HAND ARENDALL
LLC ▪ LAWYERS

CYBERSECURITY
Alert

Breach Response

An employee in the human resources department receives an e-mail purportedly from the chief financial officer of the company complaining that she has not received certain payroll information necessary for an audit of the company. The e-mail states that the audit must be completed by the following day and demands that the employee send the payroll information immediately. The employee dutifully complies.

The secretary to a company executive receives an e-mail purportedly from the company's attorney requesting certain confidential and proprietary information. The company is in the middle of a massive lawsuit, so the secretary assumes the information is needed for the case. The secretary immediately sends the requested information.

A spear phishing attack occurs when an e-mail, appearing to come from a known or trusted source, is sent to induce a targeted individual to reveal confidential information. The above examples illustrate the sophistication of spear phishing attacks. The creators of the spear phishing or spoofing e-mails have researched an organization through websites, social media, and public records, and have identified specific individuals to target. The spear phishing attacks use realistic requests from seemingly legitimate senders to induce the target to respond. The attackers often include deadlines to generate urgency in the request. Spear phishing attacks are occurring on a daily basis in epidemic proportions.

Spear phishing is just one of many tactics used by criminals to breach cybersecurity. The best way to guard against a cyber breach is to implement cybersecurity training for all personnel, maintain firewalls, spam filters, and antivirus software, and institute policies and procedures regarding internet use, passwords, e-mail communications, and social media activities. See HA's First Cybersecurity Client Alert: *Is your company's cybersecurity at risk?* Finally, a plan must be in place to respond if a breach occurs.

If you experience a cybersecurity breach, the following steps may help guide the management of the breach:

1. **Contain the breach.** If an attack is ongoing, action must be taken immediately to contain or isolate the attack and implement patches and repairs. The breach must be contained as soon as possible to minimize the scope and damage. If your IT professionals need technical assistance (or you do not have IT professionals) contact us as soon as a breach is discovered. We have relationships with trained IT professionals that may be able to provide technical assistance with containing a breach.

2. **Identify the scope of the breach.** What information, systems, programs, users, data, or devices were affected? Corrective action cannot begin until the breach is contained and the scope of the breach is known.

3. **Identify a point person.** Every company or organization should identify one person internally to notify if a breach or potential breach is discovered. This person should be an IT professional, risk officer, manager, or executive that works for the company or organization. Every person involved in day-to-day operations should know who to contact and how to contact that person twenty-four hours a day in the event a breach is discovered. The point person should understand these steps for managing the breach.

This alert was prepared by Hand Arendall's Cybersecurity Practice Group. For further information or assistance, please contact any member of the practice group below.

George M. Walker
Practice Group Chair
gwalker@handarendall.com
251-694-6296

Practice Group Members:

Roger L. Bates
Joseph L. Cowan
Kelly Thrasher Fox
Christopher M. Gill
C. Dennis Hughes
Sarah Outlaw McLaughlin
J. Burruss Riis
Christopher S. Williams

4. **Contact legal counsel.** Substantial liability can result from a data breach. Complex litigation, regulatory penalties, criminal fines, and even prosecution can result from a cybersecurity breach. A breach can also do irreparable harm to public image, employee morale, consumer loyalty, and the value of a business. Legal counsel should be consulted immediately when a breach is discovered to begin navigating the business and legal fallout. Important decisions with significant legal repercussions will need to be made within hours or days of the breach, including possible disclosure of the breach, investigation into the cause of the breach, execution of employment decisions resulting from the breach, cooperation with external agencies (including regulatory and insurance) and preparation of defenses for future claims. Counsel also should assist in the below steps.

5. **Preserve the evidence.** A forensic investigation of the breach should occur immediately. Documents and information concerning the breach should be preserved including system and intrusion detection logs. Through counsel, an interview of witnesses or employees that were involved with the breach should occur immediately. Only legal counsel and authorized personnel should be involved in the investigation to maintain confidentiality and certain legal privileges.

6. **Notify authorities and insurance representatives.** Depending on the circumstances, federal, state, and/or local authorities may need to be notified of the breach. There are many federal agencies that can assist in the response and identification of responsible criminal parties. Legal counsel should be involved in notification to protect the interests of the business or organization and mitigate exposure. Insurance representatives may need to be put on notice of the breach in accordance with insurance policies. Note: Many commercial general liability policies do not provide coverage for a cyber breach, so you should investigate whether cyber liability coverage is appropriate.

7. **Develop a response plan.** Having a general response plan is important. However, the appropriate response to a breach must be evaluated on a case by case basis. Responses can range from doing nothing to implementing widespread institutional change and making early financial restitution to potential victims. Legal counsel should be consulted in the implementation of a response as the response could trigger future legal consequences and may be used against the company in a future lawsuit.

8. **Implement the response plan.** Action may need to be taken immediately to minimize exposure and mitigate damages.

9. **Disclosure.** Depending on the circumstances, there are several federal or state laws that may require notification of the breach to the affected parties and/or governmental agencies. While most states require some form of disclosure, the laws vary by state, industry, and scope, each with different requirements for the timing, manner, and detail of the disclosure. A breach in some states may not require any disclosure. Disclosure of a breach may also lead to public relations, business, and political fallout, so the disclosure should be carefully crafted with advice of counsel.

10. **Learn from past mistakes.** After the breach, you can implement policies, training, and procedures to avoid the circumstances that led to the breach. Unfortunately, the importance of training, cyber policies, and a response plan is often not realized until after a breach occurs. In those situations, learn from past mistakes and develop and implement cyber policies, training, and procedures to guard against the next threat.

If you have questions about a cyber breach, please contact Christopher S. Williams at (251) 694-6233 or another member of Hand Arendall's Cybersecurity Practice Group.