Exercise 6

CSCI - C437 | *Brandon Young*

1

In OPSEC the difference between threats and vulnerabilities is nearly identical to what we have already learned in this book. A threat is a person or party that might attempt to access our data for some reason. This could be a competitor or a internal person trying to gain elevated access. The vulnerability is a flaw or path in the system to breach security. It is a practical problem that could be exploited, even if it is not at the moment. Only once we have both the threat and a vulnerability do we have a threat to our system.

2

For my company, the critical information is going to come in three areas. We must keep all government required information safe, as well as sales information, and most importantly engineering and product information. This would include CAD files as well as designs for in-house machinery and parts lists. This information would be considered core to the operation of my company.

Threats would include our competitors, as well as parties interested in our projects and customers. Our competitors may seek to steal or copy product design and engineernig research. In addition, because of our work with the government as well as many other manufacturers, parties interested in manipulating customers by gathering information on our designs would also be a threat.

As for vulnerabilities, our backend security is relatively lacking in certain areas. We lack a clear plan for certain core data and how to handle a disaster if one were to happen. Another vulnerability could be door policy. While the company has encouraged employees to scrutinize tailgaters, this does not always work, and many times people simply walk into the building, no questions asked. This would pose a vulnerability for physically gathering engineering samples or information that ought otherwise to be kept secret. Another vulnerability would be phishing attacks. While we are stepping up our email filtering significantly and we do have antimalware that blocks malicious links, we have still been continually hit with phishing attempts, and many users are not aware of the risks or fall into the ploy of the attackers.

One of the risks we have is phishing attacks. While we are stepping up our email filtering significantly and we do have antimalware that blocks malicious links, we have still been continually hit with phishing attempts, and many users are not aware of the risks or fall into the ploy of the attackers, causing website blocking to occur. The parties seeking to influence the government or another customer could be another risk, though I do not know of any such attemps happening.

When we apply countermeasures there is often good communication as to the requirements of these new procedures. This allows those who pay attention to remain informed of the actions they need to take in order to keep the company information secure. We are implementing better email protections as well as continuing to improve our information security in our backend. This includes better programming and core service APIs.