California State University, Sacramento

Cybersecurity: Risk and Strategy Assessment

MindfulTech

Braulio Montoya, Yin Lor, Rehemet Negus, Ruth Brooks, Sana Asghar, Trung Pham

MIS 170

Professor Aivazpour

12/07/2025

Table of Contents

Introduction

Mindful Tech is an innovative and rapidly growing SaaS startup focused on the mental wellness space. The platform (app) offers personalized meditation, stress management exercises, and telehealth connectivity between users and licensed therapists.

The Security Challenge: As Mindful Tech scales up, culture must evolve to fast securely. The current use of cryptography and secure communication is ad-hoc. Lacking a standardized, in-house strategy for encrypting data both in transit and at rest, exposing to significant compliance and reputational risk.

Responses to the Questions (Part I)

1. Identity & Access Management (IAM)

- **How should the organization handle user authentication and authorization?**

Mindful Tech must adopt strong layered authentication and authorization controls to protect its highly sensitive data and microservices-based SaaS platform. Authentication should rely on strong passwords, multi-factor authentication for employees, such as therapies and administrators. It should also incorporate Single Sign-On using SAML or OAuth to centralize identity verification. Adaptive authentication measures like geolocation should be implemented to detect suspicion login activity. With OpenSSL securing all TLS connections, credentials and MFA codes will be encrypted in transit to prevent interception. For Authorization, Mindful Tech should implement Role-Based Access Control for the most sensitive PHI. This hybrid approach ensures each user only accesses the minimum data necessary for their role, maintaining strong privacy protections in a mental-health environment.

- **What IAM policies should be implemented (e.g., Role-Based Access Control, Multi-Factor Authentication)?**

Mindful Tech should implement a comprehensive set of IAM policies to ensure secure and appropriate access to its systems and sensitive mental health data. A Role-Based Access Control policy should assign each user a single primary role with only the minimum privileges required. This means that therapists may access client notes but not system back-end functions. Multi Factor Authentications must be mandatory for all internal users and therapists.They must use combinations such as passwords with TOTP apps, SMS one-time codes or mobile biometrics to provide a strong second layer of defense against account compromise. A strict password and credential policy should require passwords of at least 12 characters, block commonly used or predictable passwords, prohibit reuse and ensure all credentials are encrypted. An Access Review Policy should mandate quarterly access audits,immediate deactivation of accounts during offboarding and automatic session timeouts after periods of inactivity to reduce risk of unauthorized access.

- **What are the best practices for managing privileged accounts?**

Managing privileged accounts at Mindful Tech requires strict controls due to their elevated access to sensitive systems and PHI. Following the principle of least privilege, administrators should be granted only specific permissions necessary for their duties. Each admin must maintain two separate accounts. A regular account for everyday tasks and a privileged account for administrative functions. This is to ensure stronger accountability and clearer audit trails. All privileged access should require Multi-Factor Authentications and sensitive administrative operations must be performed only form secure Privileged Access Workstations. All administrator actions should be thoroughly logged and regularly reviewed which aligns with IAM accountability and auditing principles. Mindful Tech should also adopt Just-In-Time privileged access so elevated permissions are granted only temporarily when needed and shared administrator accounts should be prohibited to ensure every privileged action can be traced back to a unique individual.

- **How can IAM improve regulatory compliance in the chosen industry?**

IAM helps Mindful Tech meet regulatory requirements under both HIPAA and GDPR by controlling who can access sensitive mental-health information. Under HIPAA, IAM supports key Administrative and Technical Safeguards by enforcing unique user identification, implementing access control through RBAC and ABAC failed login and maintaining audit logs. It also tracks failed login attempts and requires strong authentication mechanisms such as MFA. For GDPR, IAM contributes to compliance by ensuring data minimization through role-based restrictions. This provides access transparency via comprehensive audit trails. This ultimately reduces likelihood of security incidents through strong authentication and continuous monitoring to protect user privacy. When combined with OpenSSLs encryptions, IAM further strengthens Mindful Tech's Security by ensuring all data is encrypted in transit while access to encrypted information remains strictly controlled. These measures provide a comprehensive framework that enables Mindful Tech to meet industry regulatory expectations and maintain protection for user data.

2. Cryptography & Data Protection

- **How should the organization protect sensitive data at rest, in transit, and in use?**

Mindful Tech must implement a layered cryptography strategy to protect patient data across all stages of storage and processing. Data that is at rest should be encrypted using full-disk encryption and database-level encryption, such as AES-256, to make sure that even if it is compromised in cloud storage or endpoints, stored user information still remains unreadable.. Data that are in transit must always be protected using TLS 1.3 with strong ciphers to maintain secure communications between users, therapists, and backend API servers. This will prevent man-in-the-middle attacks during telehealth sessions, login requests, and data synchronization. Data in use, which is the most vulnerable state, should be protected using secure memory handling, role-based access controls, and encrypted application-layer tokens so data that are exposed in RAM or during any active processing can't be accessed by any unauthorized processes or employees.

- **What encryption methods (e.g., AES, RSA) and hashing techniques (SHA-256, bcrypt) are most relevant?**

Mindful Tech must implement industry level encryption methods that align with HIPPA, GDPR, and NIST proposals. AES-256 is the best choice for encrypting sensitive data that is at rest such as therapy notes, telehealth metadata, and user records, because it can provide strong symmetric encryption and is fully supported by OpenSSL. For protecting encryption keys and establishing secure communication channels, RSA-2048 or RSA-4096 should be used for generating certificates, key exchange, and digital signatures within TLS. Passwords must never be encrypted but should be stored using slow salted hashing algorithms such as bcrypt, PBKDF2, or Argon2, which will resist password-cracking attempts even when a breach occurs. SHA=256 remains relevant for integrity verification and digital signature, but not for storing passwords. With the combination of these techniques it creates a strong cryptographic foundation..

- **How does cryptography help in securing passwords, databases, and communications?**

Cryptography secures Mindful Tech's platform by protecting all sensitive information across authentication, storage, and communication processes. Passwords will be safeguarded through salted hashing with algorithms like bycrpt or Argon2, making it extremely difficult for attackers to recover plaintext passwords even if they obtain the hashed database. Databases containing PHI, therapy notes, and user profile information should be encrypted using AES-256, supported by OpenSSL-managed key storage to keep data unreadable to unauthorized users. Communication between clients, therapists, and backend servers is protected using TLS 1.3, which encrypts all traffic and prevents eavesdropping, replay attacks, and man-in-the-middle attacks, By using OpenSSL to manage certificates, negotiate secure ciphers, and enforce strong encryption.

- **What are the legal and regulatory requirements for data protection in this industry?**

Mindful Tech operates in the mental-health and telehealth industries, which means it must comply with several strict regulations designed to protect sensitive health information. HIPPA requires encryption for data at rest and in transit, unique user identification, strict access controls, audit logging, and immediate breach notification when PHI is exposed using AES and TLS through OpenSSL helps satisfy these technical safeguards. For users in the European Union, GDPR mandates strong encryption, data minimization, explicit consent, user data rights, and rapid breach reporting. Depending on operating regions, CCPA may also apply requiring strong protection of personal information and transparency into how data is used. In addition to legal requirements Mindful Tech should follow cybersecurity frameworks such as NIST CSF, ISO 27001, and SOC 2 Type II to strengthen governance, risk management, and documentation practices. These combined regulations and frameworks ensure that Mindful Tech protects user privacy while maintaining industry-required security standards.

3. Network Security & Threat Mitigation

- **How should the organization secure its internal and external network infrastructure?**

They can secure the internal network by having strong access control like implementing MFA. Also encrypting all traffic while regularly updating the systems and servers is important too. For the external network infrastructure the organization should deploy a firewall to filter traffic, use WAF (Web Application Firewall) , and conduct vulnerability scans often on the systems.

- **What network security measures (e.g., firewalls, VPNs, IDS/IPS) are essential for the industry?**

The network security measures essential for the industry are firewalls, VPN, DDos Protection, Network segmentation, etc. Firewalls help block unwanted traffic from entering the network, while a VPN allows for encrypted remote access for users. DDos Protection stops attackers from flooding systems and Network segmentation also limits attackers' methods of trying to get further in the network.

- **How can the organization prevent and mitigate cyber threats like DDoS, phishing, or insider threats?**

The organization can prevent/mitigate cyber threats in many ways. For phishing they can conduct employee training that teaches them about security awareness and also use email filtering tools which blocks out malicious emails. In order to prevent DDoS attacks they can use AWS Shield which is a cloud-based mitigation tool and it identifies security configuration issues. Furthermore, when it comes to insider threats the main idea is to implement the principle of least privilege access, where employees only access exactly what they need and nothing else. In addition to that, continuous monitoring and reviewing logs is important too.

- **What role does security monitoring play in network security?**

Security monitoring plays a big role in network security as it has to do with detection. This is helpful as it allows you to detect suspicious behavior, identify intruders before something serious possibly happens, monitor logs throughout the system, alert the rest of the team about the suspicious activity for further review, and overall tracking activity which would help prevent data breaches. The tools that are commonly used are SIEM tools and this is what you would use to collect and analyze logs. SOC analysts also monitor the systems 24/7 to ensure everything is secure.

4. Risk Assessment & Compliance Strategy

- **What are the biggest cybersecurity risks for the chosen industry?**

Mindful Tech works in the mental health and telehealth fields, which means it has to deal with a lot of very private health and personal information. Because of this, the main cybersecurity threats are data breaches, unprotected communication channels, and misconfigured cloud systems that could expose protected health information (PHI). The company's existing encryption procedures are random and not always the same, so data that is in transit or at rest could be intercepted or accessed without permission. Also, scaling up quickly makes it more likely that there may be setup errors, access controls that are too open, and systems that aren't patched. Mindful Tech also uses a number of third-party APIs, such as healthcare, authentication, and messaging systems. Any of these could pose indirect security risks. Lastly, human error is still a big danger because employees could mishandle PHI, fall for phishing attacks, or use unsafe code if there isn't a standardized training program in place.

- **What security frameworks or compliance standards (e.g., NIST, ISO 27001, GDPR, HIPAA) should be followed?**

To lower these risks, Mindful Tech should make sure that its business follows a number of important cybersecurity principles and rules. Because the platform stores PHI from therapy sessions and other health-related contacts, it must follow HIPAA rules, including the Security Rule, the Privacy Rule, and the Breach Notification Rule. If the business has European customers, it must also obey GDPR rules, including those about encryption, data minimization, user consent, and the right to be forgotten. Mindful Tech would benefit from using the NIST Cybersecurity Framework since it would give them a clear way to find, protect, find, and respond to threats.Furthermore, adherence to ISO 27001 would enhance governance, risk management, and documentation practices. Adherence to SOC 2 Type II compliance, a standard expectation for Software-as-a-Service (SaaS) providers, demonstrates the existence of comprehensive controls pertaining to security, privacy, and confidentiality. OpenSSL is a widely adopted cryptographic toolkit that directly addresses numerous encryption requirements inherent to these frameworks.

- **How should the organization train employees to improve security awareness?**

To build a strong cybersecurity culture at Mindful Tech, employees also need to be more aware of security issues. All new hires must go through onboarding training. This course will teach you how to handle Protected Health Information (PHI) correctly, the basics of HIPAA, how to spot phishing scams, the best ways to keep your passwords safe, and, for those who work in technical roles, how to write secure code. There should be regular revision meetings to go over important ideas, spot new threats, and make sure that staff members are up to date on changes to policies and procedures. Periodic phishing tests help determine how ready employees are and find people who need further training. Training programs should be tailored to each person's job. For example, developers should learn how to make secure application programming interfaces and encrypt data with OpenSSL, while support staff should learn how to handle data safely. DevOps engineers should learn how to manage secrets and make systems more secure. Mindful Tech might create a workplace where employees feel comfortable asking questions, reporting strange behavior, and making security a top priority in their daily tasks. Documentation that is easy to find should be made available to make these tasks easier. This should include things like rules on how to use the system, how to log in, and how to respond to incidents.

5. Incident Response & Disaster Recovery

- **What should the organization's incident response plan (IRP) include?**

Mindful Tech's incident response plan should clearly outline procedures that deal with the weakness of the lack of standard encryption for sensitive user health data. Mindful Tech handles strictly regulated data under HIPAA and GDPR. Because of that, the incident response plan must have steps for finding encryption failures. The incident response plan must have steps for spotting system misconfigurations, including steps for detecting compromised communication channels and for catching unauthorized access to stored data. The IRP should include the roles and responsibilities for the security personnel, the escalation pathways, the communication protocols with the users and the regulators, and the predefined actions for isolating the systems that show signs of breach. Mindful Tech is scaling rapidly. The IRP should detail how each service that uses OpenSSL will be monitored and audited, and should detail how each individual service that uses OpenSSL will be monitored for any SSL/TLS failure. The IRP should detail how each service that uses OpenSSL will be checked for the certificates, the expired keys, or the downgraded security protocols. Additionally, the IRP should detail how any SSL/TLS failure will be quickly contained. Documentation procedures, forensic data collection, and post-incident review cycles should also be included to ensure continuous improvement of the organization's security posture.

- **What disaster recovery strategies (e.g., backups, redundancy, cloud failover) are necessary?**

Mindful Tech must keep encrypted data safe when an outage occurs and keep encrypted backups of user data. Redundant encrypted backups will protect encrypted data. Mindful Tech will use the OpenSSL framework for storage for APIs and for communication channels. Redundancy must exist at the layers of the lower levels in Mindful Tech's architecture. The system will be built so that if one service fails, another encrypted instance can take over. It is important that an encrypted instance does not expose data. As a cloud-based startup, Mindful Tech would benefit from automating cloud failover procedures to ensure encrypted TLS connections are reestablished seamlessly. Additionally, backup key stores, certificate repositories, and configuration files will be recreated to prevent Points of Failure. These measures support safety measures and drastically reduce downtime, protecting both users and the company's reputation.

- **How should the organization ensure business continuity after a security breach or system failure?**

To keep business continuity after a breach, Mindful Tech will use the platform that OpenSSL provides. Encryption will be built into every service. While an incident is being fixed, encryption will occur to let a user continue to work. Business continuity will occur by means of encrypted communication channels that stay functional to be quickly restored. Encrypted communication channels let users keep using telehealth and meditation services and protect data from being exposed. The company should activate redundant systems, deploy secure backup servers, and replace TLS keys and certificates as needed to neutralize vulnerabilities. Since compliance is central to Mindful Tech's mission, continuity efforts must include transparent communication procedures for notifying users, regulators, and partners in a way that demonstrates responsible data handling. Finally, continuous monitoring and automated deployment will be used. This will re-establish secure services quickly to ensure that operations can continue with minimal disruption.

- **What are the best practices for cybersecurity awareness training to improve incident response?**

Cybersecurity awareness training will help Mindful Tech's employees see why encryption is essential. To protect mental wellness data and telehealth data. The training must make sure every employee—including developers, support staff, and product managers—knows how SSL/TLS works, how OpenSSL fits into the system, and what signs show encryption failures or suspicious system behavior. Staff should be trained to recognize phishing attempts, insecure data handling practices, and improper storage of keys or certificates, which are common errors. Just as important, the training should reinforce the cultural shift toward "secure growth" that Mindful Tech needs as it scales, encouraging developers to integrate security checks into the system. To incorporate this shift in mindset at Mindful Tech, regular refresher sessions, simulated incident drills, and education on HIPAA responsibilities occur periodically. This will help employees respond more quickly and confidently when real incidents occur.

Introducing the Cybersecurity Tool (Part II)

OpenSSL is an open-source software library that provides a robust implementation of SSL and TLS protocols. It includes a powerful set of cryptographic tools for encrypting and decrypting data, generating keys, and managing digital certificates. Developed in the 1990s, OpenSSL has become one of the most widely used encryption libraries in the world.

Key Features: Cryptographic Functions: OpenSSL supports a range of cryptographic algorithms, including AES, RSA, SHA and ECC, enabling encryption, decryption, hashing and digital signatures. Certificate Management: Allowing users to generate and manage digital certificates, Certificate Signing Requests (CSRs), and private/plublic keys. Command-Line Utility: The command-line tool built in Openssl provides options for testing SSL/TLS configurations, converting certificates formats, verifying certificates and debugging network connections. Functionality: OpenSSL serves as both a library and a toolset. As a library, it allows developers to embed cryptographic functionality directly into software applications. As a tool, it provides an interface performing tasks like creating self-signed certificates and testing SSL connections, verifies certificate chains and encrypts and decrypts files. It supports generation of random numbers, password hashing, and digital signature verification.

Demonstration Description

In this demonstration Mindful Tech aims to securely relay a confidential note from a doctor to an authorized personnel. To ensure the privacy of the information, the doctor's message will be encrypted using OpenSSL. This encryption guarantees that only the authorized recipient, who also knows the password, can decrypt and read the message. This is also in line with Kerckhoffs's Law, that the system security relies on secrecy of the password rather than the secret of the encryption method itself. This ensures that the sensitive data is protected.

Conclusions

Mindful Tech is a rapidly growing company in the telehealth industry, which means they handle sensitive PHI. The company dances major cybersecurity risks that can directly threaten the confidentiality , integrity and availability of user data. To address these issues, we proposed the use of OpenSSL as the foundational tool for encryption across all services. OpenSSL was chosen because it is reliable and provides industry-standard cryptography. Many of OpenSSL benefits include secure SSL/TLS encryption for data in transit, strong key and certificate management. It is compatible with HIPPA, ISO 27001, SOC 2 and NIST requirements. By adopting OPenSSL, Mindful Tech reduces the risk of data exposure during communication and storage.

References

Department of Health and Human Services. Guidance on Risk Analysis. HHS.gov, 26 Sept.2025, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

"OpenSSL." F5 Glossary, F5, https://www.f5.com/glossary/openssl

National Institute of Standards and Technology. Recommendation for Password-Based Key Derivation, Part 1: Storage Applications (SP 800-132), 2010, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf

Rescorla, Eric. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, Internet Engineering Task Force, Aug. 2018, https://datatracker.ietf.org/doc/html/rfc8446

Student Evaluation Form

Name of student	Meeting date (present/ absent)	Task (completed/ incomplete)	Other notes
Yin Lor	11/11 Tuesday @2pm - Present 11/31 Monday @2pm - Present	- Create Part 1 response presentation slides - Submit all deliverables	- Work on summarizing the key points and importing into the presentation for part 1. - Work on Part 2 video tool demo. - Work on Report.
Braulio Montoya	11/11 Tuesday @2pm - Present 11/31 Monday @2pm - Present	- Part 1: Identity & Access Management (IAM) - Support Part 2 tool description	- Work on assigned task - Braulio will work/support on Part 2 tool introduction / description
Trung Pham	11/11 Tuesday @2pm - Present 11/31 Monday @2pm - Present	- Part 1: Cryptography & Data Protection	- Work on assigned task - Rehearse slide
Ruth Brooks	11/11 Tuesday @2pm - Present 11/31 Monday @2pm - Present	- Part 1: Incident Response & Disaster Recovery	- Work on assigned task - Rehearse slide
Sana Asghar,	11/11 Tuesday @2pm - Present 11/31 Monday @2pm - Present	- Part 1: Network Security & Threat Mitigation	- Work on assigned task - Rehearse slide
Rehemet Negus,	11/11 Tuesday @2pm - Present 11/31 Monday @2pm - Present	- Part 1: Risk Assessment & Compliance Strategy	- Work on assigned task - Rehearse slide