mySymptoms Health App

Cybersecurity Investment Strategy & Risk Management

Security Case Study

Stephanie (Seeyeon) Oh

Executive Summary

Following the October 2025 cybersecurity breach at mySymptoms, this document presents a comprehensive risk assessment and investment strategy to strengthen the organization's security posture. Through systematic evaluation of organizational assets using a Threat Asset Matrix, we have identified critical vulnerabilities and developed a tiered investment approach that prioritizes resources based on risk magnitude.

This strategy allocates security spending across three tiers: Tier 1 (60% of budget) focuses on critical assets including source code repositories, financial systems, and customer data platforms; Tier 2 (30%) addresses important developer endpoints and infrastructure; Tier 3 (10%) maintains baseline security for public facing assets. By anchoring investment decisions to quantified risk values, mySymptoms ensures each dollar of cybersecurity spending directly mitigates the most consequential threats.

1. Threat Asset Matrix

The Threat Asset Matrix evaluates organizational assets across four risk dimensions: Confidentiality, Integrity, Availability, and Theft/Fraud. Risk scores are calculated using the formula $R = P \times C$, where P represents the probability of compromise (1-3 scale) and C represents the consequence severity (1-3 scale). Scores range from 1 (minimal risk) to 9 (critical risk).

Developer MACs (Software, code, credentials)

Risk Dimension	Score	Calculation	Rationale
Confidentiality	6	P=2, C=3	Loss or theft could expose proprietary code and credentials
Integrity	4	P=2, C=2	Unauthorized modifications could insert malicious code
Availability	3	P=1, C=3	Device failure or ransomware may delay development
Theft/Fraud	5	P=2, C=2-3	Theft could lead to credential resale or IP loss

Developer iPhones (Email, credentials, test builds)

Risk Dimension	Score	Calculation	Rationale
Confidentiality	2	P=1, C=2	Limited data exposure if lost; MDM reduces risk
Integrity	3	P=1, C=3	Spoofed messages could damage internal trust
Availability	4	P=2, C=2	Device loss impacts testing and communication
Theft/Fraud	3	P=1, C=2	Medium risk of impersonation or data resale

Rackspace Website (Web hosting, public content)

Risk Dimension	Score	Calculation	Rationale
Confidentiality	1	P=1, C=1	Public-facing, low confidentiality requirement
Integrity	4	P=2, C=2	Website defacement could harm reputation
Availability	5	P=2, C=3	DDoS attacks could cause significant downtime
Theft/Fraud	3	P=1, C=2	Low theft risk but possible phishing exploitation

Git Cloud Storage (Production software) - CRITICAL

Risk Dimension	Score	Calculation	Rationale
Confidentiality	9	P=3, C=3	Core intellectual property and algorithms exposed if compromised
Integrity	9	P=3, C=3	Code corruption or injection of malware poses critical risk
Availability	6	P=2, C=3	Service downtime delays patches and releases
Theft/Fraud	8	P=2-3, C=3	Source code theft could damage competitiveness

ADP Payroll (Employee PII, salaries) - CRITICAL

Risk Dimension	Score	Calculation	Rationale
Confidentiality	8	P=2-3, C=3	Sensitive employee financial data exposure
Integrity	6	P=2, C=3	Tampering could alter pay or tax information
Availability	4	P=1, C=3	Downtime delays payroll cycles
Theft/Fraud	9	P=3, C=3	High fraud potential (identity or financial theft)

Office 365 (Email, documents) - CRITICAL

Risk Dimension	Score	Calculation	Rationale
Confidentiality	7	P=2, C=3	Compromised accounts leak sensitive correspondence
Integrity	6	P=2, C=3	Tampered files could misinform executives or partners
Availability	5	P=2, C=2-3	Account lockout affects daily operations
Theft/Fraud	7	P=2, C=3	Phishing or impersonation could result in fund diversion

Wells Fargo Bank (Corporate accounts) - CRITICAL

Risk Dimension	Score	Calculation	Rationale
Confidentiality	9	P=3, C=3	Account credentials expose financial data
Integrity	7	P=2, C=3	Altered transaction records cause reporting discrepancies
Availability	6	P=2, C=3	Bank downtime halts vendor and payroll payments
Theft/Fraud	9	P=3, C=3	Direct theft via fraudulent wire transfers

Salesforce (CRM, customer data) - CRITICAL

Risk Dimension	Score	Calculation	Rationale
Confidentiality	8	P=2-3, C=3	Customer data exposure breaches privacy laws
Integrity	7	P=2, C=2-3	Modified client data harms business reliability
Availability	5	P=2, C=2-3	Outage disrupts customer support and sales
Theft/Fraud	8	P=2-3, C=3	Data theft could fuel identity fraud or phishing attacks

Risk Scoring Methodology: Probability (P) scores trend to "2" where credible attack paths exist despite controls. Consequence (C) scores reach "3" wherever compromise touches regulated data or could propagate to customers. The resulting risk focus emphasizes Git/CI supply chain, Office 365, payroll fraud prevention, and CRM hardening, supported by MFA everywhere, hardware keys for finance, secret scanning, SSO with conditional access, least privilege roles, and tested incident playbooks.

2. Security Investment Strategy

Every organization faces resource constraints when developing a cybersecurity budget. To maximize impact, mySymptoms' security spending focuses on assets whose compromise would produce the greatest operational, financial, or reputational damage.

Based on the Threat Asset Matrix risk estimates, three priority tiers emerge:

Priority Tier	Risk Level	Budget Allocation	Key Assets
Tier 1 - Critical	$R \geq 6$	60%	Git, Wells Fargo, ADP, Office 365, Salesforce
Tier 2 - Important	R = 3-4	30%	Developer MACs, Rackspace, Developer iPhones
Tier 3 - Controlled	$R \leq 2$	10%	Public facing websites, low sensitivity assets

Tier 1: Critical Assets (60% Budget Allocation)

Git Cloud Storage ranks at the top because it holds the company's source code and proprietary algorithms that define mySymptoms' competitive edge. Investment priorities:

- Repository access controls with role based permissions
- Automated secret scanning to prevent credential exposure
- Code signing pipelines for integrity verification
- Dependency security auditing with automated vulnerability detection

Wells Fargo Bank & ADP Payroll involve real monetary assets and employee PII. Investment priorities:

- Multi factor authentication (MFA) with hardware security keys
- Transaction approval workflows with dual authorization
- Strict access segregation for finance and HR personnel
- Real time fraud detection and alerting

Office 365 serves as the primary communication platform. Investment priorities:

- Advanced threat protection (ATP) for email security
- Quarterly phishing simulations and user awareness training
- Data loss prevention (DLP) policies
- Email authentication (SPF, DKIM, DMARC)

Salesforce stores customer contact details and engagement records. Investment priorities:

- Role based access control (RBAC) with least privilege principle
- Strong API security with OAuth 2.0 and token management
- Periodic third party security audits of configurations
- Data encryption at rest and in transit

Tier 2: Important Assets (30% Budget Allocation)

Developer endpoints and infrastructure form the second tier. While important, the likelihood or impact of compromise is comparatively lower. Investment priorities:

- Endpoint detection and response (EDR) on all developer laptops
- Mobile device management (MDM) for company iPhones with remote wipe capability
- Web application firewalls (WAF) for Rackspace
- DDoS mitigation services for public facing websites

Tier 3: Controlled Assets (10% Budget Allocation)

Assets in this tier have low inherent sensitivity or external exposure. Investment priorities:

- Routine monitoring and log collection
- Regular patch management and updates
- Automated backups and disaster recovery testing
- Content integrity monitoring for public websites

3. Incident Prevention Strategy

The 2025 data breach at mySymptoms exposed weaknesses in cloud infrastructure and dependency management. The following investment strategy addresses these vulnerabilities while strengthening the organization's overall security posture across people, processes, and technology:

3.1 Cloud and Application Security

- **Automated Patch Management:** Implement GitHub Dependabot to identify and remediate vulnerabilities in third party libraries before exploitation
- **Zero Trust Architecture:** Require authentication and authorization for every user, device, and application before accessing any system, reducing lateral movement opportunities
- **Enhanced WAF:** Deploy advanced web application firewall with real time traffic monitoring to block intrusion attempts
- **Continuous Vulnerability Scanning:** Automated security testing of all code dependencies and infrastructure components

3.2 Data Protection and Privacy

- **Encryption Standards:** AES-256 encryption for all databases at rest and in transit
- **Data Tokenization:** Replace PII with tokens to limit exposure even if breach occurs
- **Key Rotation Policies:** Regular cryptographic key rotation to reduce long term exposure
- **Data Minimization:** Collect only necessary information for application functionality
- **Automated Classification:** Tools to label and protect data based on sensitivity levels
- **Regulatory Compliance:** Adopt NIST Cybersecurity Framework and maintain HIPAA alignment

3.3 Continuous Monitoring and Incident Response

- **24/7 Security Operations Center (SOC):** Real time monitoring of threats across all assets including cloud storage, developer endpoints, and network infrastructure
- **SIEM System:** Security Information and Event Management system to collect and correlate logs from every service, enabling faster anomaly detection
- **Reduced MTTD:** Decrease mean time to detection through automated alerting and correlation
- **Formal Incident Response Plan:** Predefined playbooks for common attack types (phishing, DDoS, data exfiltration)
- **Regular Tabletop Exercises:** Quarterly simulations to test response procedures and employee readiness

3.4 Human and Vendor Security

- **Cybersecurity Awareness Training**: Quarterly training sessions for all employees covering current threats
- **Phishing Simulations:** Regular testing to measure employee readiness and identify training needs
- **Third Party Risk Management:** Vendor security assessments requiring strict compliance standards before integration

- **Supply Chain Security:** Enhanced due diligence for all third party software components and services
- **Vendor Monitoring:** Continuous assessment of vendor security posture and breach notifications

4. Conclusion

Through a balanced investment strategy that targets vulnerabilities across technology, data management, monitoring, and human behavior, mySymptoms will drastically reduce the likelihood of another major breach. By allocating 60% of the security budget to critical assets (source code, financial systems, customer data), 30% to important infrastructure, and 10% to controlled assets, the organization ensures that every security dollar directly addresses the highest priority risks.

The comprehensive approach addresses the root cause of the 2025 breach (unpatched third party vulnerabilities) while building resilience across the entire security ecosystem. These proactive investments not only safeguard the company's intellectual property and user trust but also demonstrate a long term commitment to cybersecurity excellence, transforming the lessons of a single incident into the foundation of a resilient, security conscious organization.

By anchoring investment decisions to quantified risk values in the Threat Asset Matrix, mySymptoms ensures that cybersecurity spending is strategic, data driven, and aligned with business priorities. This framework provides transparency, accountability, and a clear path toward continuous security improvement.