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

□ 8. Contact your insurance company
- Find out if you are covered for the attack

□ 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

PREFERRED
WORLD CLASS IT • DRIVING BUSINESS GROWTH

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, company websites and in the public domain, especially job duties/descriptions, hierarchal information, and out of office details
- Identify email addresses that may be searchable in the public domain

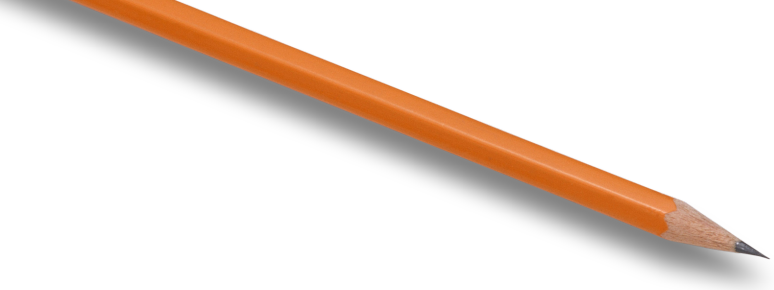
□ 2. Institute technical controls

- 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 – email and in person, for example
  - 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

- Make staff study security policy and enforce this
- 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 as possible company domains that are slightly different than the actual company domain
- Implement Domain Spoof Protection
- Create intrusion detection system rules that flag emails with extensions that are similar to company email

□ 6. Cyber-risk planning

- Develop a comprehensive cyber incident response plan
- Consider taking out comprehensive cyber security 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 top of mind

□ 8. Red flags

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