Final Exam

Marcus Sowers

Department of Cybersecurity, Old Dominion University

CYSE495: Introduction To Cyber Risk Management

Dr Professor Demirel

April 26, 2024

Introduction

Mitigation and risk assessments are very important and much needed components of successful organizational management. Effective mitigation and risk assessment can ensure a higher percentage for a successful business or company. This can involve identifying and mitigating risks that could potentially impact future reputation, financial stability, and even business sales and operations. Risk assessment is a process that is used to identify potential threats while analyzing the damage that could happen if a threat were to occur. Risk Mitigation on the other hand is creating and developing different strategies to reduce or disrupt the potential threats. In this paper it will explain and discuss the importance and process of formulating a Business Impact Analysis, a Business Continuity Plan, a Disaster Recovery Plan, and a Computer Incident Response Team Plan while highlighting how these strategies can assist an organization in mitigating potential risks and ensuring operational resilience.

Business Impact Analysis

The first process that will be discussed in this paper is a Business Impact Analysis. Business impact analysis is the foundation of risk assessment as it provides a structured approach to locate and identify critical business functions and create solutions on successful recoveries. The business impact analysis predicts the consequences of potential threats and disruptions and gathers needed information to form the best recovery plan and strategies. This particular process involves several key steps which include identifying critical business functions, prioritizing functions, assessing the potential impact, and determining recovery time and recovery point objectives. Identifying critical business functions involves developing a list of the most important business operations and understanding their functionality and importance. The critical functions are the ones whose disruption or failure would significantly hurt the business or company tremendously and the recovery process would be unpleasantly difficult. If the impact of the disruption or threat impacts sales or dissatisfaction from customers, then this would definitely be considered a critical business function. Another key step in business impact analysis is assessing impact, which is just identifying the impact the disruption would cause. This following assessment can include many factors like customer impact, financial sale losses, and even legal implications. After those key steps, it is followed by determining recovery time objective and recovery point objectives. Recovery time objective is basically a set time that a company must fully recover from a previous attack or disruption. It is the maximum acceptable time for regaining access to company and business data. Recovery point objectives on the other hand are very similar but indicate the maximum amount of data a company can lose during a disruption. Both of these objectives go hand in hand and guide the development of recovery strategies. The last key step that will be discussed under business impact analysis is prioritizing functions. By identifying critical business functions and assessing the impact, it gives the ability to narrow down and prioritize business functions for recovery. It will decide the more important functions that will allow the most efficient recovery objectives. All these steps accumulate for an important and beneficial role in risk mitigation. Business impact analysis is very important and benefits in many ways because it sets a clear understanding and acceptance of what does or doesn’t need protection and how significant that can be. The benefits business impact analysis provides include better decision making, well guided recovery planning, and even focused risk mitigation. This process ensures that both the Business Continuity Plan and Disaster Recovery Plan are aligned with organizational priorities.

Business Continuity Plan

The next process that will be discussed is the Business Continuity Plan. This specific plan is a strategy that provides a company or business information on how to operate properly after a successful disruption or attack. It is generally an outlined document that provides critical information needed to operate expanding from company staffing to data recovery. There are a few major types of continuity plans which include Crisis Management Plans, Crisis Communications and Emergency Response Plans, IT Disaster Recovery, and Business Recovery. A business continuity plan has many key components that are needed to execute successfully which include training and testing, communication strategies, emergency response procedures, critical resource management, and alternate work arrangements. The training and testing components are programs or courses that are provided to employees to keep them well updated and informed for full readiness. Communication strategy is another component that is very important to a business continuity plan. This strategy explains how communication will be managed and operated if attacked, ensuring an efficient and accurate information and communication flow throughout the company. Emergency response procedures include and outline steps to follow during an attack or disruption. This can expand from contacts for emergency services to communication with employees, if the plan is followed and done successfully it can lead to a better recovery. A well-prepared business continuity plan provides many benefits like improving customer trust, reducing financial loss, and ensuring continuity of operations. A business continuity plan is needed for every business if they want the ability to run a company the most efficient way possible even when continuing through disruptions.

Disaster Recovery Plan

Another plan that is needed for every business if they want the ability to run a company successfully even through disruptions is the Disaster Recovery Plan. The disaster recovery plan is another strategy that provides a company or business information on how to operate properly, for a significant disaster. These disasters can include natural disasters, cyber-attacks, power outages and any other significant disaster that disrupts a company. It is another outlined document that is a little more broader than the business continuity plan, that provides critical information needed to operate properly after these disasters. This specific plan highlights and focuses on restoring the IT infrastructure after a hit which is very important in today's age. With technology continuously growing, companies are having to adapt to these technological business operations advancements. Data backup and recovery, hardware and software restoration, communication protocols, and coordination with IT teams are all elements of the disaster recovery plan. Data backup and recovery discusses different ways for saving critical data and obtaining it after an attack or disruption. Hardware and software restoration include the methods for fixing broken hardware and reinstalling the software that was previously used. Communication protocols create the plan for contacting and communicating about subject time and recovery progress. Coordination with IT teams is another great way for communication, which leads to the most efficient solutions to disruptions. Having a strong Disaster recovery plan installed can lead to strong advantages for the company or business. These advantages can include boosting business resilience, quicker technological fixes, and even mitigate data loss risks. With this plan installed and followed, a company can be sure that they will be well prepared for any bad event that could occur.

Computer Incident Response Team Plan

The last plan that will be discussed in this paper is the Computer Incident Response Team Plan. Just like the previous plans, with this plan installed and executed properly it can allow a company to be sure they are well prepared for any bad event. This specific plan goes more into the cyber security threats. With technology continuing to grow and advance, it leaves technology vulnerable to cyber attacks and malicious breaches. The computer incident response team is very important in today's age as everything is stored and operated through technology and is at risk of cyberattacks. Some key components of the computer incident response team plan are detection and reporting, analysis and containment, recovery review, and transparent communication. The computer incident response team helps explain how incidents are detected and reported, then transferred to the correct solution team. They are able to dissect the problem and figure out the diagnosis while preventing it from growing further. After each disruption is solved and contained, a post incident review is always conducted which allows the company to learn and understand prevention for the future. If the plan is executed properly, it can be very beneficial to the company or business. With this plan, it allows quicker and more efficient response time for the organizations allowing easier solutions and preventions. It also shows a proactive approach to cybersecurity which is very much needed in today's cyber advancements.

Conclusion

Throughout this paper, it went into great detail and understanding about the importance and process of formulating a Business Impact Analysis, a Business Continuity Plan, a Disaster Recovery Plan, and even the Computer Incident Response Team Plan. Mitigation and risk assessment are key for maintaining operational resilience. If every organization and business implemented these plans and procedures, potential successful attacks are less likely to happen because of better preparation and proper prevention tactics. Organizations are now able to work faster and more efficiently when applying these plans which allow quicker fixes, better preventions, and easier communication. Understanding the different aspects of risk assessment and mitigation produces better work operations, work environments, company to customer trust, and even better data security.