and provide valuable threat intelligence through reporting, but it won't take it down to zero. There is always someone who doesn't pay attention, is in a hurry that day, or is simply outsmarted by a clever cyber criminal. Comprehensive data security best practices must also be enforced.

Simulated Phishing
Security awareness training is best accompanied by simulated phishing. The initial simulation establishes a baseline percentage of which users are phish-prone. Continue simulated phishing attacks at least once each month, but twice is better. Once users understand that they will be tested on a regular basis and that there are repercussions for repeated fails, behavior changes. They develop a less trusting attitude and get much better at spotting a scam email. Phishing should not just be blasts to all employees with the same text. In this case, one employee spots it and leans out of the cubicle to warn the others. Instead, send different types of emails to small groups of users and randomize the content and times they are sent.

Red Flags
Security awareness training should include teaching people to watch out for red flags. In emails, for example, look for awkward wording and misspelling. Be alert to slight alterations of organization names, such as "Centriffy" instead of "Centrify" or "Tilllage" instead of "Tillage". Hackers have become very good at creating spoofed email addresses and URLs that are very close to actual corporate addresses, but only slightly different.

Another red flag is sudden urgency or time-sensitive issues. Scammers typically manufacture some rush factor or other that can manipulate reliable staff to act rapidly.

Phrases such as "code to admin expenses," "urgent wire transfer," "urgent invoice payment" and "new account information" are often used, according to the FBI. Any time an email or text message causes a strong emotional response, it should be treated with additional scrutiny. This is important because cyber criminals use emotions to cloud critical thinking.

Resolution and Restitution
Should a CEO fraud incident take place, there are immediate steps to take:

1. Contact your bank immediately
Inform them of the wire transfer in question. Give them full details of the amount, the account destination and any other pertinent details. Ask the bank if it is possible to recall the transfer. Get in touch with the cybersecurity department of the bank, brief them on the incident and ask for their intervention. They can contact their counterparts in the foreign bank to have them prevent the funds from being withdrawn or transferred elsewhere.

2. Contact your attorneys
In some cases, especially in the event of a significant loss, communications may have to be made to shareholders and stakeholders, and regulations may require reporting of the incident within a certain timeframe. Your attorneys can provide guidance on next steps, help prepare a notification statement if needed, and assist in navigating regulatory and insurance processes.

3. Contact law enforcement
In the U.S., the local FBI office is the place to start. The FBI, working with the U.S. Department of Treasury Financial Crimes Enforcement Network, may be able to return or freeze the funds.

When contacting law enforcement, identify your incident as "BEC," provide a brief description of the incident and consider providing the following financial information:

- Originating Name
- Originating Location
- Originating Bank Name
- Originating Bank Account Number
- Recipient 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

4. File a complaint

Visit the FBI's Internet Crime Complaint Center (IC3) at www.IC3.gov to file your complaint.
Victims should always file a complaint regardless of dollar loss or timing of incident at www.IC3.gov.
In addition to the financial information and the bullet points in the previous section, victims should also provide the following descriptors:

- IP and/or email address of fraudulent email
- 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 emails
- 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 emails
- Reports of any previous email phishing activity

5. Brief the board and senior management

Call an emergency meeting to brief the board and senior management on the incident, steps taken, and further actions to be carried out.

6. Conduct IT forensics

Have IT investigate the breach to find the attack vector. If an executive's email has been compromised, take immediate action to recover control of that account, such as changing the password and checking any account recovery email addresses for changes made by the attackers. But don't stop there. It's likely that the organization has been further infiltrated and other accounts have been compromised. Have them run the complete range of detection technologies to find any and all malware that may be lurking to strike again.

7. Contact your insurance company

Once gone, in most cases, funds cannot be recovered. This is especially true if the victim does not move quickly. Therefore, it is necessary to contact your insurance company to find out if you are covered for the attack. While many organizations have taken out cyber insurance, not all are covered in the event of CEO fraud.

This is a grey area in insurance and many refuse to pay up. Many people who have reported CEO fraud to their insurer find that this type of incident is not covered. Despite the presence of a specific cyber insurance policy, the unfortunate fact is that no hardware or software was hacked. It was the human that was hacked instead.

Insurance companies draw a distinction between financial instruments and email fraud. Financial instruments can be defined as monetary contracts between parties, such as cash (currency), evidence of an ownership interest in an entity (share), or a contractual right to receive or deliver cash (bond). Many companies are covered in the event of a fraudulent financial instrument.

However, CEO fraud is often categorized differently. It is regarded by some insurance firms as being purely an email fraud and not a financial instrument fraud. In other words, it is being regarded in many cases as a matter of internal negligence or email impersonation as opposed to being a financial instrument matter. That said, there are dozens of carriers in the market providing up to $300 million in limits. Coverage extensions have developed to include both the third-party liability and first-party cost and expenses associated with a data breach or cyber attack.

Even if the insurance company is not willing to pay immediately, they may have resources available. These resources may include security specialists on retainer, who can help perform forensics and ensure the attackers are out of the system.

8. Bring in outside security specialists

If the organization was breached, it should highlight deficiencies in existing technology safeguards. These will prove harder for IT to spot. So, bring in outside help to detect any area of intrusion that IT may have missed. The goal is to eliminate any and all malware that may be buried in existing systems. The bad guys are inside. The organization isn't safe until the attack vector is isolated and all traces of the attack have been eradicated. This is no easy task.

Remember that your insurance company may have recommended groups or resources available that could be covered or offered with a discount through them. So, be sure to ask your insurer before hiring a security specialist.

9. Isolate security policy violations

For such an incident to happen, there is likely to be evidence of violations of existing policy. Conduct an internal investigation to cover such violations as well as to eliminate any possibility of collusion with the criminals. Take the appropriate disciplinary action.

10. Draw up a plan to remedy security deficiencies

Once the immediate consequences of the attack have been addressed and full data has been gathered about the attack, draw up a plan that encompasses adding technology and staff training to prevent the same kind of incident from repeating. As a vital part of this, be sure to beef up staff awareness training.

Conclusion

There is no substitute for preparation when it comes to dealing with cyber criminals and the many flavors of CEO fraud. The CEO Fraud Prevention Checklist given here will guide you through necessary steps to take to educate the organization against this type of incident.

While these steps will greatly reduce the likelihood of an incursion, all it takes is one gullible or inattentive user to let the bad guys inside. In those cases where CEO fraud is being perpetrated, the CEO Fraud Response Checklist applies.

In the case of both checklists, security awareness training plays an essential role in creating a human firewall around your organization. Only when users are fully aware of the many facets of phishing will they be capable of withstanding even the most sophisticated attempts at CEO fraud.

KnowBe4

CEO Fraud Response Checklist

- [ ] 1. Contact your bank
  - Give them full details of the amount of wire transfer, the account destination and other details.
  - Recall the transfer if possible.
  - Have them contact the foreign bank to freeze the funds.

- [ ] 2. Contact your attorneys
  - Inform them of the facts.

- [ ] 3. Contact law enforcement
  - Identify your incident as "BEC," provide a brief description, provide complete financial information.

- [ ] 4. File a complaint
  - Visit the FBI's Internet Crime Complaint Center (IC3) at www.IC3.gov to file your complaint with full details of the crime.

- [ ] 5. Brief the board and senior management
  - Call an emergency meeting to brief the board and senior management on the incident, steps taken and further actions to be carried out.

- [ ] 6. Conduct IT forensics
  - Have IT investigate the breach to find the attack vector, recover control of hacked email accounts, and find any malware remaining anywhere within the network.

- [ ] 7. Contact your insurance company
  - Find out if you are covered for the attack and if they have resources to help resolve it.

- [ ] 8. Bring in outside security specialists
  - Bring in outside help to detect areas of intrusion that IT may have missed. All traces of the attack and all traces of malware must be eradicated.

- [ ] 9. Isolate security policy violations
  - Investigate violations as well as the possibility of collusion with criminals. Take the appropriate disciplinary action.

- [ ] 10. Draw up a plan to remedy security deficiencies
  - Beef up security technology and procedures.
  - Bolster staff security training, especially security awareness training.

KnowBe4

CEO Fraud Prevention Checklist

☐ 1. Identify your high-risk users such as HR, executives, IT managers, accounts and financial personnel.

- Review each for what is posted on social media, organization websites and in the public domain, especially job duties/descriptions, hierarchical information and out-of-office details.
- Identify email addresses that may be searchable in the public domain.

☐ 2. Institute technical controls.

- Email filtering
- Two-factor authentication
- Automated password and user ID policy enforcement
- Patching/updating of all IT and security systems
- Manage your network boundaries
- Manage access and permission levels
- Adopt whitelists or blacklists for external traffic

☐ 3. Policy

- Institute wire transfer policy, such as:
  - Multiple points of authorization (not just the CEO and one other person)
  - Out of band verification – for example, email and in-person
  - Digital Signatures: Both entities on each side of a transaction should utilize digital signatures
  - Time delays for all wire transfer over a certain amount

☐ 4. Institute policy concerning access to and release of financial information, IP, customer records and employee records.

☐ 5. Procedures

- Enforce mandatory studying of security policy for all staff.
- Establish how executive leadership is to be informed about cyber threats and their resolution.
- Establish a schedule for the testing of the cyber-incident response plan.
- Register as many organization domains that are slightly different than the actual organization domain, aka "look-alike domains," as possible.
- Implement Domain Spoof Protection.
- Create intrusion detection system rules that flag emails with extensions that are similar to company email.
- Utilize the Domain Doppelganger.

☐ 6. Cyber-risk planning

- Develop a comprehensive cyber-incident response plan.
- Consider taking out comprehensive cybersecurity insurance that covers data breaches and CEO fraud.
- Include cyber risk in existing risk management and governance processes.
- Understand what information you need to protect: identify the corporate "crown jewels."
    - How to store the information
    - Who has access
    - How to protect it

☐ 7. Training

- Train users on the basics of cyber and email security.
- Train users on how to identify and deal with phishing attacks with new-school security awareness training.
- Frequently phish your users to keep awareness up.
- Implement a reporting system for suspected phishing emails such as the PhishAlert Button.
- Continue security training regularly to keep it fresh in users' minds.

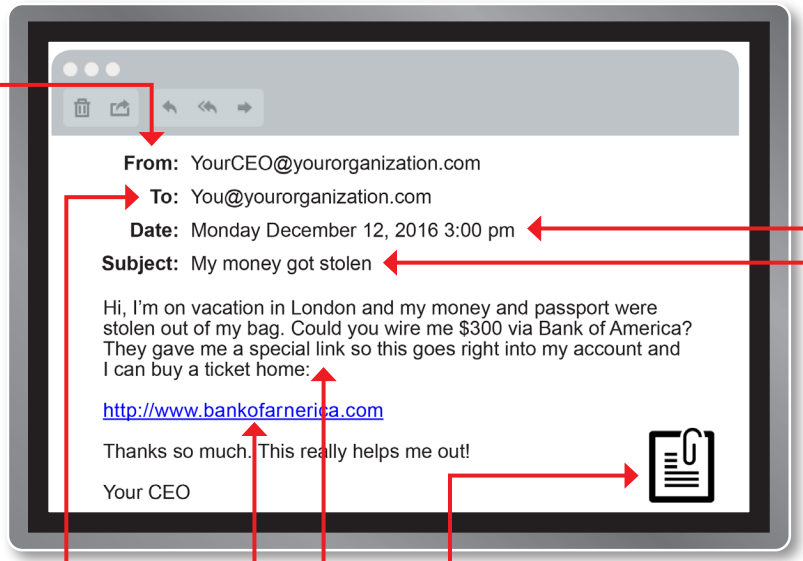
☐ 8. Red flags

- Watch out for fraudulent or phishing emails bearing the following red flags, such as urgency, spoofed email addresses, and demands for wire transfers.

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

Mark R. Torello, CPA, CFE, CISA, CRISC, CITP
Partner-in-Charge, Technology

860.524.4433
mtorello@WAdvising.com

Whittlesey
Forward Advising™

Headquarters
280 Trumbull Street, 24th Floor
Hartford, CT 06103
860.522.3111

One Hamden Center
2319 Whitney Avenue, Suite 2A
Hamden, CT 06518
203.397.2525

14 Bobala Road, 3rd floor
Holyoke, MA 01040
413.536.3970

WAdvising.com

KnowBe4
Human error. Conquered.