The Importance of BIA, BCP, DRP, and CIRTs.

Alexander O. Kotzian

School of Cybersecurity, Old Dominion University

CYSE495: Introduction to Cyber Risk Management

Hamza Demirel

April 28, 2024

Introduction

Upholding a functioning business requires significant planning and resources. Providing a service or product is the primary function of a business. For a business to perform effectively it must be able to perpetuate a revenue stream that exceeds its expenses. Therefore its critical infrastructure must be secure and well maintained. This security is not only in its ability to function, but also its ability to function effectively. Security of a business's means of production is not limited to physical security. It also includes its resistance to cyber attacks as well as outlying occurrences. The most important things a business must have in the event that any of this occurs are; Business Impact Analysis, Disaster Recovery Plans, and Computer Incident Response Team Plans which help to create the overall Business Continuity Plan.

Business Impact Analysis

Business Impact Analysis is the study of "the effects of disruptions in business, especially focusing on critical information technology functions." This process is essential to understanding the consequences of disruptions on the business's critical functions. Firstly we must identify critical business functions and the resources that allow them to function. The next step is to determine the Maximum Acceptable Outage and Maximum Tolerable Period of Disruption, this provides the knowledge required to properly implement a plan that allows operations to continue during a disruption. There are direct and indirect costs associated with a disruption. Direct costs could be considered as an immediate loss of sales or destruction of property. An indirect cost could be a societal shift of trust away from your business. Additionally a business must understand what infrastructure depends on what to properly function. Identifying these interdependencies allows a business to set up a proper organization based on the importance of the infrastructure. A BIA provides the stepping stone for a BCP to be conducted, with recommendations and other guidelines. The BIA provides a resource allocation that assists in properly allowing resources to be used for recovery efforts and the BCP. In order for a business to function properly, we must understand what makes this business function, and the costs associated with it in the event of a non-functionary period.

Business Continuity Plan

The BCP is created to conduct a collaborative plan between the Disaster Recovery Plan and the Business Impact Analysis. In order for a Business Continuity Plan to be effective, it must use the identifications provided by the BIA. In totality the BCPs function is to provide a plan for the business and specialized staff to follow in the event of a disruption that affects the primary business operations. The BCP provides a secondary option of function in this event, and allows for a business to mitigate consequential losses during the event of an outage.

The staff involved in the BCP have specialized roles and provide unique responsibilities in its implementation. The BCP program manager supervises several BCP projects occurring within a singular organization. The coordinator develops the BCP and is responsible for its activation in the event of an event. Additionally the team leads collaborate for an effective BCP activations. These teams include the Emergency Management Team, Damage Assessment Team and the Technical Recovery Team. The Emergency Management Team is made up of senior level managers that work in tandem with the BCP coordinator, Damage Assessment Team, and the Technical Recovery Team. The Damage Assessment Team identifies the severity of the technical occurrences. Finally the Technical Recovery Team is responsible for the recovery of information technology resources that are essential to the function of the business. In addition to the on-site staff, there are also key-personnel assigned different essential tasks, these would be persons or entities that are required to perform a consistent stream of critical resources.

Disaster Recovery Plan

The Disaster Recovery Plan that outlines a recovery process that occurs in the event of an outage. Multiple DRPs are involved in the creation of the BCPs. In the event of any type of disaster, whether it be natural or technical, the DRP provides a guideline for the process required to restore a system after a disturbance that ceases its function. The DRP needs to be proactively created in order to provide a detailed plan. The plan will not work effectively if it is not created prior to the event of a disaster. Each unique potential disaster requires its own complex step-by-step DRP. In order for a DRP to be successful, it requires support, employees, and other resources from managers to develop a DRP and provide the resources necessary for it to properly be attained. Managers are responsible for providing a sponsorship and teaching role for the DRP to be properly trained for and the reliability of the employees to respond appropriately. The DRP requires a backup plan that effectively addresses potential losses such as critical data. A DRP also needs a backup of data in the event of a data loss. The DRP provides a plan that mitigates potential losses in the event of an unforeseen disaster.

Computer Incident Response Team Plan

Finally the Computer Incident Response Team operates in a similar fashion to the DRP. A CIRT plan deals with computer related disruptions such as; denial of service attacks, viruses, worms, etc. Like with the DRP a CIRT plan designates roles and responsibilities to the team members such as; team leaders, human resources, network administrators, and information security specialists. A CIRT develops their own procedures through an adaptive process. The CIRT holds a responsibility to be proactive in responses to computer related disruptions. The CIRT has many policies it must abide by depending on its response. These policies include; to retaliate against the attacker or not, communication procedures, how to properly handle evidence involved in the disruption, and preventive risk measures for team members. A CIRT provides an adaptive team that mitigates risks by staying up to date, preparing for evolving computer threats, providing a policy for employees to abide by, and removing threats once discovered with potential retaliation.

Conclusion

The BIA, DRP, and CIRTs work in tandem to sustain the continued functioning of a business. These three are all necessary to help create a successful BCP. The DRP and the CIRTP are parallel to each other, and deal with the possible events that could disrupt business functions. The Business Impact Analysis provides the consequences and costs associated with the loss of these functions. This allows them to prioritize what functions to recover first. The Business Continuity Plan itself exists to prepare the business for any disruption in its operations. Just like with the CIRTP, if there was no BCP when any type of incident occurs, the company would scramble to find a solution, potentially damaging the company further. The BCP allows a company to quickly respond to an incident and mitigate the impact associated with the event.