Importance of Formulating Proper Plans in Risk Mitigation

Branden Barnes

CYSE 495: Final Exam

Professor Demirel

Introduction

Risk mitigation is important to an organization's survival. To promote risk mitigation, effective strategic plans will ensure system success. An organization's strategic priority should be a cutting-edge Business Impact Analysis (BIA). The BIA will be responsible for implementing optimal allocation of resources to maximize an organization's survival. In making an adequate BIA, a Business Continuity Plan (BCP), a Disaster Recovery Plan (DRP), and a Computer Incident Response Team plan (CIRT) will assist an organization in mitigating potential risks and ensuring operational resilience. The BIA's point of focus relies on Critical Business Functions (CBFs) to operate successfully for they are crucial to an organization's mission. The collection of data produced by the BIA will aid the BCP in carrying out operations during attacks or disasters. From there the DRP takes effect, addressing disasters and generating an outlined approach for restoration/recovery. Team members responsible for the preparation of an organization during calamity are defined in the CIRT plan.

BIA

The comprehension of MAO, CBFs, and CSFs are fundamental to the Business Impact Analysis. MAO refers to the Maximum Acceptable Outage an organization can permit. MAO is represented in two factors (high, medium, low) and direct and indirect costs. High, medium, and low symbolize high risk, mild risk, and low risk which prompt how much attention risk factors achieve. Direct costs are defined as immediate loss of sales, cash flow, equipment, building costs, penalties, cost of data recovery, and wages compensated to employees during an outage. Indirect costs are not always foreseeable but should still require as much attention. These include factors such as loss of customers, loss of public trust/reputational risk, retrieval for diminishing market shares, regain of an organizations credit rating, and the opportunity cost/loss of client

base during an outage. To develop a BIA report, the first level is to identify the environment. This entails a comprehensive evaluation of the ongoings on a day-to-day basis. Operations may vary, but CBFs demonstrate the critical components of operation. Critical business functions, for example, include all server types, software types, infrastructure necessities (electricity, water, HVAC systems), remote servers, and firewalls. How long the organization can go without these functions demonstrates the MAO. Identifying recovery priorities using high to low necessity, indicates what should come back online and how quickly. Collection of data during the BIA report should be laid out in the BIA's scope for risk mitigation, allowing the implementation process to occur. Best practices should be preformed and reevaluated annually.

BCP

Business Continuity Plan is made available when the organization is facing a disruption either from an attack or circumstance beyond one's control. This plan is comprised of DRPs that aid in the continuity of functions after disruption. The flow of operations, like CBFs, encapsulate the plan of action needed to uphold standards of performance contingent with elements such as location, systems, staff, and suppliers. The location of the business is dependent on what coverage should be held. For example, if the location of operation is at high risk for hurricanes, then their responses will differ from coverage that only relies against power outages. The BCP plan follows procedures based on location, notification, and transportation. To keep the organization running effectively through disaster, a transition of resources to a safe location must occur. This could be a transition to alternative servers to backup communication during disruption. The Business Continuity Plan should list critical equipment, software, data, documents, supplies and transport them to the proper location where they can be recovered and maintained. Certain organizations opt for "crash carts," which comprise all the necessary

components for rebuilding systems. The BCP should incorporate a program manager to supervise the process to make sure the BCP is running well during a procedure. Also, teams, key personnel, and delegation of authority should be part of the plan. Mitigating an organizations risk from potential disaster is the role of the BCP. Best practices to follow include finishing an accurate BIA. Be watchful over critical systems when returning to primary locations. Keep an up-to-date model of your BCP. Be sure to evaluate and exercise your BCP, by keeping tabs on data collection and possible faults in training procedures.

DRP

Disaster Recovery Plan is the restoration process of critical systems after a disaster has occurred. The goal of the DRP is to return basic business functions back to normalcy, facilitating the Business Continuity Plan (BCP). The DRP goes by many other names, all of which are compatible; “contingency planning, emergency management procedures, business resumption planning, corporate contingency planning, business interruption planning, and disaster preparedness” (Week 14).

Terms associated with Disaster Recovery Planning (DRP) include:

- **Critical Business Functions (CBFs):** business activities required to carry out day-to-day operations which must be restored post downtime.
- **Maximum Acceptable Outage (MAO):** Acceptable amount of downtime that won’t impede on a company’s chance of survival during an outage, also referred to as Maximum Tolerable Downtime (MTD)
- **Recovery Time Objective (RTO):** Like the MAO, RTO is the acceptable amount of time it takes for a system to go back online before there are repercussions.

- **Business Impact Analysis (BIA):** Mentioned earlier, the comprehension of MAO, CBFs, and CSFs reported for further implementation.
- **Business Continuity Plan (BCP):** plan of action needed to uphold standards of performance contingent with elements such as location, systems, staff, and suppliers.
- **Minimum Business Continuity Objective (MBCO):** The lowest amount of work acceptable to continue operating during a disaster.

DRP is a precautionary measure used when disasters occur to promote a smooth transition during crisis. Its critical success factors contain support financially and respectively from management, earning important attention from staff members to carry out actions thoughtfully. Proper allocation of leadership to endorse the DRP, will contribute to proper backup policies and recovery times. One of the DRP's main functions is to plan a data backup strategy. Backups include storing, recovering, and the duplication of data, but also protect applications if they are created by the organization. Replication of data processing, stores database servers in secondary locations. This is because if a data wipe from one server occurs, that data can still be recovered. Types of data backup policies include electronic vaulting and remote journalling. Electronic Vaulting is a method in which stored data can be transferred to "off-site location over wide area network (WAN) links or tunnels through the Internet" (Week 14). The Remote Journalling method takes backup data and sends that data to the remote site periodically. This allows for up-to-date transfers of the transaction logs and records. Big organizations promote resilience engineering that proactively allow them to operate from anywhere. This deems local downtime ineffective, allowing them to save costs while continuing to keep a positive customer satisfaction rate. Ways to uphold this model is by creating alternate locations. These can be grouped in three ways, hot sites, cold sites, and hybrid sites.

Hot sites have around the clock functionality, fully equipped with operational machinery, staff, and amenities. However, this is costly to maintain but allows organizations to swap locations at any moment, saving time on labor and downtime loss.

Cold sites lack the moments notice ability to function, but still hold basic amenities and ability to transfer operations. They are lower on cost for maintaining, but an increase in labor as well as time to fulfill.

Virtualization is a method that allows for the transfer of servers to hot sites. This permits virtual servers to be transmitted to a physical server at any location.

Proper budgeting plans need to be incorporated into your DRP plan. Organizations must figure out in their cost benefit analysis what they can cover.

Guidance for what should be included:

- Backups.
- Alternate locations.
- Power outage restoration gear.
- Amenities for staff members who cannot leave the site during a disaster.
- Emergency funds.

How does the DRP assists an organization in mitigating potential risks and ensuring operational resilience? DRPs suppress the impact a disaster has on an organization. DRPs establish a plan of action before events occur, reducing errors for an on-the-spot decision making process.

CIRT

Computer incidents are known vulnerabilities to companies. They infringed on the three basic security properties: confidentiality, integrity, and availability. The Computer Incident Response Team plan is to react to incidents like DDoS Attacks, Ransomware, SQL Injection Attacks, Malware Attacks, unauthorized access, and any other computer security incident. CIRT is like DRP in a way that they both propose a preliminary plan when disaster strikes. Their goal is to mitigate damage to the operation by applying "the five Ws: what (type of attack), where (the attack occurred), who (launched the attack), when (it happened), and why (motive behind the attack)" (Week 14). The CIRT establishes various roles and responsibilities to coordinate an intent of action. Team members use these three steps when handling attacks: containment, eradication, and recovery. Variables within those groups differ when dealing with separate attacks. For example, handling unauthorized access incidents, the CIRT confines the vulnerable system, then identifies weaknesses being exploited while monitoring other systems. The CIRT resolves infected systems by strengthening measures like changing passwords and deleting added accounts. Subsequently, the CIRT recovers systems after closing vulnerability openings and verifying correct operations through monitoring.

Containment, eradication, and recovery assist an organization in mitigating potential risks and ensuring operational resilience. The CIRT plan will define security incidents clearly, include policy guidelines during attacks, implement training of team members to mitigate threats, include checklists for essential steps, and remains to stay informed on current threats through subscriptions to security bulletins.