O'HAGAN MEYER

RAPID RESPONSE & INCIDENT MANAGEMENT

Best Practices for Preventing & Responding to Business E-Mail Compromises

Business e-mail compromises are the most common type of cyber-attack. These incidents can be relatively benign or can result in widespread disruption with devastating impacts. Understanding how to prevent business e-mail compromises, and then respond when such an event occurs, is important with the amount of data that is communicated electronically through e-mail.

Employee Training: Your employees are your first line of defense to protect your business from cyber-attacks. At least annual cybersecurity training should be required for every member of your workforce. Completion of this training should be documented. Supplemental training and as-needed updates regarding specific cyber threats should be provided. Some examples that employees should look for are, changed e-mail address during an e-mail thread, slight changes to an e-mail address and improper grammar in the body of the e-mail. Regular training will not only help your workforce identify common threats but ensure that your workforce appreciates the importance of cyber security.

Enable Multi-Factor Authentication: Your organization should use multi-factor authentication for all e-mail accounts. Doing so requires that a threat actor cannot access an account without being in possession of something besides the account password, such as a phone, key, fob, or authentication app.

Monitor, Limit, or Prevent Inbox Rules: Threat actors commonly use inbox rules to carry out common e-mail scams and disguise their unauthorized presence in an e-mail account. At the very least, you should monitor the establishment of inbox rules to prevent a threat actor from establishing an unauthorized rule.

Identify E-Mails that Originate Outside of your Organization: Using a banner to identify e-mails that originate outside of your organization is a simple way to help your workforce identify e-mails that require additional scrutiny. A warning not to click on links or open attachments in e-mails originating from outside the organization, unless the attachment or link is expected, is also a recommended practice.

Employee Reporting: As part of your employee training, your workforce should understand how to properly report a cybersecurity incident. Oftentimes, the damage done by cyber attacks is increased because employees are either unaware, or afraid, to report a cyber incident. An environment where employees can recognize potential dangers, and feel comfortable reporting a suspected incident, is crucial to preventing and limiting damage from cyber-attacks.

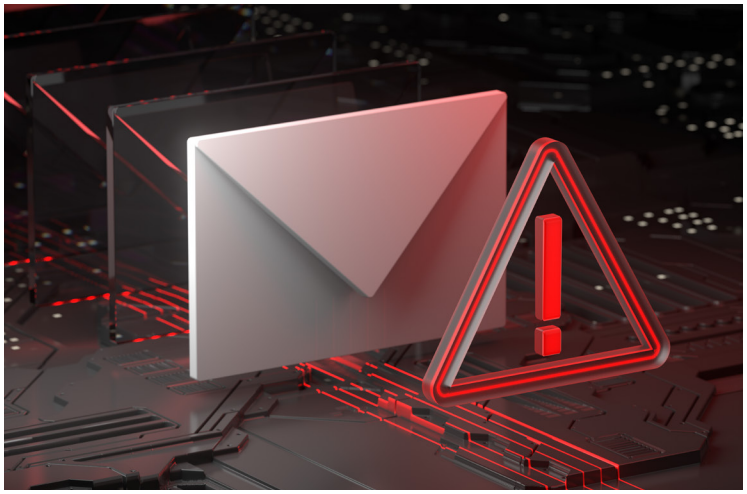
O'HAGAN MEYER

RAPID RESPONSE & INCIDENT MANAGEMENT

Incident Response Plan: Every company should have a written incident response plan addressing various types of cybersecurity incidents. Considering that business e-mail compromises are one of the most common types of cyber-attack, your IRP should specifically address how you will respond if you discovery a business e-mail compromise. The IRP should also identify the various members of the IRP team, along with their contact information, so that they can be contacted immediately upon discovery of the attack.

Sign-Out and Change Password: Upon discovery of a potential business e-mail compromise, the affected user should change their password and sign out of their account on **all devices** (laptop, phone, tablet, etc.). This action will stop the unauthorized access to the account.

Notify your Insurance Carrier: A business e-mail compromise is likely a reportable incident under your cyber insurance policy and your insurance carrier should be notified as soon as possible to ensure that all notification requirements are satisfied. Once reported, your insurance carrier will assist you by identifying the appropriate vendors (forensics, legal, notification, etc.) to respond to this incident. The best practice is to have already identified, and created relationships with, vendors that have been pre-approved by your insurance carrier that can be contacted immediately upon discovery of an incident.



Notify Impacted Individuals and Businesses: The investigation of the business e-mail compromise may indicate that information for individuals and businesses was compromised. This compromise may trigger notification requirements under applicable laws or may necessitate notification to limit potential liability exposure. These decisions should be made in consultation with counsel.

O'HAGAN MEYER

ATTORNEYS ▲ ADVISORS