Cybersecurity Policy and Incident Response Plan

Submitted by:

Vinayak Sinha

Institution:

GL Bajaj Institute of Technology and Management

Course:

CYBERSECURITY

Date:

15th July 2025

Supervisor:

Hrushikesh Dinkar

Cybersecurity Policy and Incident Response Plan

Abstract

In the evolving digital landscape, cybersecurity is paramount for protecting organizational assets and maintaining business continuity. This project addresses the critical need for a comprehensive cybersecurity policy and incident response plan tailored for SecureTech Solutions Pvt. Ltd., a mid-sized IT services company. The objective was to design a framework that not only ensures data protection but also enables swift and effective incident handling.

The solution was structured around globally recognized standards such as NIST, ISO/IEC 27001, and OWASP. Key policy areas included Acceptable Use, Password Management, BYOD, Data Classification, and Remote Access, enforced using tools like Microsoft Purview, Intune, pfSense, and CrowdStrike. The Incident Response Plan was built on the NIST model, encompassing preparation, identification, containment, eradication, recovery, and lessons learned. Tools like Splunk, Snort, and Cortex XSOAR facilitated automation and real-time monitoring.

Key outcomes include enhanced threat detection, improved response times, and increased staff awareness through regular drills and training. A simulated ransomware attack demonstrated the policy's effectiveness, where swift isolation, eradication, and recovery minimized downtime and data loss. The project concluded with recommendations for continuous improvement through automation, regular audits, and Zero Trust architecture. This comprehensive approach positions SecureTech as a resilient and security-aware organization in the face of modern cyber threats.

Table of Contents

Introduction

Introduction

This project, titled "Cybersecurity Policy and Incident Response Plan," is focused on creating a structured and comprehensive approach to protect an organization's digital infrastructure and sensitive data. In today's digital age, cyber threats are increasing rapidly and affecting businesses of all sizes. This project aims to build a solid foundation for managing cybersecurity risks and responding to security incidents effectively.

I chose this project because cybersecurity is a growing concern for companies, especially mid-sized businesses that often lack robust security systems. With digital operations expanding, even one successful cyberattack can result in data breaches, financial loss, and reputational damage. This project addresses these issues by designing and implementing clear security policies and a step-by-step response plan for incidents.

To solve this, I developed a detailed set of cybersecurity policies including acceptable use, password management, BYOD guidelines, data classification, and remote access. Additionally, I created an incident response plan based on NIST standards, covering preparation, detection, containment, eradication, recovery, and lessons learned.

I used tools and frameworks like the ELK Stack for log analysis, Splunk for monitoring, Snort for intrusion detection, and CrowdStrike for endpoint protection. The project also utilized methods like STRIDE threat modeling, OWASP secure coding practices, and compliance guidelines from ISO/IEC 27001. Together, these tools and practices ensure that the organization is well-prepared to defend against and recover from cyber threats.

Literature Review

Literature Review

This project builds upon established cybersecurity frameworks, tools, and methodologies that are widely recognized in the industry. A thorough review of these technologies was conducted to ensure that the cybersecurity policy and incident response plan are built on solid foundations.

One of the primary references for this project is the NIST Cybersecurity Framework, which provides a comprehensive structure for identifying, protecting, detecting, responding to, and recovering from cyber threats. This framework has been adopted by numerous organizations across sectors for its clarity and effectiveness in managing cybersecurity risks.

The project also integrates principles from ISO/IEC 27001, a leading international standard for information security management systems. It emphasizes risk management, access control, and continuous improvement, which are essential for implementing robust security policies.

In terms of technology, tools like the ELK Stack (Elasticsearch, Logstash, Kibana) were explored for real-time log collection, analysis, and visualization. Splunk, another powerful SIEM solution, was studied and utilized for security event monitoring and correlation. For intrusion detection, Snort was chosen due to its open-source flexibility and strong community support.

OWASP guidelines and the OWASP Top 10 list served as the foundation for secure coding practices. These resources highlight the most common web application vulnerabilities and offer best practices to prevent them.

This literature review confirms that the project is grounded in well-established cybersecurity principles and technologies, ensuring both relevance and effectiveness in real-world application.

Methodology / Approach

Methodology / Approach

Approach:

The project aimed to develop a practical and scalable Cybersecurity Policy and Incident Response Plan for SecureTech Solutions Pvt. Ltd., a mid-sized IT services company. The approach was to adopt industry standards like NIST and ISO/IEC 27001 and align them with tools and workflows suited for small to mid-sized teams. The objective was to establish both preventive and responsive cybersecurity measures.

Tools and Technologies:

- ELK Stack: Used for aggregating, parsing, and visualizing logs from across systems.
- Splunk: Real-time security event monitoring and alert generation.
- Snort: Open-source intrusion detection system for identifying malicious traffic.
- CrowdStrike: Endpoint detection and response (EDR) tool used for threat intelligence and remediation.
- OWASP ZAP & Burp Suite: Used for vulnerability scanning of internal web applications.
- Checkov: Infrastructure-as-Code scanning tool to detect security misconfigurations.
- Jira & Cortex XSOAR: Used for orchestrating and managing incident response playbooks.
- Ansible & WSUS: Automating system patching and updates to reduce vulnerabilities.

Step-by-Step Process:

1. Conducted initial requirement analysis using ISO 27001 checklists to define security needs.
2. Drafted cybersecurity policies, including Acceptable Use, Password, BYOD, Data Classification, and Remote Access.
3. Built the Incident Response Plan following NIST's six-phase model.
4. Set up ELK Stack and Splunk for log management and real-time alerts.
5. Deployed Snort for network-based threat detection.
6. Scanned applications with Burp Suite and ZAP for security flaws.
7. Used Checkov to audit infrastructure code for misconfigurations.
8. Managed patches and updates using Ansible and WSUS.
9. Simulated a ransomware attack to validate the response workflow and improve policy enforcement.

Results and Discussion

Results and Discussion

Results:

The implementation of the cybersecurity policy and incident response plan at SecureTech Solutions Pvt. Ltd. led to a more structured and proactive security posture. Key outcomes include successful deployment of log monitoring through ELK Stack and Splunk, detection of simulated attacks using Snort, and secure endpoint coverage via CrowdStrike. A ransomware simulation was conducted, where logs in Splunk showed abnormal file encryption activity, leading to swift containment and recovery using playbooks in Cortex XSOAR.

Web application testing using OWASP ZAP and Burp Suite revealed vulnerabilities such as missing security headers and input validation issues. These were addressed by enforcing OWASP-recommended coding practices and deploying updated security configurations.

Discussion:

The findings confirm the effectiveness of combining layered cybersecurity policies with an automated response framework. Real-time monitoring tools enhanced threat visibility, while the response workflow reduced downtime during incidents. Vulnerability detection validated the need for secure coding practices and ongoing testing.

Challenges:

Some of the key challenges included configuring tools like ELK Stack to properly ingest and visualize logs from multiple sources, and balancing strong policies with user convenience. Additionally, ensuring employee awareness without overwhelming non-technical staff was a hurdle. Cost-effective implementation of enterprise-grade tools in a mid-sized setup also required careful planning.

Despite these challenges, the project successfully enhanced the organization's security readiness and built a scalable model for ongoing improvement.

Conclusion

Conclusion

The Cybersecurity Policy and Incident Response Plan project successfully addressed the core challenges faced by SecureTech Solutions Pvt. Ltd. in protecting its digital infrastructure. By implementing a structured set of policies and an effective incident response framework, the organization is now better equipped to prevent, detect, and respond to cyber threats. The project achieved its primary goal of strengthening security practices using widely recognized standards like NIST and ISO/IEC 27001.

Throughout the project, I gained valuable experience in designing real-world cybersecurity strategies, configuring advanced tools, and executing simulations like a ransomware attack. I also learned the importance of aligning technical solutions with organizational workflows and employee awareness. Integrating tools like Splunk, Snort, CrowdStrike, and ELK Stack gave me practical insights into modern security operations.

Future Work:
With additional time and resources, the project could be enhanced by integrating AI-based threat detection, expanding Zero Trust architecture, and automating forensic analysis post-incident. Conducting regular red team-blue team exercises would also provide deeper insights into potential vulnerabilities. Further improvements could include advanced SOC (Security Operations Center) features and dynamic policy enforcement through machine learning.

In conclusion, this project not only met its objectives but also laid a strong foundation for continuous security improvement and future innovation.

Cybersecurity Policy and Incident Response Plan

SecureTech Solutions Pvt. Ltd.

Submitted by: Vinayak Sinha

Email: vinayaksinha344@gmail.com

Methodology

- Used NIST, ISO/IEC 27001, and OWASP guidelines as base.
- Sections included: Acceptable Use, Password Policy, BYOD, Data Classification, Remote Access.
- Incident Response Plan built on NIST framework: Preparation, Detection, Containment, Eradication, Recovery, Lessons Learned.

Cybersecurity Policies

- Acceptable Use Policy: Enforced via GPO, DLP tools.
- Password Policy: Strong passwords, MFA (Okta, Azure AD).
- BYOD: MDM Enrollment (Intune, MobileIron).
- Data Classification: Using Microsoft Purview, Varonis.
- Remote Access: VPN + MFA, pfSense, CrowdStrike.
- Incident Response Policy: Playbooks, Splunk, Cortex XSOAR.

Incident Response Plan

- 1. Preparation – Awareness training, asset inventory.
- 2. Identification – Splunk & Snort monitoring.
- 3. Containment – Isolate systems, apply patches.
- 4. Eradication – Malware removal, system restore.
- 5. Recovery – Validate system health, resume ops.
- 6. Lessons Learned – Review, update policies.

Workflow and Tools

- Requirement Analysis – Compliance checklists.
- Planning – Threat modeling (STRIDE).
- Development – OWASP secure coding (Snyk, SonarQube).
- Testing – Burp Suite, ZAP.
- Deployment – CI/CD scanning (Checkov).
- Monitoring – Splunk, Nagios.
- Response – Jira, Splunk playbooks.
- Maintenance – Ansible, Veeam, WSUS.

Challenges

- Making policies simple and actionable for small teams.
- Choosing affordable, scalable tools.
- Ensuring staff awareness without technical overload.
- Maintaining compliance with minimal IT resources.

Cybersecurity Policy and Incident Response Plan

Organization Name: SecureTech Solutions Pvt. Ltd. **Sector:** Information Technology (IT) Services **Location:** Bengaluru, India **Size:** Mid-sized, ~150 employees

---

Table of Contents

---

1. Introduction

In today's digital era, protecting information assets is crucial for any business. SecureTech Solutions Pvt. Ltd. aims to safeguard its digital infrastructure and customer data using a comprehensive cybersecurity policy and a well-defined incident response plan.

---

2. Organization Blueprint

SecureTech Solutions Pvt. Ltd. is a mid-sized IT services company specializing in cloud computing, mobile app development, and data analytics. The company operates with a workforce of around 150 employees across different departments:

- IT & Development
- Cybersecurity
- Operations
- Human Resources
- Finance
- Customer Support
- Sales & Marketing

Key Features:

- 24x7 service delivery
- Remote and in-house development teams
- Agile project management methodology

3. Technology Stack

Category	Technologies Used
Cloud	AWS, Azure, GCP
DevOps	Docker, Kubernetes, Jenkins
Development	GitHub, React, Node.js, Python
Operating Systems	Windows 10/11, Ubuntu, CentOS
Communication	Microsoft Teams, Slack
Database	MySQL, PostgreSQL, MongoDB
Monitoring	Zabbix, Nagios
Security Tools	Splunk, Nessus, Snort, CrowdStrike

4. Workflow and Operations

1. **Requirement Analysis**
2. **Planning & Design**
3. **Development (Agile Sprints)**
4. **Testing (Manual & Automated)**
5. **Deployment (AWS/Azure Environments)**
6. **Continuous Monitoring**
7. **Incident Detection & Response**
8. **Maintenance & Upgrades**

5. Network Architecture Overview

- Multi-tier architecture with DMZ (Demilitarized Zone)
- Firewalls (pfSense), IDS (Snort)
- Cloud-hosted services with VPN access
- Segmented VLANs for isolation

6. Security Tools in Use

Purpose	Tool
Network Scanning	Nmap
Vulnerability Scanning	Nessus
Endpoint Protection	CrowdStrike

Purpose	Tool
Log Management	Splunk
Firewall/IDS	pfSense, Snort
Backup & Recovery	Veeam, AWS S3
SIEM	ELK Stack

---

7. Cybersecurity Policies

A. Acceptable Use Policy

Defines acceptable practices for using company assets.

B. Password Policy

Strong password enforcement with MFA.

C. BYOD Policy

Secure usage of personal devices.

D. Data Classification Policy

Data labeled as Public, Internal, Confidential, or Restricted.

E. Remote Access Policy

Use of VPN and endpoint security.

F. Incident Response Policy

Defines roles, responsibilities, and procedures.

---

8. Incident Response Plan

1. Preparation

- Security awareness training
- Asset inventory and configuration baseline

2. Identification

- Monitoring via Splunk
- Alert generation using Snort

3. Containment

- Short-term: Isolate systems
- Long-term: Patch and harden affected assets

4. Eradication

- Malware removal
- Restore clean system states

5. Recovery

- Validate system health
- Resume operations

6. Lessons Learned

- Post-incident analysis
- Update response playbooks

---

9. Case Study: Ransomware Attack Simulation

Scenario:

Employee clicks on malicious email attachment, launching ransomware.

Response:

- **Detected** via abnormal file encryption patterns (Splunk logs)
- **Isolated** affected machine
- **Eradicated** ransomware using forensic tools
- **Restored** data from AWS backup
- **Updated** email filters and conducted retraining

---

10. Lessons Learned

- Need for real-time threat hunting
- Importance of phishing awareness
- Enhanced logging and alert tuning

---

11. Recommendations

- Regular penetration testing
- Zero Trust Architecture
- Frequent policy updates
- Automate patch management

Enhanced Cybersecurity Policy and Operations Report

1. Enhanced Workflow and Operations Description

Requirement Analysis

Engage with stakeholders to identify regulatory, legal, and business requirements.
Tools: Compliance checklists, ISO 27001 templates.
Purpose: Early identification of data sensitivity and risk zones.

Planning & Design

Integrate threat modeling using STRIDE and Zero Trust architecture.
Tools: ThreatModeler, Microsoft Threat Modeling Tool.
Purpose: Prevent design-level vulnerabilities.

Development

Enforce secure coding standards based on OWASP guidelines.
Tools: SonarQube, Snyk.
Purpose: Prevent security bugs.

Testing

Automated and manual vulnerability testing.
Tools: OWASP ZAP, Burp Suite.
Purpose: Detect security loopholes before deployment.

Deployment

Secure CI/CD pipelines and use IaC scanning.
Tools: Checkov, Jenkins.
Purpose: Prevent misconfigured environments.

Monitoring

Continuous infrastructure and application monitoring.
Tools: Splunk, Nagios, CrowdStrike.
Purpose: Real-time threat detection.

Incident Response

Triage alerts using SIEM, assign tasks via playbooks.
Tools: Jira, Splunk.
Purpose: Rapid containment and recovery.

Maintenance

Routine patching and auditing.
Tools: WSUS, Ansible, Veeam.
Purpose: Maintain current and secure systems.

2. Cybersecurity Policies (Expanded)

Acceptable Use Policy

Implementation: Enforced via Group Policy Objects (GPO).
Impact: Implemented - Reduces misuse; Not Implemented - Risk of data leakage.
Tools: Microsoft GPO, Symantec DLP, Proofpoint.

Password Policy

Implementation: Enforce strong passwords and MFA.
Impact: Implemented - Prevents brute-force attacks; Not Implemented - Risk of compromise.
Tools: Okta, Azure AD, Bitwarden.

Bring Your Own Device (BYOD)

Implementation: Enroll in MDM with security policies.
Impact: Implemented - Secures endpoints; Not Implemented - Entry points for malware.
Tools: Intune, MobileIron, AirWatch.

Data Classification

Implementation: Label and protect based on sensitivity.
Impact: Implemented - Enforces control; Not Implemented - Higher risk of data breach.
Tools: Microsoft Purview, Symantec DLP, Varonis.

Remote Access Policy

Implementation: Use VPN + MFA, restrict access.
Impact: Implemented - Secures access; Not Implemented - Vulnerable to intrusions.
Tools: pfSense VPN, Okta MFA, CrowdStrike.

Incident Response Policy

Implementation: Regular drills and updated playbooks.
Impact: Implemented - Quick recovery; Not Implemented - Worsened damage.
Tools: Jira, Splunk, Cortex XSOAR.

12. Conclusion

This policy and response plan ensures SecureTech is prepared to face cyber threats effectively, minimizing damage and ensuring continuity of operations.

---

13. References

- NIST Cybersecurity Framework
- ISO/IEC 27001 Standards
- OWASP Top 10
- SANS Institute Guidelines

Submitted by - Vinayak Sinha
Email - vinayaksinha344@gmail.com