Software and Cybersecurity Lab

CS445 Lab9

Name: Dipean Dasgupta **ID: 202151188**

Task: Cyber Contingency and Recovery Planning

DATASHIELD CORP

Contingency Planning Policy

[1] Policy Statement

This policy's objective is to provide **DATASHIELD CORP.** with an organized framework for creating, carrying out, and maintaining a successful contingency plan. In the case of a cyber incident or system outage, this plan is intended to minimize downtime, guarantee the continuity of IT operations, and safeguard the integrity of customer and company data.

Scope:
This policy is applicable to all of **DATASHIELD CORP.**'s IT systems, apps, networks, and employees, as well as to all of its branch offices and outside contractors that work with IT.

Responsibilities:

- ❖ **Executive Management:** Provide oversight and assistance for contingency planning by assigning required resources and guaranteeing congruence with corporate goals.
- ❖ **IT and cybersecurity departments:** Create, carry out, and continually improve the backup strategy, especially by regularly testing and training.
- ❖ **Department Heads:** Maintain operational readiness and make sure the department complies with the contingency plan.
- ❖ **Employees and contractors:** As part of the broader contingency preparedness, take part in compliance exercises, training, and simulations.

Policy Statement:
DATASHIELD CORP. is dedicated to protecting its data and IT systems' confidentiality, availability, and integrity. The contingency plan will include the following in order to do this:

- ➢ A thorough **Business Impact Analysis (BIA)** to identify and rank essential systems.
- ➢ **Preventive measures** to improve system resilience and reduce possible dangers.
- ➢ **Recovery plans** designed to promptly resume operations following interruptions.
- ➢ To guarantee the efficacy of the plan and the readiness of every employee, regular testing, training, and simulation exercises are conducted.
- ➢ **Constant upkeep and revisions** to keep the strategy up to date with changing organizational structures and threats.

Policy Compliance:
All employees, subcontractors, and pertinent outside vendors are required to abide by this guideline. Discipline up to and including contract or employment termination may result from noncompliance.

[2] Business Impact Analysis (BIA)

BIA Objective:
Critical IT systems that are vital to **DATASHIELD CORP.**'s operations are identified and assessed by the BIA, which also looks at the possible effects of different kinds of interruptions.

Critical Systems:

- **Customer Database (Priority 1):** Keeps track of personal information, purchasing history, and client data. Disruption could have a negative effect on revenue, legal responsibilities, and customer relationships.
- **Order Processing System (Priority 2):** Manages logistics, inventory, and sales. Order fulfillment would be hampered by downtime, which would affect sales and customer satisfaction.
- **Email Server (Priority 3):** Essential for communication both inside and outside the company. Even if there is less financial risk, a disruption could cause delays in client communications and decision-making.
- **Intranet and HR Systems (Priority 4):** Facilitates internal knowledge sharing and non-core functions like human resources. Employees would be inconvenienced by the outage, but primary activities would not be significantly impacted.

Impact Assessment Process:

- **Customer Database and Order Processing System:** System that are unavailable for more than 12 hours run the risk of losing money and harming their reputation. The database recovery time objective (RTO) is four hours, while the order processing RTO is six hours.
- **Email Server:** Priority recovery in 12 hours; workarounds allow up to 24 hours of downtime.
- **HR and Intranet Systems:** Up to 48-hour outages without significant disruption. 24 hours is the recovery goal.

[3] Preventive Controls

Preventive Measures Implemented:

I. **Access Controls and Multi-Factor Authentication (MFA):** MFA lowers risk by demanding several forms of identity, which decreases the likelihood of unauthorized access and limits system access to authorized users exclusively.

II. **Frequent System Backups:** Every day, important data is backed up to cloud and on-premises locations. This reduces the chance of data loss during incidents and allows for speedy data recovery.

III. **Intrusion Detection and Prevention Systems (IDPS):** Proactive reaction to threats is made possible by real-time monitoring and alerting technologies that detect possible security breaches.

IV. **Patch Management:** Protection against known vulnerabilities is ensured by automatically updating all systems. Frequent patching guarantees that systems are current and lowers risk exposure.

V. **Redundant Power and Network Connectivity:** Systems are always available thanks to backup power systems like uninterruptible power supplies (UPS) and redundant internet connections.

[4] Recovery Strategies

Scenario-Based Recovery Strategies:

1. **Data Loss (e.g., Ransomware Attack):**

   - **Immediate Action:** Disconnect affected systems to prevent further spread.
   - **Recovery Plan:** Restore data from the latest uninfected backup stored on an isolated network or in the cloud.
   - **Rationale:** Timely data restoration prevents ransom payments and guarantees continuation. Regular backup procedures enable this.

2. **System Outage (e.g., Hardware Failure):**

   - **Immediate Action:** Switch to a mirrored cloud-based system to maintain operations.
   - **Recovery Plan:** Use hot-swappable hardware and replicate the primary systems to an alternative site.
   - **Rationale:** Critical services will continue to function even in the event that primary hardware fails when a cloud failover is used.

3. **Cyber Attack (e.g., Phishing Incident):**

    - **Immediate Action:** Isolate the infected system, change compromised credentials, and conduct a security assessment.
    - **Recovery Plan:** Revalidate security measures, keep an eye out for any residual dangers, and adhere to a methodical incident response and recovery procedure.
    - **Rationale:** Ensures immediate containment and minimizes additional compromise.

4. **Natural Disaster (e.g., Power Outage):**

    - **Immediate Action:** Activate backup power systems and notify employees to ensure their safety.
    - **Recovery Plan:** Reroute data and applications to a secondary data center or cloud environment.
    - **Rationale:** Ensures continued operations and limits business interruptions.

[5]IT Contingency Plan

IT Contingency Plan Overview:

1. Notification/Activation Phase:

- **Activation Process:** The IT manager assesses the situation and alerts the Cybersecurity Incident Response Team (CIRT).
- **Stakeholder Notification:** Key stakeholders, including department heads and the CIO, are notified.
- **Documentation:** Initial information about the incident is recorded, including the time, date, systems impacted, and preliminary findings.

2. Recovery Phase:

- **System Restoration:** Use offshore backups to restore systems. Cybersecurity experts thoroughly inspect retrieved systems for any malware.
- **System Testing:** Before restarting full operations, verify functionality, test connectivity, and examine access controls.
- **Communication:** Regular updates provided to stakeholders, employees, and customers to maintain transparency.

3. Reconstitution Phase:

- **Full System Restoration:** Systems are progressively brought back online. Evaluating any pending fixes or updates is one of the follow-up steps.
- **Debrief and Lessons Learned:** To stop recurrence, the team performs a thorough post-event study, records problems, and suggests fixes.

[6] Testing, Training and Exercises

Mock Drill for Phishing Attack:

Scenario Setup:
In order to find employees who might unintentionally compromise critical information, the simulation uses a phishing email campaign.

Steps for the Drill:

- ❖ **Send Simulated Phishing Emails** to employees, containing realistic but fake links to test their response.
- ❖ **Monitor Employee Actions:** Track how employees respond, whether they report, ignore, or engage with the email.
- ❖ **Activate Response Plan:** The incident response team intervenes to mimic containment and recovery processes after compromised accounts are identified.
- ❖ **Post-Simulation Analysis:** Discuss areas for improvement, give employees a briefing on appropriate answers, and offer extra training to any staff members that interacted with the phishing emails.

Objectives:

- Assess the employees' level of awareness.
- Evaluate the efficacy of the answer and pinpoint any procedural flaws.
- Boost general preparedness for cybersecurity.

[7] Plan Maintenance

Ongoing Maintenance and Update Protocols:

- ➢ **Quarterly Plan Review:** Review and revise the plan frequently to account for emerging technology and security risks. The CIRT leads the cybersecurity and IT teams in this review.
- ➢ **Annual Full Plan Testing:** To make sure all parts work as intended and adjust to modifications in infrastructure or business procedures, run a thorough test.

- **Post-Incident Revisions:** Conduct a review following any occurrence to take into account the lessons learnt and modify the strategy as necessary.
- **Change Management Integration:** Make sure that any system changes or adjustments are incorporated in the contingency plan by coordinating with the change management team.
- **Employee Training Updates:** To keep everyone informed and ready, incorporate fresh training sessions whenever the strategy is modified or new staff members join.

-------------------End of POLICY----------------------

SUMMARY

In the task, cyber contingency and recovery planning for **DATASHIELD CORP** is prepared. By empowering **DATASHIELD CORP.** to proactively manage possible interruptions, the policy statement promotes organizational resilience. According to BIA, **DATASHIELD CORP.** needs to give top priority to quickly restoring its order processing and customer database systems because of their vital roles in generating income and ensuring customer satisfaction. By putting these measures in place, **DATASHIELD CORP.** improves system availability and reduces the chance of interruptions, guaranteeing business continuity. By using these recovery techniques, **DATASHIELD CORP.** can minimize downtime and preserve operational integrity while promptly handling various incident types. The IT Contingency Plan aims for effective restoration and operational continuity while guaranteeing full recovery capabilities.

These steps guarantee that **DATASHIELD CORP.'s** contingency plan stays up to date, operational, and efficient while adjusting to organizational changes and changing cybersecurity threats.

---**END of ASSIGNMENT**---