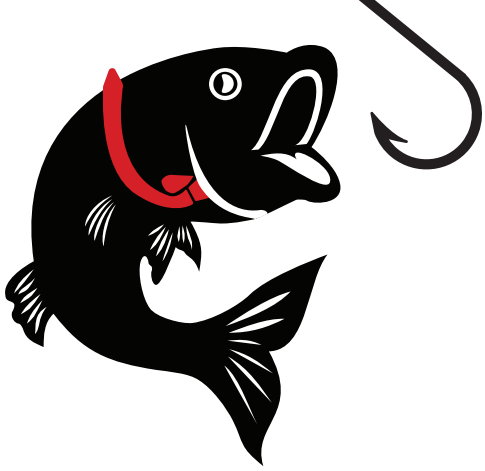
exclusive content from

simpleplanit

CEO FRAUD
PREVENTION MANUAL



WHAT TO EXPECT

Introduction

Part I: Understanding CEO Fraud

- What is CEO Fraud?
- Who Is at Risk?
- Risk or Reputation - Who Is a Target?
- Board Oversight and Fiduciary Duty
- Technology vs. The Human Firewall

Part II Prevention, Resolution, and Restitution

- Prevention
- Identifying High-Risk Users
- Technical Controls
- Policy
- Procedures
- Cyber-Risk Planning
- Training
- Simulated Phishing
- Red Flags
- Resolution and Restitution

Conclusion

INTRODUCTION

It's ruined the careers of many executives and loyal employees. Successful CEOs get fired because of it. Stock prices have collapsed. IPOs and mergers get taken off the table. Known as CEO fraud or the Business Email Compromise (BEC), the FBI reports that this type of cybercrime has victimized more than 22,000 organizations worldwide and is responsible for losses of more than $3 billion.

Despite these statistics, cyber-risk management remains a blind spot for most C-level executives. Any company, 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 cybercrime. Part I explains how top executives in Finance get hoodwinked, how companies get compromised, how millions are siphoned off by criminals, and fiduciary responsibilities. Part II covers how to prevent such an attack as well as what to do if you become the latest victim.

Part I: Understanding CEO Fraud

What is CEO Fraud?

The FBI calls it Business Email Compromise and defines BEC as "a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds."

CEO fraud is another name for this scam, and it usually involves tricking someone into making a large wire transfer into what turns out to be a bogus account. On a few occasions, however, checks are used instead of wire transfers. In the 18 months following January 2015, the FBI reported a 1,300% rise in identified exposed losses. The fraudulent transfers have been sent to 79 countries, but most end up in China and Hong Kong. Unless the fraud is spotted within 24 hours, the chances of recovery are small. Only 4% of the funds are ever retrieved.

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 regarding a focus on a particular sector or type of business. The bad guys don't discriminate.

What is known, though, is 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 to people who don't use that bank, for example, but by sheer weight of numbers, these emails arrive at a certain percentage of likely candidates.

Spear Phishing: This is a much more focused form of phishing. The cybercriminal has either studied up on the group or has gleaned data from social media sites to con users. The email 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 originally meant 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 might include mining information from social media sites. LinkedIn, Facebook and other venues provide a wealth of information about organizational personnel. This can include their contact information, connections, friends, ongoing business deals, and more.

Unfortunately, these scams have a high rate of success. The Verizon 2016 Data Breach Investigations Report revealed a shocking 30% of recipients open phishing messages and 12% click on attachments. Many of these breaches happen within two minutes of receipt. That means IT has little chance of catching this malicious traffic before it hits inboxes.

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, cybercriminals can bide their time casing out the financial connections and interactions within the company. They eventually learn enough to spring a convincing BEC attack, usually posing as a company executive or accounts personnel. They can sit unobserved for months while they study the key individuals and protocols necessary to perform wire transfers within that business environment.

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

- 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.
- 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 company to send funds to another account. These requests appear genuine as they come from the correct email address.
- Business contacts receiving fraudulent correspondence: By taking over an employee's email account and sending invoices out to company suppliers, money is transferred to bogus accounts.
- Executive and attorney impersonation: The fraudsters pretend to be lawyers or executives dealing with confidential and time-sensitive matters.
- Data theft: Fraudulent e-mails request either all wage or tax statement (W-2) forms or a company list of personally identifiable information (PII). These come from compromised and/or spoofed executive email accounts and are sent to the HR department, accounts, or auditing departments.

Who Is at Risk?

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

Ubiquiti Networks, $46.7 million: This Silicon Valley computer networking company had employee emails impersonated and money transferred to overseas accounts held by third parties. The company recouped about $15 million.

The City of EL PASO, Texas: El Paso lost $3.1 million intended for a streetcar project to a person pretending to be a legitimate vendor. The city made two payments before discovering the scam. The city recovered half of the money.

Xoom: This Internet money-transfer service lost $30.8 million via employee impersonation and fraudulent requests to the finance department. The CFO resigned.

SS&C Technologies Holdings: A lawsuit by Tillage Commodities Fund alleges that financial services software firm SS&C fell for an email scam that led to Chinese hackers stealing $5.9 million. Staffers inadvertently aided the criminals by helping them fix the transfer orders so the money could be transferred. The scam emails added an extra "L" to Tillage as in Tilllage and contained unusual syntax and grammatical errors. The lawsuit seeks $10 million in damages, plus punitive damages and legal fees. A spoofed email, claiming to come from the CEO, requested that accounting transfer money to a foreign account for a fake acquisition. Although the company recovered some of the funds, the CEO lost his job.

Leoni AG: This cable manufacturer lost $44 million to a CEO fraud attack using emails crafted to appear like legitimate payment requests from the head office in Germany, asking for the money to be sent from a subsidiary in Romania. The CFO of the Romanian operation was the victim of the scam. She was taken in by the realistic looking emails and by the fact that the scammers had extensive knowledge about the internal procedures for approving and processing transfers at Leoni. This indicates that they had penetrated the network earlier, probably through phishing emails and had been snooping for months.

Mattel: The toy manufacturer Mattel transferred $3 million to an account in China after receiving a spoofed email supposedly from the CEO. Fortunately, the finance executive who transferred the money bumped into her boss a short time later and mentioned the deal. As little time had elapsed, the bank in China still had the funds and returned them to Mattel.

Pomeroy Investment Corp: Not so lucky was this firm in Troy, Michigan after it transferred almost $500,000 to a Hong Kong bank. This followed the email account of a company executive being hacked. The error was noticed eight days after it took place, and the money was long gone.

Unnamed U.S. company: Nearly $100 million was transmitted by multiple wire transfers after receiving spoofed emails that claimed to be from a legitimate vendor. The bank flagged the transfers and managed to recover $74 million. The rest was laundered through accounts in Cyprus, Latvia, Hungary, Estonia, Lithuania, Slovakia, and Hong Kong.

In many of the publicly disclosed cases, funds are recovered. But this may give a false impression. The FBI cites a recovery rate of 4%, and the overall losses in the billions. But beyond the immediate funds looted, the damage caused by CEO fraud is 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 cybercrime may be CEO fraud. But that doesn't mean the CEO is the only one in the criminal's crosshairs. The HR team, IT manager, C-level and other senior executives, and anyone with finance approval are likely to be on the receiving end of one of these attacks.

Finance: The finance department is especially vulnerable in companies that regularly engage in large wire transfers. All too often, sloppy internal policies only demand an email from the CEO or another senior person to initiate the transfer. Cybercriminals usually gain entry via phishing, spend a few months doing recon and formulate 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 anyone in accounts that are authorized to transfer funds.

HR: Human Resources represents a wonderfully open highway into the modern enterprise. After all, it has access to every person in the organization, manages the employee database, and is in charge of recruitment. As such, a major function is to open résumés from thousands of potential applicants. All the cybercriminals need to do is include spyware inside a résumé, and they can surreptitiously begin their early data gathering activities. In addition, W2 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 financial authority. If their email accounts get hacked, it provides cybercriminals access to all kinds of confidential information, not to mention intelligence on the type of deals that may be ongoing. 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 further high-value targets. If their credentials can be hacked, they gain entry to every part of the Organization.

Board Oversight and Fiduciary Duty

Virus and malware defense has long been viewed as a purely IT problem. 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 dangers of this viewpoint. A cyber breach could cause the loss of a bid on a large contract, and could compromise intellectual property (IP) and loss of revenue (to name just a few). That places cybersecurity firmly at the top of the organizational chart, similar to all other forms of corporate risk.

Organizations, **led by their CEO**, must integrate cyber risk management into day-to-day operations. Additionally, companies must take reasonable measures to prevent cyber-incidents and mitigate the impact of inevitable breaches. 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 that company assets and the company's reputation are protected.

Technology vs. The Human Firewall

Most efforts towards risk mitigation concentrate on technology. Certainly, antivirus, anti-malware, 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 can spot a phishing email a mile away, and won't fall prey to CEO fraud.

Regardless of how well the defense perimeter is designed, the bad guys will always find a way in. They know that employees are the weakest link in any IT system. The Verizon 2016 Data Breach Investigations Report (DBIR) found human error to be the weakest link based on a study of 100,000 security incidents and 2,260 confirmed data breaches across 82 countries. Thus, cybercriminals continue to rely on phishing and other tricks from the social engineering playbook.

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 proofs them up against falling for social engineering attacks. Establishing a human firewall won't eliminate breaches entirely, but it will reduce them.

> "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

Part II Prevention, Resolution, and Restitution

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 list of connections.

Technical Controls

Various technical controls should be instituted to prevent the success of phishing attacks. Email filtering is the first level, 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 has on them 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 methods, but we prefer the Google authentication app.

Automated password and user ID policy enforcement is another wise defense. Comprehensive access and password management also can minimize malware and ransomware outbreaks. 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 WiFi 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 the handling of confidential information. It should never be possible for a cybercriminal 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 that 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, keeping 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 conducting regular penetration tests on WiFi and other networks to see just how easy it is to gain entry.

Procedures must also be developed to prevent CEO fraud. Wire transfer authorization is one scenario demanding careful attention. Set it up 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 as 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 cybercriminal 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

The CEO must fully understand the company's cyber risks, its plan to manage those risks, and the response plan when the inevitable breach occurs. CEOs also must consider the risk to the company'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 as to 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 up 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 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 some rapidly. Go over the details of cyber security insurance to ensure it covers the various types of data breaches and includes the various types of CEO fraud.

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 to never 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 cyber security insurance.** As it represents one of the biggest dangers, phishing demands its own training and instruction. 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 to not open unknown file types, click on links, and 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 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, 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 very clever cybercriminal.

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 a 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. One employee might spot it and 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 wordings and misspelling. Be alert for slight alterations of company names such as Centriffy instead of Centrify or Tilllage instead of Tillage. Hackers have gotten 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.

Resolution and Restitution

Should a CEO fraud incident take place, these are the 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 put 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 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:

3. 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 and, in addition to the financial information, 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

4. 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.

5. Conduct IT forensics

Have IT investigate the breach to find the attack vector. If an executive's email has been hacked, take immediate action to recover control of that account such as changing the password. But don't stop there, the likelihood is that the organization has been further infiltrated and other accounts have been compromised. Have them run the gamut of detection technologies to find any and all malware that may be lurking to strike again.

6. Bring in outside security specialists

If the organization was breached, it highlights 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.

7. Contact your insurance company

FBI data shows that less than 4% of CEO fraud funds are recovered. 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.

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.

CEO fraud is often categorized differently; regarded by some insurance firms as being purely an email fraud and not a financial instrument fraud. In other words, it is 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. 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.

8. Isolate security policy violations

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

9. Draw up a plan to remedy security deficiencies

When 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. Be sure to beef up staff awareness training as a vital part of this.

CONCLUSION

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