Kroll | A Division of DUFF & PHELPS

Incident Response Workshop

Michael Quinn & Lucie Hayward

August 20, 2018

Goal of a Table Top Exercise

- To test the readiness of the Organization to respond to cyber incidents
- Key Objectives:
  - Identify gaps in the current Incident Response Plan
  - Strengthen Communication between stakeholders
  - Familiarize all participants with key definitions and decision making criteria.
  - Enable participants to adapt this IRP to the dynamic nature of cyber incidents

Overview of Exercise

- Walk through of a incident response scenario
  - You will be provided with an initial set of facts for discussion.
  - Following the initial set of facts, additional information will be provided for discussion.

Learning Objectives

- Understand the roles for the participants on an Incident Response Team.
- Understand what defines an incident and how to identify when an incident has occurred, as well as who can formally declare an incident.
- Understand when and how to escalate an incident.
- Understand and articulate Attorney/Client privilege.
- Understand and recognize when an incident can be closed.
- Understand how to conduct Lessons Learned following an incident, and how to apply those lessons.

Learning Objectives

- Understand the role of Human Resources when responding to an incident.
- Understand and demonstrate Lead Tracking
- Understand the importance of employee awareness of the IRP.
- Understand and apply forensic considerations when responding to an incident.
- Understand the role for the Insurance Liaison
- Understand when a third party firm should be engaged to conduct forensics or assist with the investigation.

Scenario Background

- You work for a global organization (“SANS International”) that has offices around the world.
- Your company’s name is very recognizable and you have a positive reputation.
- Your business involves providing time sensitive services to clients.
- You hold a significant amount of PII that belongs to your clients.

Scenario Begins: Friday, August 17, 2018, 10:30 EDT

The service desk receives phone calls from several employees in the New York sales office, stating that your CRM, Phoenix, is running really slowly.

The service desk cannot resolve the issue, so the tickets are escalated to the application team, who finds a process running named “xmrig” that seems to be using a high percentage of CPU cycles and is located in the C:\temp directory.

Inject 1: Monday, August 20, 2018, 8:00 am

At 8 am on Monday, August 20, an employee in your New York office reports for work and finds the following displayed on her computer:

"Your client database has been collected and your data has been encrypted with a private and unique key generated for this computer. This means that you will not be able to access your files until they are decrypted. The client database and private key are stored in our servers and the only way to ensure we destroy your client data and to receive your key to decrypt your files is making a $900,000 payment in bitcoin.

Send the payment to 12t9YDPguweZ9NymGW519p7aA8ISJr6smW

Contact us at pwnd@protonmail[dot]com"

Inject 2: Monday, August 20, 2018, 9:30 EDT

By 9:30 AM the same day, the US based Service Desk is overwhelmed with calls from employees, some of whom cannot log on, while others are receiving the ransomware message.

While fielding the calls, the Service Desk discovers they also have lost access to network applications and shares.

While they are dealing with the overwhelming number of phone calls, the lines go dead.

Team Work!

Take the next ten minutes and work with your table to come up with a high level investigative plan, including:

- Who is on the IR Team
- Who is in charge
- What are your immediate next steps
- How to keep the ransomware from spreading
- How to get team members back up and running

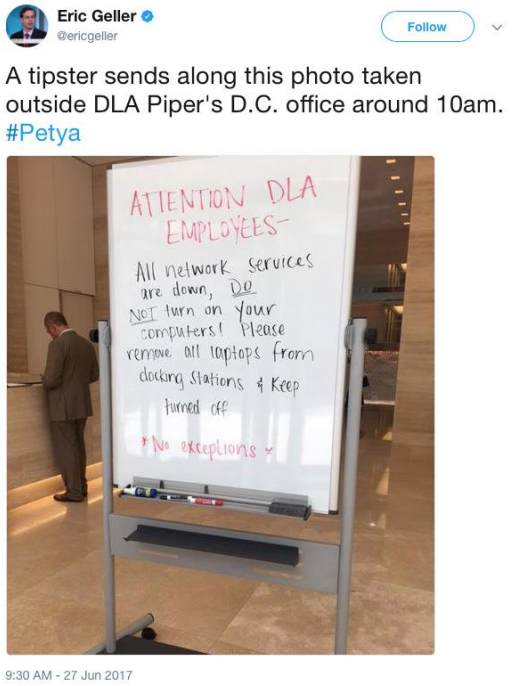
Report Back

What is your plan?

Inject 3: Monday, August 20, 11:30 am

Your public relations team has identified the trending hashtag #SANSInternationalDown on Twitter.

A review of the hashtag shows images of your office in London with a whiteboard advising employees to keep laptops removed from docking stations and powered down.



Kroll | A Division of DUFF & PHELPS

Inject 4: Monday, September 24, 12:30 pm

Employees are receiving calls from clients wanting information as to what exactly is going on. Employees are desperate to get work done to meet deadlines. The media is reaching out in various forms, phone calls, email, Twitter, etc asking for updates on the “cyber attack at SANS International.”