Chad Ballay

Week 2 Project Checkin – Outline

Overarching goal will be to use the NIST SP 800-30 framework. It’s in use at my workplace and seems as good as any boilerplate approach. Downside is this is a learn as I go since the silo I’m in at work only has me only loosely interacting with the security folks. If you can give me a thumbs up/thumbs down on this goal it would help me to focus and commit.

References for Risk Assessments goal.

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

<https://www.cybersaint.io/blog/risk-assessment-tips-based-on-nist-800-30>

<https://www.isaca.org/bookstore/cybersecurity-resources/wcsnistf> (Still trying to arrange access.)

<https://www.cybok.org/media/downloads/Risk_Management__Governance_issue_1.0.pdf>

1. Purpose & Scope definition – Hypothetical audience may need to be bootstrapped in.
   1. Goal of undertaking this assessment
   2. Use of NIST SP 800-30
   3. Establish charter statements.
2. General Company Background – Provided due to context for rest of report.
   1. Overview of history
   2. Links to timeline events
   3. List of corporate officers
   4. Overall industry recap for context
3. Branch [1-6] – Break down each site into individual section and then use 7 domains upon each section.
   1. Location specific overview with relevant info to risk assessment
   2. User Domain
   3. Workstation Domain
   4. Lan Domain
   5. Lan-Wan Domain
   6. Wan Domain
   7. Remote Access Domain
   8. System/Application Domain
4. Identified Risks – This will need some guardrails. Giant asteroids are risks but I don’t think they should be listed here. Where to draw the line?
   1. Global
      1. Classified into 7 domains structure
         1. Seems to be a lot of outdated hardware
         2. Robust patching needs to be done.
         3. Best practices are not being implemented enterprise wide.
   2. Individual location [1-7]
      1. Classified into 7 domains structure
5. Proposed Solution
   1. Technical Solutions – Easiest to enumerate
   2. Process Solution – Description of solution or at least the shape of the hole that needs to be addressed.
   3. Mitigations – Can’t fix everything so how do we compartmentalize it?
6. References and Appendixes
   1. Document Dictionary
   2. Reference material