**The Cybersecurity Business Continuity Plan or CSBCP**

Being  IT Security Manager in a mid sized company I have formulated the following CSBCP

**Introducing Threat and Carrying Out Risk Evaluation:**

Developing a good cybersecurity business continuity plan entails a deep appreciation of risks or threats that may be posed to an organization. For a mid-sized company, key threats include:

**Phishing Attacks:**

An employee’s knowledge can be bypassed by a scammer who will intend to extract some valuable information or install a virus.

**Ransomware Attacks:**

Virus can lock important information and deny user access to it until he or she renews a prepaid ransom.

**Data Breaches**:

Unauthorised access to confidential information results in monetary risks, business harm, legal consequences.

**Supply Chain Attacks**:

Third party vendors with weaker security can give the attackers access.

**Insider Threats**:

Negligent or ill intentioned courses of actions among employees are hazardous.

When evaluating threats that threaten the organization, compare and contrast the likelihood and the impact each threat has on the organization, as well as the overall ability to address each.

**Risk Assessment:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat** | **Likelihood** | **Impact** | **Mitigation Strategies** |
| Phishing Attacks | High | High | Employee awareness training, strong email filtering, and user education. |
| Ransomware Attacks | High | High | Regular backups, strong endpoint security, and network segmentation. |
| Data Breaches | High | High | Access controls, encryption, and regular security audits. |
| Supply Chain Attacks | Medium | High | Careful vendor selection and monitoring. |
| Insider Threats | Low | High | Background checks, access controls, and employee monitoring. |

**Incident Response Procedure:**

1. Detection and Identification: Incident Report Template. There are certain steps which should be followed if incident happens.

2. Containment: The networks connected to the given machines should be isolated so that no more damage occurs.

3. Eradication: Stop the threat and repair all the compromised systems.

4. Recovery: Bring data and systems to each its original state before the extreme event occurred.

5. Lessons Learned: Carry out a post-incident examination in an organization in order to note down Best practices and shared experience that can help in future crisis to certain extent.

**Roles and Responsibilities:**

• IT Security Team: In charge of a certain incident, and also manage the responses, collaborations with other teams and deliveries of updates regarding the case.

• Finance: Consider the financial loses and approve funds for recovery.

• Human Resources: They are supposed to help employees, inform and any other required tasks.

• Sales & Marketing: Oversee response to customer relations and act in the capacity of public relations.

• Operations: Maintain the company’s specific objectives and keep disruptions in organizational activities to a low level.

**Communication Plan:**

• Internal Communications: Keep employees briefed on the situation, share information regarding the situation and response to questions from employees.

• External Communications: Especially, address customers, business counterparts and government authorities as and when required.

• Crisis Communication Team: Ensure externally communicated information is communicated to the right audience by the right team.

**Business Impact Analysis (BIA)**

• Identify Critical Functions: Identify those activities that are crucial in any business.

• Prioritize Functions: Rank the functions as far as operational impact is of consideration.

• Maximum Tolerable Downtime (MTD): Outline all possible structures of the work by determining the maximum acceptable outage time of each important work.

**Techniques of Data Backup and Data Retrieval**

• Regular Backups: These backup messages should be on a daily, weekly and monthly basis so that all the messages are safe.

• Disaster Recovery Plan: Construct an empowerment map of how to manage a large scale calamity impacting on the activity of the firm.

**Vendor Management**

• Contractual Obligations: Vendor should put security requirements in their contracts of with their clients.

• Regular Monitoring: Generally identify and manage vendor performance and potential or real security issues.

**Testing and Maintenance Plan**

• Tabletop Exercises: Perform periodic drills in order to confirm readiness of cyber threats reactions.

• Plan Updates: Prepare and consider the CSBCP for updating at least once a year or on any observed necessity.

• Employee Training: Make it mandatory to train the employees about the security awareness period to period.

With this detailed CSBCP, I think it is easy for an organization to minimize the effects of cyber-attacks and continue with operations.