Planning Risk Mitigation Throughout an Organization

Branden Barnes

CYSE 495: Intro to Cyber Risk Management

Professor Demirel

November 5, 2023

Abstract

Planning risk mitigation throughout an organization begins with identifying assets, threats, and vulnerabilities. When starting mitigation techniques, business operations must be sought out to identify environmental processes allowing protective measures to focus on addressing possible risks linked to the critical areas of business. Key focus should include protecting critical business operations and functions and ensuring compliance within applicable laws and guidelines.

First Steps of Risk Mitigation

Asset identification determines relatively how valuable to the organization an asset is if it could suddenly become damaged, offline, or lost (e.g., high, medium, low). When assets are identified, and risk impact is calculated then assessments can occur. Assessments of database servers provoke evaluating loss of confidentiality, loss of integrity, and loss of availability. Basically, how sensitive is the data? Is the authenticity of the data intact? Is the data available for restoration? For each asset, a threat assessment, vulnerability assessment, and exploit assessment are done. When assessments conclude, controls for risk mitigation should be evaluated. For example, NIST SP 800-53 supplies detailed documentation of controls. Evaluating these controls should be based on a cost-benefit analysis (CBA).

Risk Management Scope

The scope of risk management defines areas of concern, covering elements that an organization can influence and those it cannot. The primary aspects include Critical Business Operations, the Business Impact Analysis (BIA), Maximum Acceptable Outage (MAO), Customer Service Delivery, the Service Level Agreement (SLA), and Maximum Acceptable Downtime (MAD).

Mission-Critical

Tying back into maintaining valuable assets, mission-critical systems such as critical business functions (CBFs) and critical success factors (CSFs) are vital to an operation. For example, without reliable internet access your server availability diminishes resulting in a failed web application transaction. Missing Payment Card Industry Data Security Standard (PCI DSS) compliance wields the potential for liability issues and fines occurring from failure to properly process credit card transactions.

Legal Compliances

1. Health Insurance Portability and Accountability Act (HIPAA, enacted 1996). Health data protection framework. For one of the most sensitive subjects, severe penalties can ensue (imprisonment, fines). Securities include the safeguard of data physically and digitally allowing for proper training of employees and allowing for best data handling practices for financial protection.
2. Sarbanes-Oxley Act (SOX, enacted 2002). Securities and Exchange Commission framework. Act requires a heightened level of accuracy regarding the validity of financial information within a business including mandatory audits that leave the CEO and CFO liable to scandals.
3. Federal Information Security Management Act (FISMA, enacted 2002). Applies to U.S. federal agencies. Compliance includes authorization of baseline IT systems within the organization.
4. Family Educational Rights and Privacy Act (FERPA, enacted 1974). Applicable to educational institutions that receive funding from the government's Department of Education. Involve student records integrity and accord to authorized parent/student profile upon request.
5. Children's Internet Protection Act (CIPA, enacted 2000). Compliance entails the identification and filtration of offensive content based on local standard in schools or Libraries recipient to U.S. E-Rate funding.
6. Payment Card Industry Data Security Standard (PCI DSS, enacted 2004). Standard of compliance for organizations using payment card transactions. Framework built upon six principles; build

and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an information security policy.

Key Findings

If I were to open a small business, after identifying my assets I will create a cost-benefit analysis allowing me to evaluate my inventory and prioritize risk. My mission-critical system defined in CBF will be the web servers allowing me to process credit card payment transactions. If systems were to go down, completing the business impact analysis should locate a cost of maximum acceptable outage integrated with BIA showing my loss in profit from customers inability to buy goods. Failover clusters may be applied to MAOs to mitigate downtime delay. Using PCI DSS protects my stored data and provides a framework for best practices improving budget and operations.