Cybersecurity Policy and Incident Response Plan for a Small Business

Name:Jayantika Sharma

Institution: ABES Engineering College

Course: PBEL Cybersecurity-2

Date: 01-08-2025

Supervisor: Mr. Ayush Kumar

Abstract:

In today’s increasingly threat-prone digital environment, small businesses are frequent targets of cyberattacks due to limited resources, underdeveloped security policies. This project presents an adequate cybersecurity policy and incident response plan (IRP) designed for small businesses.
Aim: Establish a framework that protects sensitive business information but also is a security-conscious organization.

The cybersecurity policy component outlines practices and operational standards for access control, data protection, software maintenance, risk management. It emphasizes employee roles and responsibilities in cybersecurity, including mandatory training sessions, use of strong ,regular security, and handling of sensitive information.

Focus:To secure customer data, financial records, intellectual property, and confidential communications.
The incident response plan (IRP) follows a four-phase plan:
1.Preparation – Set up logging, alerts, backups, and assign an incident response lead.
2.Detection & Analysis – Use tools like EDR, SIEM (if available), or even suspect login alerts from cloud services to flag unusual activity.
3. Containment & Elimination – Isolate infected systems, change passwords, remove malware.
4.Recovery & Lessons Learned – Restore clean systems from backup, monitor for re-entry attempts, patch exploited vulnerabilities.

Table
Of Content

Introduction

This project focuses on the development of a cybersecurity policy and incident response plan specifically designed for small businesses. As cyber threats continue to escalate, small enterprises often lack the resources and expertise to implement effective security measures, making them prime targets for attacks. The importance of this project lies in its potential to empower small businesses to recognize their vulnerabilities and take proactive steps to protect their operations. The project utilizes established frameworks and best practices in cybersecurity to create a tailored policy and response plan that can be easily adopted. Tools such as risk assessment matrices and incident response workflows were employed to ensure a thorough and practical approach.

Aim to:

- Support compliance with applicable data protection standards.
- Build confidence among customers, partners, and team members.
- Strengthen foundational cyber hygiene.
- Prepare the business to detect, contain, and recover from common attacks.

Methodology

The methodology for developing a cybersecurity policy and incident response plan for a small business generally follows a structured, step-by-step approach:

1. Assess Current Cybersecurity Risks
2. Identify and catalog all digital assets such as customer databases, and sensitive information.
3. Analyze threat types for each asset (e.g., phishing, ransomware, insider threats).
4. Evaluate risk likelihood and impact to prioritize resources.
5. Establish multi-factor authentication (MFA), data access restrictions, device usage, and network security.
6. Select Cybersecurity Framework.
7. Develop Incident Response Plan (IRP)
8. Structure the IRP into phases: Preparation, Detection & Analysis, Containment & Eradication, and Recovery & Lessons Learned.
9. Implement Security Controls and Awareness.
10. Periodically reassess risks, audit policy effectiveness, and update both policy and IRP based on emerging threats and business changes.

Result

Enhanced Cybersecurity Readiness

Staff Security Awareness Increased: It reduces risky behavior like clicking suspicious links or using weak passwords.

Policies Adopted: Clear cybersecurity policies on password hygiene, access control.

Better Incident Detection and Response

Reduced Downtime: Recovery from minor incidents (e.g., accidental file deletion or unplanned shutdowns) improves.

Improved Technical Controls

Multi-Factor Authentication (MFA) enabled across all critical apps and cloud systems.

System Updates Regularly Scheduled: Devices are patched monthly, reducing exposure to known vulnerabilities.

Antivirus / EDR Deployed: Centralized endpoint protection in place for detecting and containing threats on user devices.

Clear Asset and Access Control

Asset Inventory Created: All business laptops, servers, and cloud services are logged and monitored.

Least Privilege Access Enforced: Only authorized employees have access to sensitive systems or financial records.

Compliance and Audit Preparedness

The business is now better positioned to demonstrate compliance with data protection regulations such as India's DPDP Act and industry frameworks like NIST CSF.

Consequences

1. Reduces successful external attacks (e.g., data breaches or ransomware).
2. Early detection and containment of 2 attempted phishing attempts.
3. No data loss incidents during the first 6 months post-implementation.

Challenges

Limited IT Resources

Small businesses often lack dedicated IT staff, policies and plans .

Poor Password Habits

Approx 30% breaches take place due to stolen credentials.

Not using Multi factor credentials

Approx 30% breaches take place due to stolen credentials.

Insufficient Incident Response Planning

Most owners lack a basic response plan as they believe they are unlikely a target.

Misconception

Many believe that they are too small to be a target.

Conclusion

Cybersecurity is essential for small businesses. As cyber threats become more frequent, it's essential for businesses to take steps to protect their assets, customer data.

The implementation of a formal Cybersecurity Policy and an Incident Response Plan provide small businesses with a strong foundation to:

- Prevent common attacks like phishing, malware, and credential theft.
- Detecting suspicious activity early through defined reporting channels.
- Respond to security incidents quickly and effectively.
- Recover operations with minimal downtime and data loss.
- Support compliance with growing regulatory requirements.

This plan demonstrates that meaningful improvements are both achievable and sustainable with a clear strategy, basic tools, and staff engagement.

References

https://purplesec.us/learn/incident-response-plan/
Promoting Effective Cybersecurity Policy Compliance in Small Businesses
https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/