SECURITY MANAGEMENT- ASSIGNMENT NO.2

DISHA MEGHNANI
HARSHITHA KUMARESAN
PRUTHA MANE
SUSHMA SIDDARAJU
PRIYANKA PAWAR

INTRODUCTION

Objective: Help the company build a scalable and effective cybersecurity strategy to support growth and instil client confidence.

Key Concerns:

- Align security spending with company priorities.
- Reduce reliance on the security team's intensive efforts.
- Build a clear, understandable security framework for clients.

Approach:

- Develop a comprehensive cybersecurity policy and framework.
- Focus on scalable processes that evolve with company growth.

CONDUCTING A STRATEGIC RISK ASSESSMENT

- **Goal: Identify gaps and prioritize risks.**

Actions:

- ❑ Audit current systems for vulnerabilities and redundancies.
- ❑ Engage stakeholders to understand business-critical assets and workflows.
- ❑ Map risks to regulatory requirements:
    1. GDPR: EU privacy law ensuring data compliance.
    2. PCI DSS: Security standard for safe payment card transactions.

Outcome:

- ○ Risk Matrix: A visual tool to prioritize risks based on likelihood and impact.
    - ▪ Likelihood: How likely the risk will occur.
    - ▪ Impact: Severity of consequences.

EXAMPLES OF RISKS TO ADDRESS & LEAVE UNTREATED

- **Serious Risks to Address:**
  1. Advanced Persistent Threats (APT):
     - Mitigation: Real-time monitoring, next-gen firewalls.
  2. Third-Party Vendor Risks:
     - Mitigation: Vendor assessments, and enforce cybersecurity clauses.
  3. Data Breaches & Customer Trust Loss:
     - Mitigation: Encrypt data, enforce access controls, and regular audits.
- **Risks to Leave Untreated:**
  1. Minor Unpatched Software:
     - Rationale: Prioritize higher-risk issues first.
  2. Non-Critical Devices' Physical Security:
     - Rationale: Focus on high-risk systems.
  3. Low-Impact Phishing Attempts:
     - Rationale: Allocate resources to advanced persistent threats (APTs).

DEVELOP A COHERENT CYBERSECURITY POLICY

Policy Draft: ***"A unified cybersecurity policy will be established to ensure consistent security practices, governance, and compliance across all departments and teams.“***

□ **Security Objectives:**

1. Protect Customer Data: Secure sensitive client and company data from unauthorized access and breaches.
2. Safeguard Intellectual Property: Implement strong access controls and secure repositories for company assets.
3. Shield Critical Systems: Use proactive monitoring and incident response to ensure uptime and resilience.
4. Prioritize Risk Mitigation Investments: Focus resources on addressing high-risk areas to maximize impact.

KEY COMPONENTS OF THE CYBERSECURITY POLICY

❑ **Governance:**

- Roles and Responsibilities: Define accountability across teams, such as appointing a Chief Information Security Officer (CISO), forming an Incident Response Team (IRT) and ensuring all the employees participate in the training and report suspicious activity.

- Regular Reviews: Schedule quarterly reviews to adapt to new challenges and maintain alignment with business goals.

□ **Core Practices:**

- Incident Response Plans: Establish protocols for detection, containment, and recovery from cyber threats.

- Secure Vendor Onboarding: Use risk assessments and clear security requirements for third-party integrations.

- Regular Staff Training: Conduct ongoing programs on phishing, password hygiene, and secure data handling.

□ **Compliance Standards:**

- Align with frameworks like ISO 27001 (Information Security Management) or NIST (Cybersecurity Framework) to meet industry benchmarks.

RESOURCE ALLOCATION POLICY

Resource Allocation Policy; ***"Cybersecurity investments will align with risk priorities to ensure optimal use of resources."***

Purpose: **Ensure cybersecurity investments align with high-priority risks to maximize impact and optimize spending.**

- **Key Goals:**

1. Enhance scalability and efficiency through targeted investments.
2. Balance expenditures between emerging threats and operational needs.

- **Spending Priorities:**

1. High Priority:

a) Automation tool for threat detection (e.g., SIEM solutions).

b) Endpoint security for remote work environments.

c) Regular employee training to prevent phishing and social engineering attacks.

2. **Low Priority:**

a) Legacy system with limited impact on the current security landscape.

b) Non-critical physical security enhancements.

EFFECTIVE RESOURCE ALLOCATION STRATEGIES CONTENT:

Implementation Plan and Examples:

- Conduct quarterly risk assessments to guide spending decisions.
- Establish a Cybersecurity Investment Plan based on the risk matrix.
- Reallocate resources to high-impact areas identified in assessments.

Examples of High-Impact Investments:

- Automated Threat Detection: Deploy SIEM solutions for real-time monitoring.
- Strengthened Perimeter Defenses: Use next-gen firewalls and intrusion prevention systems.
- Employee Awareness Programs: Phishing simulations and secure data handling workshops.

Review Mechanisms:

- Annual audits to measure ROI on cybersecurity investments.
- Continuous feedback loops from the security team to refine priorities.

This policy ensures resources are allocated where they are most needed, safeguarding critical assets while avoiding unnecessary expenditure.

IMPLEMENT A SCALABLE SECURITY FRAMEWORK

Approach: **Shift from intensive manual operations to automation and standardization to improve efficiency and scalability.**

Policy Draft: **"*The company will adopt scalable security practices, including automation of threat detection and incident response, to manage growing infrastructure securely.*"**

Key Components:

- **Automated Security Solutions**
  Deploy SIEM, IDS/IPS to reduce manual workload.

- **Automated Security Incident Response (SIR)**
  Faster threat mitigation through automation.

- **Centralized Access Management**
  Implement role-based access controls (RBAC) across the organization.

- **Regular Security Audits**
  Assess the effectiveness of tools and processes.

STEPS TO IMPLEMENT THE FRAMEWORK

Action Plan:

1. Adopt SIEM Solutions:
   - Centralize security event monitoring to detect threats in real time.
2. Build an IAM Framework:
   - Implement Identity and Access Management to control and manage user access.
3. Create Playbooks for Automated Incident Response:
   - Develop standardized playbooks to automate and accelerate incident response procedures.

Benefits of This Framework:

- Reduces manual effort.
- Enhances threat detection and mitigation speed.
- Ensures consistent security practices as infrastructure scales.

BUILD TRUST THROUGH TRANSPARENCY

Purpose: Enhance customer credibility by demonstrating a commitment to security and openness.

Key Actions to Achieve Transparency:

1. **Develop Client-Facing Security Materials**
   - Create comprehensive, easy-to-understand documents explaining your security protocols and measures.
   - Include visual aids like flowcharts, diagrams, and infographics to illustrate technical concepts.
   - Ensure content highlights compliance with relevant industry standards (e.g., ISO 27001, SOC 2).
2. **Publish an Annual Cybersecurity Report**
   - Share key updates on cybersecurity initiatives, new implementations, and any challenges faced.
   - Incorporate metrics like threat detection rates, incident response times, and results of penetration testing.
   - Include forward-looking strategies to show continuous improvement and vigilance.
3. **Share Independent Audit Reports with Key Clients**
   - Provide access to third-party security assessments or certifications, building confidence in your controls.
   - Offer briefings to explain audit outcomes and address client-specific concerns.
   - Highlight any remediation plans for identified gaps to showcase proactive risk management.

BUILD TRUST THROUGH TRANSPARENCY"

Our policy is clear: *“**The company will demonstrate transparency to clients and stakeholders by regularly reporting on security efforts, audits, and risk mitigation strategies.”***

To achieve this, we’ve outlined three key initiatives:

1. Regular Security Reporting:
   We’ll provide clients with detailed security reports that include audit outcomes and risk assessments. These reports help clients understand how we’re safeguarding their data and addressing potential risks.

2. Independent Audits:
   To validate our security claims, we’ll engage trusted third-party auditors. Their assessments provide unbiased confirmation of our robust security measures and give our clients added confidence in our systems.

3. Proactive Incident Communication:
   In the rare event of a security incident, we commit to immediate client communication. We’ll share the issue, our response strategy and the resolution process transparently to keep stakeholders informed and reassured.

These steps underline our dedication to earning and maintaining trust through transparency. It’s not just a policy; it’s how we demonstrate accountability and partnership with our clients every day.

CONCLUSION

- Implementing a Comprehensive Cybersecurity Management Framework ensures alignment between security efforts and business goals, enhancing efficiency, scalability, and client trust.
- This approach involves prioritising risks through strategic assessments, establishing clear objectives and compliance through a cohesive policy, and optimising resources by focusing on scalable and automated solutions.
- The framework safeguards critical assets while building trust and demonstrating accountability by adopting centralized monitoring, automated incident response, and transparent client communication.

THANK YOU