HAND ARENDALL LLC ▪ LAWYERS

WilkinsMiller Information Technologie

Partners for Environmental Progress Presentation

PROTECTION, DETECTION, AND REMEDIATION OF CYBERSECURITY BREACHES

Thursday July 20, 2017

Example 1- Spear phishing:

Suzy works as the HR and Payroll Director for XYZ Bank. Suzy received an e-mail from Josh, the bank's chief financial officer, asking for certain payroll and tax information for the past year. The e-mail from Josh states that the information is necessary for an ongoing audit and the information must be sent immediately. The e-mail states that the request is urgent. Suzy thinks the e-mail is odd because she was not aware of an ongoing audit and Josh typically calls her to make similar requests. Because the request is urgent, Suzy immediately replies to the e-mail and sends payroll and tax information for over 100 employees.

Example 2- Ransomware:

ABC Chemical Company has an industrial manufacturing and production facility that is fully automated. The automation drives down payroll costs and also avoids problems that the Company previously experienced caused by human error. The facility still employs 100 workers to supervise, inspect, and perform quality assurance checks at the facility. In addition to being fully automated, the Company keeps electronic records of its production figures, inspection and QA logs, customer purchase information, and financial data. One day, ABC Chemical Company's computers are encrypted with malicious software from an unknown foreign actor, with a demand for payment in bitcoin to unlock the computers. ABC Chemical Company has not backed up its data in weeks, and is unable to continue its manufacturing and production process without getting its automated equipment operational. ABC Chemical Company pays the bitcoin ransom, only to learn that the malicious software actually deleted data so it cannot be restored, causing ABC Chemical Company to lose manufacturing and production capability for several weeks, along with losing several purchase orders from customers.

Example 3- Data loss by mistake

Lawyerly Lawyers Law Firm has over 1,000 active clients. The Law Firm [just to be clear, this is not a story about Hand Arendall] outsourced its IT Department, which is being handled by an outside vendor. To cut costs, the Law Firm also outsourced its server and data back-up responsibilities to a separate outside vendor. The Law Firm has a server on site where all of the client's files, data, and confidential information is stored and a back-up server with the outside vendor responsible for backing up the information daily. One day, the back-up server experienced a technical glitch which caused it to stop backing up the Law Firm's data. The IT Department was unaware of the problem, as the vendor responsible for maintaining the daily backup of data had the responsibility to monitor the back-up server. Unfortunately, the vendor responsible for monitoring the back-up was in the middle of a personnel shortage and did not detect the problem with the back-up server. Approximately a month later, during regular maintenance on the main server, the IT Department accidentally deleted several weeks of data. The IT Department was concerned, but believed everything would be okay because the back-up server was in place, and the IT Department thought the data could be restored from the daily back-up server. It then discovered the back-up server had been down for over a month. The Law Firm lost all client file information, including documents, correspondence, notes, memos, and business documents during the month when the back-up was down.

PROTECTION, DETECTION, AND REMEDIATION OF CYBERSECURITY BREACHES

I. PROTECTION

a. Policies and Best Practices
b. Training
c. Response Plan
d. Redundancies

II. DETECTION

a. Reports
b. Audits
c. Testing
d. Managed services

III. REMEDIATION

a. Identification of breach and scope
b. Containment of breach
c. Implement response plan
d. Investigation into cause of breach
e. Assess defenses and potential legal impact/future liability
f. Notification to government, insurance, outside help
g. Take action to avoid in the future
h. Disclosure to affected customers
i. Corrective action to minimize impact on affected customers

10 Cybersecurity Questions for Every Company:

1. Does your company have an internal point person that every single employee or contractor knows to contact at the first sign of cybersecurity problems or a breach?

2. If your company has an internal point person, does that person know what to do in the event of a breach and who to contact immediately?

3. Does your company have legal counsel (either in-house or outside) that can assist in the investigation and containment of the breach, advise on employment decisions, disclosure requirements, and defense of potential claims arising from the breach?

4. Does your company have policies, procedures, and training in place to protect against a breach, detect and minimize a breach, and respond to a breach such that the company can defend its practices against a claim of negligence or negligent training or supervision?

5. Does your company specifically have cyber liability insurance?

6. Does your company have a specific backup policy and how many backups do you have?

7. Does your company test backups? (file restores or full disaster recovery)

8. Does your company have a firewall that did not come from your internet provider?

9. Does your company have any type of internal cyber security training?

10. Does your company have encryption on devices?

Chris Williams
(251) 694-6233
cwilliams@handarendall.com

Andy Odle
(251) 410-6731
aodle@wilkinsmiller.com