Section 1: Week 1: Analyzing Potential Risks

Nate Bachmeier

TIM-7030: Managing Risk, Security, and Privacy

June 7, 2020

North Central University

# Analyzing Potential Risks

1. Introduction
   1. ~~What is security risk assessment~~
   2. ~~Explain and defend importance~~
   3. What is risk program
   4. ~~What are the benefits of incorporating this strategy into corp strategy~~
2. What primary threats are
   1. Current
      1. Discuss collusion
      2. Discuss MAC collision
      3. Server compromise
   2. Impact
   3. How security must address these issues
3. Regulatory requirements
4. Taxonomy of risk
   1. Define concept of taxonomy and importance
   2. Develop a table and relation diagram
5. Requirements to initiate risk assessment and management
   1. Process flowchart
   2. Explanation

* MAC address conflicts that need to be resolved between telecommunications and network appliances (routers, switches, firewalls, servers, etc...)
* Security warnings coming from the proxy and email servers
* Constant firewall alerts classified as high
* Employee collusion in certain processes that can result in a significant financial loss to the organization
* Inconsistencies in data transmissions
* Attacks detected from external international sources caused by multiple critical servers that have been compromised due to vulnerabilities in the operating system,
  + where the presence of additional services,
  + opened ports,
  + additional dynamic link libraries (DLLs),
  + additional files and scripts added to the system partitions, and
  + critical data missing from the server issues were detected