mySymptoms Health App

Cybersecurity Breach & Incident Response

Security Case Study

Stephanie (Seeyeon) Oh

1. Organization Overview

In today's digital age, people turn to the internet for everything, including their health concerns. Yet, when most people type their symptoms into a search bar, they are met with overwhelming and often exaggerated information that only increases anxiety. mySymptoms is a mobile application designed to change that experience. As a health awareness platform, mySymptoms analyzes user symptoms and provides a ranked list of possible conditions, each accompanied by a percentage showing how likely the illness might be based on the provided information.

The app was inspired by a common problem: people naturally seek reassurance when they feel unwell, but online searches tend to produce alarming results that can lead to stress and misinformation. mySymptoms offers a balanced alternative by combining accessible technology with evidence based insights, helping users take control of their well being by providing structured information and gentle guidance toward professional care when needed.

Key Features:

- **User Registration:** Users enter basic personal information (name, age, sex, ethnicity, medical conditions) to personalize results
- **Symptom Input:** Users can type symptoms or select from a visual list, rating severity on a 1-10 scale
- **Condition Analysis:** The system generates the top 5 potential illnesses ranked by likelihood percentage
- **Educational Resources:** Each condition includes links to peer reviewed articles and reliable sources
- **Medication & Vitamin Suggestions:** Over the counter medication recommendations with pricing and vitamin suggestions
- **Location Services:** "Search near me" feature to identify nearby pharmacies and clinics
- **Saved Results:** Users can revisit previous analyses in their "Saved" tab
- **Account Management:** Personal and health profile data stored in "Account" tab

All information pages include clear disclaimers reminding users to consult licensed healthcare professionals if their symptoms worsen or persist. Ultimately, mySymptoms aims to reduce health related anxiety and empower users with accurate, organized, and accessible information, transforming confusion into clarity and worry into awareness.

2. Cybersecurity Incident Description

Incident Date: October 24, 2025
Classification: High Severity Data Breach
Impact: Approximately 1.4 million registered users worldwide

Incident Timeline & Attack Vector:
On October 24, 2025, mySymptoms experienced a major cybersecurity incident that compromised sensitive user data. The breach was discovered when unusual outbound network traffic was detected from one of the company's cloud storage servers hosted on AWS. Within minutes, the security monitoring

system triggered multiple alerts indicating unauthorized access attempts to an internal API used for user authentication.

Investigation revealed that attackers had exploited an **unpatched vulnerability in a third party library** used by the web application firewall. This exploit granted the intruders limited administrative privileges, allowing them to query portions of the user database over a span of two hours before automated systems began suppressing outbound traffic.

Data Compromised:

Data Type	Status	Volume
Usernames	Exposed	~1.4M records
Email Addresses	Exposed	~1.4M records
Ages & Ethnicities	Exposed	~1.4M records
Medical Symptom Histories	Encrypted (AES-256)	~5GB extracted
Passwords	Encrypted (AES-256)	Not compromised

Attack Attribution:
Forensic analysis traced the breach to a coordinated group operating through several proxy networks across Europe. The attack appeared to be targeted and deliberate, with approximately 5GB of encrypted data exfiltrated during the two hour window.

3. Incident Response & Containment

Immediate Actions (Within 2 Hours):

- All affected servers were immediately isolated from the network
- User sessions were terminated across all platforms
- New firewall rules deployed to block malicious IP addresses
- Automated systems suppressed outbound traffic
- Internal incident response team activated containment protocol

Investigation Phase (Days 1-7):

- **Collaboration Partners:** AWS Security, independent cybersecurity consultants, and local law enforcement cybercrime units
- **Forensic Analysis:** Complete examination of access logs, network traffic, and compromised systems
- **Root Cause Identification:** Unpatched third party library vulnerability in web application firewall
- **Data Assessment:** Confirmed 5GB of encrypted data exfiltrated, no confirmed misuse of data reported

User Communication (Within 48 Hours):

All 1.4 million affected users were notified via email and in app alert about the breach, along with instructions to reset their passwords and review recent account activity. The company communicated transparently with users, regulators, and the media throughout the incident response process.
FCFS implements a simple non preemptive scheduling policy where processes are executed in the order they arrive in the ready queue. The algorithm provides a baseline for comparison but may suffer from the convoy effect when long processes monopolize the CPU.

4. Post Incident Security Enhancements

Following containment and investigation, mySymptoms implemented comprehensive security measures to prevent future incidents and restore public trust:

Security Area	Implementation	Impact
Architecture	Zero trust network architecture deployment	Eliminates implicit trust. Every access requires verification.
Authentication	Mandatory MFA for all accounts	Significantly reduces account takeover risk
Vulnerability Management	Continuous vulnerability scanning of all code dependencies	Proactive identification of security flaws
Monitoring	Security Operations Center (SOC) with 24/7 monitoring	Real time threat detection and response
Testing	Regular penetration testing by external security firms	Identifies weaknesses before attackers do
Training	Expanded cybersecurity awareness training for all employees	Reduces human error and social engineering risk
Patch Management	Automated dependency monitoring	Ensures timely patching of vulnerabilities

Lessons Learned:
While the breach was contained quickly and no confirmed misuse of data was reported, the event revealed the critical importance of proactive defense and dependency management. This incident served as a defining moment for mySymptoms, transforming it into a company that not only educates users with health awareness but also leads by example in cybersecurity resilience.

The company's transparent communication, swift response, and comprehensive security upgrades demonstrated a commitment to protecting user data and maintaining trust. By investing heavily in security infrastructure, monitoring capabilities, and employee training, mySymptoms has positioned itself as a security conscious organization in the healthcare technology sector.