Chad Ballay

CIS411-342N

Week Four

1. **How would you gather the IT asset information?**

There can not be an assumption that this would be a single instance effort. Assets themselves will change over time in addition to the insertion and deletion from Dalton, Walton, & Carlton’s company ecosystem. A precondition for the work to begin would be the confirmation of an existing CMDB/ITAM solution or the selection/installation of a CMDB/ITAM solution. (Spector) No work can begin until that requirement is satisfied.

The next step is identifying the intake flows for asset acquisitions. Hardware purchase, software purchases, vendor agreements, etc… As these processes are enumerated, I would work to incorporate the IT asset input into the CMDB/ITAM as being a non-negotiable additional step going forward. In a parallel track, if a Disaster Recovery plan already exists then the assets in there would begin to be cataloged. In an third parallel track, job duties would align individuals and their job role. Starting from the smallest units larger than an individual, interviews would be conducted to identify appropriate templates to be created. As employees input the assets, they are responsible for tagging and validation would be done. Once these systems are in place and are stable, the intangible or larger asset classes will have to be systematically addressed. This would probably have to be a series of one-off projects to capture them and develop the specific process changes for keep the data accurate. (Kostadinov)

As to classifying the assets and the specific data about each asset. Standardization would be the ideal end state. The NIST Specification for asset identification gives a very good starting point for how to classify everything into a taxonomy. (Technology) The majority of items could be classified using existing accounting processes or just using the hypothetical filing of an insurance claim to drive what is the minimum information needed. The idea is to first focus on the census, then quantifiable characteristics, then by using industry standards, then by insurance claim requirements, then by business disaster recovery needs, and finally by business stakeholder ownership. Each step in that path becomes more swayed by subjective value and thus more time consuming to ensure accuracy.

1. **What are the assets that you would assess? Create a prioritized asset list based on criticality or functionality. (Feel free to make assumptions based on the case.)**

I would classify items across several dimension to identify urgency. This isn’t a list of specific items, more so a triaging process. Asset lifecycles and values shift and change so it’s a moving target. I do think applying this would yield a punch list of computers, real estate, office equipment, intellectual property, HR systems, etc…

* Physical vs intangible items – Value appreciation for physical goods is easier so able to have a higher ROI on effort.
* Static valuation vs dynamic valuation – The more stable the valuation the more durable the information will be.
* Asset Lifecycle – The earlier in the lifecycle of an asset the longer the duration the data will be utilized.
* Proximity to Business Continuity – If the asset is enumerated in Disaster Recovery documents and other mission critical plans then it should receive higher priority. This category gets veto power

1. **How would you collect threat information?**

Tactfully and discreetly…. (Glib but a needed call out. There is a fine line between being vigilant and being panicked. A workplace culture can be stifled by a fear and mistrust. Since no bell can be unrung attention must be given to the emotional impact of this effort.)

I would adopt a threat taxonomy like ENISA or one of the other standards. (European Union Agency For Cybersecurity) As threats are classified, playbooks can be created to standardize the collection process and then automate the response where possible. This is a reactive mode that will not handle every situation or scale quickly. The addition of actively researching adjacent group attacks would be the next step. Adjacent group being some grouping that includes one or more features of this business and other entities. Break-ins in the neighborhood being a physical adjacent group. Midsize architectural firms being an industry adjacent group. The final step is the most emotionally satisfying but least consistent in ROI, interviews with employees. Employees are more likely to know the boundaries of where the checks and balances fail. The weak points in the layers of defense. The risk is either installing a culture of fear or being wasteful of employee man hours.

1. **Identify and describe at least three threats to the IT infrastructure.**
   1. **What are the threat agents associated with the threats?**
   2. **Are these threats natural, accidental, or deliberate threats?**
   3. **Describe each threat's impact and likelihood.**

Destruction due to environmental disaster. Tornado, fire, flood, earthquake, solar flare, etc…. This grouping limits itself to weather or natural events in origin. Human elements can compound or mitigate the impact but the underlying genesis is a region, specific act of god level event. The impact for this class of threat are two fold. The first is that without adequate preparation the response grows to be beyond this business’s ability to respond. The second is that these events occur with enough regularity that you can predict over a large time window that they will occur. (Tornado might not hit every year, but historical forecast can reasonably predict one would occur every XXX number of years for the area.)

Outage of externally sourced service. Fiber cut, shipping delay, electrical blackout, cloud provider crashes, etc…. These are usually accidental but can be deliberate attacks. The attack may not be targeted at your business but the downstream or proximity position from the intended victim may happen. They happen infrequently as a specific instance but in aggregate are always occurring to some degree. Supply chain theory can do much to mitigate as can redundancy and resiliency design principles. But neither can eliminate.

Violation of Legal Compliance. Change of laws without awareness, failure to disclose, intentional violation for fraud, etc…These are manmade disasters that are generally unintentional due to lack of resources to adequately accomplish the task of compliance. A smaller subset is the intentional breech of legal obligations. This subset is usually due to a perception that the resultant ends are justified by the low likelihood of notice or enforcement. A robust process of roles, responsibilities, monitoring, and auditing can reduce the likelihood. This is the primary result of process implementation. At a negligible level the display of intent to comply can mitigate the severity of impact of being found out of compliance but it is not enough to offset the risk.

# Works Cited

European Union Agency For Cybersecurity. *https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view*. n.d.

Kostadinov, Dimitar. *https://resources.infosecinstitute.com/information-and-asset-classification/#gref*. n.d.

Spector, Jaime. *https://www.sunviewsoftware.com/blog/cmdb-versus-asset-management-whats-the-difference*. n.d.

Technology, National Institue of Standards and. *https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7693.pdf*. n.d.