Zachary Chandler

Date: 2/23/2020

Discussion Board 1:

A security framework will need to communicate our willingness to give up Security for the convenience and interoperability that networking with an outside organization will give us. I think that most if not all organizations should follow the Incident response life cycle from the NIST Security Incident Handling Guide: Preparation – Detection & Analysis – Containment, Eradication & Recovery – Post-Incident Activity.

We are only as strong as our weakest link, and this is very true when it comes to companies, we work with intimately but don't have a hand in how they operate their security. As we open ourselves up to automation and interconnecting computers our risk of exposure increases. Specifically using tools like an Extranet to increase the communication and collaboration between our company and outside parties bring new risk and new capabilities.

The outside entities that an organization works with will vary and be more specific to the type of services the business is providing. The most common being government, vendors, third party business partners, financial institutions and employee unions. While most if not all business will work with the Federal Government, companies that support federal departments will have significantly more interaction with them. And their requirement to communicate with the Federal Government will come with stronger requirements then a business to business. Business will need to consider how their post incident communications will be interpreted and used by the affected population.

Incidents like the Equifax breech needed to be immediate. The sooner people were made aware of the credit breech the quicker people could work to secure their potentially exposed banking information. In contrast security incidents that are more sensitive like military and Federal law enforcement will need to be more tightly controlled with information being released to the public at a controlled pace.

Finally, when we are working with outside entities about our security incidents, we should consider the relevancy, impact and need to know in regard to outside entities like vendors, third party business partners, financial institutions and employee unions. If we make a press release for every script kitty or Nmap scan on our system, our partners will ignore us when we have a real incident to communicate.