RSA Conference 2016

Learning Labs

Cyber-Alarm 2016

Post-Conference Summary

RSA Advanced Cyber Defense Practice, Asia Pacific and Japan

– Stephen McCombie, Paul Nankervis and Narelle Wakely

Cyber-Alarm 2016

Learning Lab

This session aimed to engage participants in a realistic role play of a major corporate breach from a number of perspectives. It began with the CERT/SOC triaging events which lead to the identification of a breach. That required investigation and analysis using specialist forensic resources.

The SOC Manager needed to report to executive management on the developing incident. Corporate affairs then briefed the media. After that the CIO appeared before the board, and in the wash up the CEO gave evidence before US Congress.

These role-plays aimed to provide a 360-degree view of the challenges of dealing with a major cyber security incident.

Scenario Summary

An advanced adversary has launched an email-based campaign against our organization, Glenshiel International Corporation (GIC).

A GIC sales employee is discovered to have received and opened an email attachment containing a weaponized (Flash) Excel document. As a result his computer is now compromised and is beaconing to a remote web-site.

Investigations reveal that other employees have also received similar emails, and that company data may have already been uploaded.

While our analysis continues there are reports that GIC private data has been found on the web, and information about this has leaked to the media.

Participant Roles

As employees of Glenshiel International Corporation (GIC) we were tasked with investigating and responding to this incident.

In the first part of the role-play we investigated the unfolding incident and found out more about the attack at a technical level.

In the second part we had to manage the incident and communicate with authorities about what had happened. As in any incident it was important to communicate and convey the right messages to each

of the parties who needed to be informed. In this case we had four role-plays where participants acted as:

- The SOC manager briefing the CIO
- Our CIO called before the board
- A corporate spokesperson fronting the media
- The CEO appearing before Congress

Each of these role-plays involved providing a briefing about what had happened, followed by a question and answer session. Teams at each table worked together to help role-play participants analyze the data and to produce the briefing.

Role-Play Objectives

The role-play is designed to show the challenges of managing major cyber security incidents, and the need to balance the requirement for communications. It demonstrated:

- The pressure of situations where media and other parties are finding out information at the same time as it is being investigated
- That communications need to occur even when the available information is incomplete
- Different groups require different communication strategies
- The importance of regular exercises in preparing for and understanding major events
- The importance of identifying and engaging with stakeholders ahead of time
- Communication strategies and incident processes should be in place before a major incident occurs

Audience Comments

During the wash up at the end of the exercise participants provided a number of comments. Some of these were:

- Security incidents and data breaches need a formal plan in place, otherwise you are on the run and just jump into the technical.
- It's not just an IT problem; you need to work with the Business and plan ahead of time.
- Parallels real life.
- The incident quickly spins out of control which I didn't like.
- Use a 3rd party to manage media messages.
- Have your organization go through this exercise!
- Get to know your general counsel. Exercises like this will help to do this.
- Excellent format, lots involved! RASCI this out with your teams.
- OMG!