Kroll

SANS Data Breach Summit
Table Top Exercise Scenarios

Michael Quinn

Lucie Hayward

Matt Bromiley

September 25, 2017

Scenario 1: Network Breach

Initial Facts

On a Saturday afternoon, Special Agent Bob Smith from the Chicago FBI calls your General Counsel stating that your organization's network may have been compromised.

Agent Smith states that he doesn't have any other information at this time, but would attempt to gather more and relay it back to your General Counsel.

Scenario 1: Network Breach

Inject #1

Special Agent Smith calls back and lets General Counsel know that he has acquired more information. Data traced back to your organization has appeared in an investigation of a hacker.

This data is highly confidential and proprietary, and was removed from the company sometime between March 2017 and July 2017. This is all Smith is allowed to tell you.

Scenario 1: Network Breach

Inject #2

An initial internal investigation reveals that a hacker may have phished the credentials of a user and then escalated their privileges to that of an admin. With admin credentials, sensitive data could be accessed.

Small Group Exercise

Answer the Following

- Who is in charge of the investigation?
- Who is part of the Incident Response team?
- What documents/evidence do you use to guide you?
- What role does each group provide? IT, HR, Legal, Finance, Communications, etc.?
- Do you hire outside support?
- What are you looking for – what would help you confirm a breach of your “crown jewels”?

Scenario 1: Network Breach

Inject #3

A third party investigation has confirmed that your data was taken. The incident has not yet been disclosed to clients or the public. Brian Krebs calls your Public Relations Department and asks for a statement.

Scenario 2: Ransomware

Initial Facts

An employee calls the help desk stating that her computer rebooted and is now displaying a message that says her personal files are now encrypted and that she has 4 days, 23 hours and 20 minutes to pay a ransom of 1 bitcoin in order to obtain the decryption key.

Scenario 2: Ransomware

Inject #1

7 Additional employees have called the help desk stating they can no longer access files and shared folder. They are receiving the same ransomware message.

Scenario 2: Ransomware

Inject #2

Twenty five infected computers have been pulled from the network.

Scenario 2: Ransomware

Inject #3

News that your company has been the victim of a cryptolocker ransomware attack begins to spread on social media. Moments later your Public Relations team is contacted by a local newspaper to confirm these reports.

Questions?