Group 2: Modeling a Cybersecurity Strategy Framework

Members:

Amanda Huang

Zhixuan Shen

Xiaoyang Wei

Shoujie Yang

Shuo Guan

Client:

Magellan Health

Sponsor:

Tom Britt, Chief Information Officer

Lane Sullivan, SVP, Chief Information Security Officer

Outline

1. Introduction
    - 1.1. Who we are
    - 1.2. Target Client: Y-GWASH Inc.
2. Identified Cybersecurity Risks and Threat Landscape
    - 2.1. What is Cybersecurity?
    - 2.2. What problem does it solve?
    - 2.3. Why is Cybersecurity important for a Healthcare company?
    - 2.4. What Threats and Risks are there?
    - 2.5. How many cybersecurity incidents have happened in the healthcare industry?
    - 2.6. How much investment in cybersecurity is there currently in the healthcare industry?
3. Regulations for Healthcare Industries
    - 3.1. Regulations
        - 3.1.1. National Institute of Standards and Technology (NIST)
        - 3.1.2. International Organization for Standardization (ISO)
        - 3.1.3. Health Insurance Portability and Accountability (HIPAA)
        - 3.1.4. Cybersecurity Framework (CSF)
        - 3.1.5. Center for Internet Security (CIS)
4. Our Cybersecurity Framework
    - 4.1. Framework Architecture
    - 4.2. Components
        - 4.2.1. Cryptography/ Key Management
        - 4.2.2. Asset Management
        - 4.2.3. Human Training
        - 4.2.4. Security Controls
        - 4.2.5. Third-party Relationships
        - 4.2.6. Monitoring/ Audit logging
        - 4.2.7. Business Continuity Management
        - 4.2.8. Access Control
        - 4.2.9. Compliance
        - 4.2.10. Data Lifecycle
        - 4.2.11. Physical and Environmental Security
        - 4.2.12. Risk Management
5. Cost-Benefits
6. Summary
7. Reference

1. Introduction

1.1. Who we are

We, standing in the role of the consultancy, are here to help clients in healthcare industries to build a robust cybersecurity framework. Our vision is to create a framework that is available to fit the general cybersecurity needs of healthcare companies. Our background in Operational Excellence, IT Architecture and Infrastructure, IT Governance and Risk Management, Enterprise Data Management, and Cybersecurity allows us to be the best choice for our clients.

1.2. Target Client: Y-GWASH Inc.

Our client, Y-GWASH (Your Global Welfare and Social Health Inc.), operates as a mid-sized company that specializes in offering services for family clinics and online consultations. While they have a foundational IT infrastructure in place, encompassing network, database systems, and general IT systems, a notable gap exists in the absence of established cybersecurity procedures. This oversight poses a potential risk of serious cybersecurity issues. Therefore, we are here to provide guidance on implementing a robust cybersecurity framework to proactively address and mitigate potential problems.

2. Identified Cybersecurity Risks and Threat Landscape

2.1. What is cybersecurity?

Cybersecurity protects computer systems, networks, and digital data from being stolen, corrupted, or accessed by unauthorized individuals. It includes various technologies, processes, and practices aimed at safeguarding information technology assets and ensuring that data is kept confidential, intact, and available.

2.2. What problem does it solve?

Cybersecurity acts as the guard against unauthorized access to sensitive data. It involves safeguarding internet-connected devices and services against malicious attacks created by hackers, spammers, and cybercriminals. Organizations employ this practice to shield themselves from various threats, including phishing schemes, ransomware attacks, identity theft, data breaches, and financial losses.

2.3. Why is Cybersecurity important for a Healthcare company?

In the realm of a healthcare company, cybersecurity assumes an unparalleled level of significance, transcending mere considerations of business continuity to emerge as an ethical imperative. The imperative nature of cybersecurity is underscored by a multitude of reasons:

1. **Patient Data Protection:** Healthcare institutions harbor vast repositories of personal and medical information. The stakes are profound, as a breach in data security can unleash a cascade of repercussions, ranging from identity theft and financial fraud to the unauthorized disclosure of sensitive medical histories. The failure to safeguard these critical data not only jeopardizes individual privacy but precipitates an erosion of trust, imperiling the very foundation of the healthcare business.
2. **Medical Device Security:** The contemporary healthcare landscape heavily relies on interconnected medical devices, such as pacemakers, infusion pumps, and imaging devices. The vulnerability of these devices to cyber-based attacks introduces a disconcerting prospect — the potential disruption of vital equipment. Such attacks pose direct and immediate threats to patients' health and safety, accentuating the indispensable role of cybersecurity in ensuring the integrity of medical services.
3. **Operational Continuity:** Cyberattacks wield the capacity to undermine or outright crash hospital operations, precipitating a domino effect of consequences, including appointment cancellations, delays in medication dispensing, and the postponement of critical surgical procedures. Particularly in exigent circumstances, these disruptions transcend inconvenience, metamorphosing into life-threatening scenarios that underscore the indispensability of robust cybersecurity measures.
4. **Financial Implications:** The aftermath of a cyberattack extends beyond immediate health concerns, permeating into the realm of significant financial ramifications. Operational disruptions and potential legal liabilities can plunge a healthcare company into a precarious financial state, amplifying the imperative for a fortified cybersecurity posture as a safeguard against both health and financial crises.
5. **Regulatory Compliance:** Stringent legal mandates oblige healthcare providers to fortify the bulwarks of patient data protection. A breach or lapse in cybersecurity not

only jeopardizes patient confidentiality but also exposes the organization to substantial fines and legal consequences. The inextricable link between cybersecurity and regulatory compliance underscores the non-negotiable necessity for robust defense mechanisms within the healthcare sector.

2.4. What Threats and Risks are there?

There are several key threats that are common to encounter for all businesses, especially for the healthcare industry. Threats like (Checkpoint, 2022):

- **Data breaches:** Healthcare organizations house extensive sensitive information about patients and research. Attackers frequently target healthcare organizations with the aim of stealing valuable data.
- **Ransomware attack:** Healthcare organizations heavily rely on their data and interconnected systems for providing care. Ransomware attacks can seize control of these systems, demanding compliance with the attacker's terms for their release. According to an analysis (Kost, E., 2023) conducted last year, ransomware attacks pose an escalating threat to healthcare providers. In 2020, over one-third of healthcare organizations worldwide experienced the impact of a ransomware attack.
- **Phishing:** Phishing attacks aim to deceive recipients into divulging sensitive information or infecting their systems with malware. This deceptive tactic is a prevalent initial step in data breaches, ransomware, and similar cyber threats.
- **Distributed Denial of Service (DDoS):** DDoS attacks employ a network of compromised systems to overwhelm a target with excessive traffic. Similar to ransomware attacks, DDoS attackers may demand a ransom to restore an organization's normal operations.

2.5. How many cybersecurity incidents have happened in the healthcare industry?

According to the Health Insurance Portability and Accountability Act (HIPPA) Journal, the definitive source on healthcare data breach incidents, the statistics over the past fourteen years show troubling trends. The year 2021 saw a notable spike in the number of reported breaches, eclipsing all previous records that have been meticulously documented by the Office for Civil Rights (OCR) of the U.S (United States). Department of Health and Human

Services. It is important to note that these statistics only include breaches involving 500 or more records. The OCR does not disclose details of smaller breaches.

From 2009 to 2022 (Figure 1.), reports submitted to Health and Human Services (HHS) Office for Civil Rights revealed an astounding 5,150 health data breaches, each involving 500 or more records. These breaches exposed or compromised a staggering 382,262,109 protected health information's-more than 1.2 times the entire population of the United States. Examining the escalation of this crisis over time reveals a stark revelation: In 2018, there was an alarming average of one reported healthcare data breach of 500 or more records per day. By 2022, that rate is more than double, with an average of 1.94 such incidents reported every day.

Citing HealthCare Dive, the surge in reported breaches is unequivocal, soaring from just under 200 in 2010, the inaugural year of available data, to an astonishing 700 in 2022, representing a more than threefold increase. The human toll is equally staggering, with over 52 million individuals falling victim to compromised private health information across these breaches in 2022, a stark contrast to the approximately 6 million people affected in 2010 (Han, J. Y., & Liss , S., 2023).

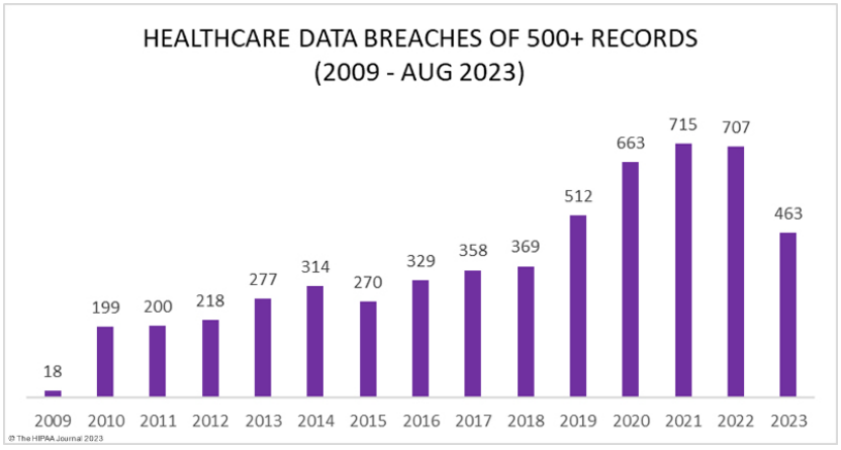

Figure 1. Healthcare data breaches (2009 to 2023 August) (HIPPA)

2.6. How much investment in cybersecurity is there currently in the healthcare industry?

In 2022, the global healthcare cybersecurity market will reach $14.7 billion and is expected to grow at an 18.4% compound annual growth rate (CAGR) from 2023 to 2030

(Figure 2.). A confluence of factors, which collectively underscore the imperative of cybersecurity measures in the healthcare sector, is driving this remarkable growth.

The escalating frequency of cyberattacks, which is forcing healthcare organizations to bolster their defenses against sophisticated threats, is a key driver of this market surge. As cyberthreats proliferate and privacy and security concerns grow, healthcare organizations are responding proactively to protect sensitive data and ensure patient information integrity.

As healthcare organizations strive to stay ahead of evolving threats and effectively secure their digital infrastructure, the burgeoning adoption of advanced cybersecurity solutions is a key catalyst. This is not only a response to current challenges, but also a strategic investment in the future to protect against the constantly evolving cyberthreat landscape.

In addition, the cybersecurity market is being driven by the healthcare industry's increasing reliance on cloud-based solutions. The adoption of cloud-based technologies presents both opportunities and challenges, requiring robust security measures to ensure the confidentiality, integrity, and availability of patient data stored and processed in the Cloud.

A major contributor to market growth is the proliferation of connected devices and smartphones in healthcare practices. The need for comprehensive cybersecurity measures to protect against potential vulnerabilities and breaches is paramount, as these devices become an integral part of patient care and medical processes.

Additionally, the emergence of 5G technology adds another dimension to the landscape, providing increased connectivity and speed while introducing new cybersecurity considerations. In order to mitigate potential risks and ensure the seamless integration of this transformative technology, the adoption of 5G in the healthcare industry requires a proactive security approach.

In conclusion, the industry's response to the escalating challenges posed by cyber threats is closely linked to the projected growth of the global healthcare cybersecurity market. A confluence of factors-increased cyber-attacks, growing privacy and security concerns, adoption of advanced cybersecurity solutions, penetration of cloud-based solutions, proliferating connected devices and smartphones, and integration of 5G

technology is reinforcing cybersecurity's critical role in protecting healthcare system integrity and safeguarding sensitive patient information.

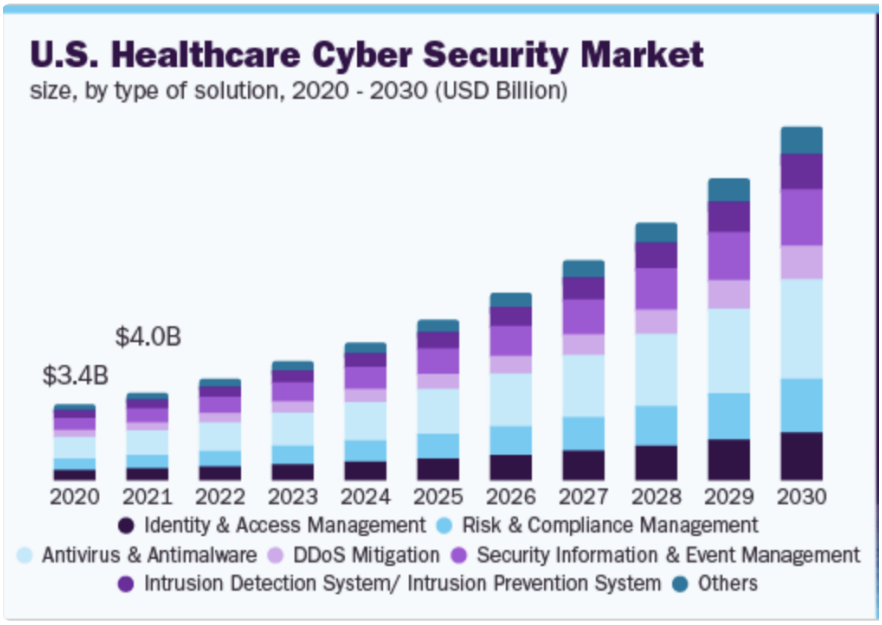

Figure 2. US healthcare cyber security market (2020 -2030) (Healthcare Cyber Security Market Size Report, 2021)

3. Regulations for Healthcare Industries

3.1. Regulations

3.1.1. National Institute of Standards and Technology (NIST)

The NIST Cybersecurity Framework is a set of guidelines and best practices designed to help organizations manage and reduce cybersecurity risk. It was developed through collaboration between industry, government, and academia and is widely recognized and adopted globally. The framework is voluntary and is intended to be adaptable to the needs of a wide range of organizations, regardless of their size or the nature of their cyber risks. The NIST Cybersecurity Framework is designed to be flexible and customizable. It can be used as a standalone framework or can be aligned with other risk management strategies and cybersecurity approaches. The framework's adaptability makes it valuable for a wide range of sectors, including critical infrastructure, government agencies, and small and medium-sized businesses.

3.1.2. International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) is a globally recognized body that develops and publishes a wide range of proprietary, industrial, and commercial standards. It is an independent, non-governmental organization made up of national standards bodies from over 160 countries. The International Organization for Standardization (ISO) has developed several standards related to cybersecurity, under the umbrella of information security management systems (ISMS). The most notable among these is the ISO/IEC 27000 series, particularly ISO/IEC 27001 and ISO/IEC 27002. Our team focuses on 27001, the leading standard for information security management systems. It provides a framework for establishing, implementing, maintaining, and continually improving an ISMS. ISO/IEC 27001 specifies requirements for assessing and treating information security risks tailored to the needs of the organization.

3.1.3. Health Insurance Portability and Accountability (HIPAA)

Health Insurance Portability and Accountability (HIPAA) is a U.S. law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other health care providers. While HIPAA itself is not a cybersecurity framework, it includes significant provisions related to the security and privacy of protected health information (PHI). HIPAA compliance is essential for covered entities not only to avoid penalties but also to ensure the trust of patients and the integrity of the healthcare system. The framework aims to balance the need for protecting patient information with the need to allow the flow of health information needed to provide high-quality health care.

3.1.4. Cybersecurity Framework (CSF)

The Cybersecurity Framework (CSF) was developed by the National Institute of Standards and Technology (NIST) in the United States. It's a voluntary framework primarily intended for critical infrastructure organizations to manage and mitigate cybersecurity risk based on existing best practices. However, it has been widely

adopted by many organizations across different sectors due to its flexibility and effectiveness. The CSF is designed to be adaptable to the needs of varying organizations, regardless of their size, degree of cybersecurity risk, or cybersecurity sophistication. The CSF is notable for its approach to balancing business needs with cybersecurity risk, focusing on outcomes rather than prescriptive measures. This flexibility allows organizations to adapt the framework according to their specific requirements, risk appetite, and technological landscape. It has become a standard reference for establishing a robust cybersecurity program in various industries and sectors.

3.1.5. Center for Internet Security (CIS)

The Center for Internet Security (CIS) is a non-profit organization that works to safeguard private and public organizations against cyber threats. Its mission is centered on leading a global community of IT professionals to continuously evolve standards and practices to protect against present and emerging cybersecurity threats. CIS is widely known for its development of the CIS Controls and CIS Benchmarks, which are globally recognized best practices for securing IT systems and data. CIS plays a crucial role in enhancing cybersecurity readiness and response among public and private sector entities. Its resources are widely used for establishing security baselines, conducting risk assessments, and implementing security best practices. The organization is instrumental in fostering a collaborative environment where experts from different fields come together to combat cybersecurity challenges.

4. Our Cybersecurity Framework

4.1. Framework Architecture

Based on the requirements of the regulations listed above, we suggest a cybersecurity framework having three aspects (Figure 1): Strategic, Managerial, Technical. Table 1. shows the components of the framework, which we extracted from the 5 regulations. The strategic aspect refers to the operations to maintain core business and continuous improvement, dedicated human resources and budget allocation. Managerial aspect refers to the operations

of data inventory, risk assessment, and outsourcing risk. The last aspect is Technical. It refers to information and security protection and control measures, disaster response, incident reporting and cyber threat assessment.

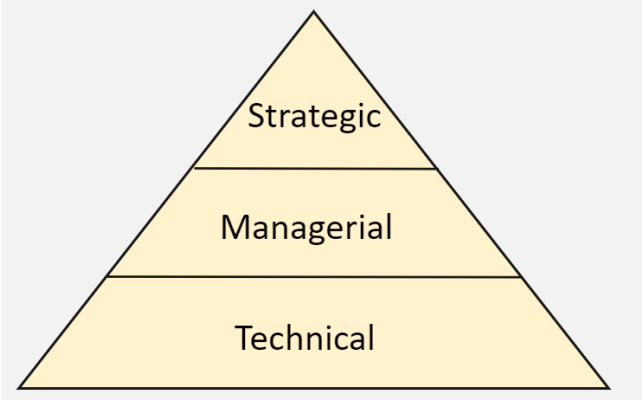

Figure 3. Our Cybersecurity Framework Architecture (Own work)

4.2. Components

In Table 1., under strategic, the standards included are Business Continuity Management, Data lifecycle, Compliance, and Human Training. This involves communicating the importance of cybersecurity throughout the organization. This helps in creating a security-conscious culture among employees, which is essential in preventing and mitigating security incidents. Under Managerial, the standards included are Asset Management, Risk Management, and Third-party Relationships. Lastly, also the button part of the framework is Technical. It is the underlying architecture and the core of the framework. The standards included are Cryptography/ Key Management, Security Controls, Physical and Environmental Security, Access Controls, and Monitoring/ Audit logging.

Table 1. Components of Our Cybersecurity Framework

Category	Standard
Strategic	Business Continuity Management
	Data lifecycle
	Compliance
	Human Training

Managerial	Asset Management
	Risk Management
	Third-party Relationships
Technical	Cryptography/ Key Management
	Security Controls
	Physical and Environmental Security
	Access Controls
	Monitoring/ Audit logging

4.2.1. Business Continuity Management (BCM)

Business continuity management refers to the strategic planning and preparation to ensure the smooth running or rapid recovery of operations following major disruptions, such as natural disasters, man-made incidents, or cybersecurity events. This planning is crucial for the resilience of business operations in the aftermath of a cyber-attack. In summary, Business Continuity Management in the context of cybersecurity is about preparing and planning for disruptions, with a focus on resilience against cyber-attacks. This involves aligning business continuity plans with cybersecurity frameworks, understanding the organization's structure and staff roles, and developing comprehensive policies and procedures to manage and mitigate the impact of cyber incidents.

4.1.1.1. Implementation

1. Leadership and Governance:

- Establish a BCM Team:
  - Form a dedicated Business Continuity Management Team comprising representatives from key departments such as IT, operations, compliance, and risk management.
- Leadership Support:
  - Gain support and commitment from senior leadership to ensure the integration of BCM into the organizational culture.

2. Risk Assessment and Business Impact Analysis (BIA):

- Conduct Risk Assessment:

- Identify and assess risks specific to the healthcare industry, considering factors such as regulatory compliance, patient care, and data security.
- Perform BIA:
  - Identify critical functions and assess the impact of disruptions on patient care, data integrity, and overall operations.

3. Strategy Development:

- Business Continuity Strategies:
  - Develop strategies to address identified risks and ensure continuity of critical functions, considering healthcare-specific challenges.
- Resource Identification:
  - Identify resources required for implementing strategies, including personnel, technology, and facilities.

4. Plan Development:

- Create Business Continuity Plans (BCPs):
  - Develop detailed BCPs for critical functions, including emergency response, patient care, data protection, and IT systems recovery.
- Incident Response Plans:
  - Develop specific plans for immediate response to incidents, such as medical emergencies, natural disasters, or cyberattacks.

4.2.2. Data Lifecycle

The purpose of data lifecycle management in a cybersecurity framework is to ensure data security throughout its entire lifecycle in an organization's systems. It is an essential aspect that ensures data security at every stage, from capture to destruction. This involves implementing effective security measures, such as encryption, and assessing risks to manage and protect data based on its classification and importance to the organization. It's a dynamic process that requires continuous evaluation and adaptation to effectively safeguard data in the face of evolving cyber threats.

4.2.2.1. Implementation

The implementation of data lifecycle in a cybersecurity framework involves a couple of steps which play essential roles in ensuring the security and integrity of data throughout its existence:

1. Data Identification and Classification:

a. Identify what data needs to be protected.
   - Classify data based on sensitivity and criticality (e.g., public, internal, confidential, secret).
2. Data Creation and Acquisition:
   - Ensure secure data creation practices.
   - When acquiring data, validate sources and ensure data integrity.
3. Data Storage and Processing:
   - Store data securely using encryption and other security measures.
   - Process data in secure environments to prevent unauthorized access.
4. Data Usage:
   - Control and monitor access to data.
   - Implement user authentication and authorization procedures.
   - Ensure that data usage complies with policies and regulations.
5. Data Sharing and Transmission:
   - Use secure methods for data transmission (e.g., encrypted channels).
   - Manage data sharing with third parties through strict agreements and monitoring.
6. Data Archiving and Backup:
   - Regularly back up data to secure locations.
   - Archive data securely, maintaining accessibility for future needs.
7. Data Destruction and Disposal:
   - Securely delete or destroy data when it is no longer needed.
   - Follow proper procedures for the disposal of physical and digital data storage devices.
8. Compliance and Audit:
   - Regularly review and update data lifecycle practices to comply with evolving cybersecurity standards and regulations.
   - Conduct audits to ensure adherence to policies and identify areas for improvement.
9. Incident Response and Recovery:
   - Implement procedures for responding to data breaches or security incidents.

- Have plans in place for data recovery in case of loss or corruption.

10. Continuous Improvement:
    - Regularly update the cybersecurity framework to adapt to new threats and technologies.
    - Educate and train staff on best practices in data security.

4.2.3. Compliance

Compliance in a cybersecurity framework encompasses adhering to a set of rules and requirements from various sources, such as laws, contracts, or industry guidelines, to protect data that is stored or transferred electronically. The aim of these rules and requirements is to ensure the confidentiality, integrity, and availability of data. Cybersecurity compliance involves evaluating risks, adopting controls, and demonstrating due diligence. It is important to note that the sources and standards for cybersecurity compliance may vary based on the sector and location of the organization. In summary, compliance in a cybersecurity framework is about adhering to a complex array of rules, regulations, and best practices to protect electronic data and ensure the security of information systems. It involves a multifaceted approach that includes risk assessment, control implementation, and demonstrating adherence to various cybersecurity standards, all of which are critical for maintaining the overall security and integrity of an organization's data and IT infrastructure.

4.2.3.1. Implementation

During the implementation phase of a robust compliance training program, it is imperative to fully educate employees on the specifics of the Cybersecurity Framework. Training should cover elements such as compliance audits, compliance documentation, data privacy, notification requirements, and supply chain compliance, as outlined in the information provided. Employees should be made aware of legal and contractual requirements, including information security audits under Compliance (A.18). The focus of this phase is to establish a basic understanding of the elements of compliance and to educate employees on how to explicitly define and document the organization's legal, regulatory, and contractual obligations, as required by Control Specification.

After implementation, ongoing training becomes critical to maintain ongoing compliance awareness and adaptability to evolving cybersecurity requirements. Changes in

laws, regulations, and industry guidelines should be incorporated into regular updates to the training program. Periodic refresher training, with a specific focus on any updates or changes that may have occurred, is essential to reinforce employee understanding of compliance elements.

Post-implementation training should emphasize practical application as well as theoretical knowledge. Simulations and exercises can enhance employees' ability to contribute to the organization's overall security posture by helping them apply compliance principles in real-world scenarios. Monitoring and evaluation of employee understanding, and compliance should be an integral part of this phase, with regular assessments conducted to identify areas that may need additional focus or improvement. Ongoing documentation of training activities and compliance efforts is critical to maintaining a record of compliance and demonstrating due diligence. By combining basic training during implementation with ongoing education and hands-on practice post-implementation, organizations can foster a culture of ongoing compliance awareness and ensure that their workforce stays abreast of the dynamic landscape of security requirements.

4.2.4. Human Training

Human training in a cybersecurity framework plays a vital role in enhancing an organization's overall security posture. An effective cybersecurity training framework should consider the human factor, focusing on the development of policies, procedures, and training programs tailored to the specific needs and roles of different employees. This includes recruiting experts to facilitate and guide the training process, ensuring that it addresses the various aspects of cybersecurity relevant to each role within the organization Effective human training in a cybersecurity framework is not a one-time activity but requires ongoing commitment, regular updates, and a top-down approach from leadership to ensure that the entire workforce is equipped with the necessary knowledge and skills to contribute to the organization's cybersecurity defenses. This comprehensive approach to training is essential in building a robust human firewall against cyber threats.

4.2.4.1. Implementation

During the initial implementation phase, the focus of the staff training program is to provide comprehensive training that is aligned with NIST standards such as 800-53, 800-171, 800-51, 800-56, and 800-37. This includes an onboarding process that teaches essential security measures through the use of workshops, online courses, and simulations to cover areas such as access control, security policies, device security, data protection, and social engineering.

After implementation, the program transitions to a continuous training model. Regular updates to the Information Security Awareness, Education, and Training Program (Control Specification 02.e) ensure that employees, contractors, and third-party users are aware of changes in organizational policy. Ongoing training during employment is essential to maintain employee vigilance and compliance with evolving security protocols. Periodic refresher courses on HIPAA privacy topics are conducted to reinforce principles and address emerging issues, fostering a sustainable culture of security awareness.

Monitoring and evaluation mechanisms continue after implementation. Regular assessments measure the effectiveness of training initiatives, allowing for necessary adjustments and improvements. Ongoing documentation of training activities, security incidents, and employee compliance serves as the basis for tracking program success and ensuring adaptability to changing circumstances.

4.2.5. Asset Management

The purpose of asset management is to identify organizational assets and define appropriate protection responsibilities. It works as a critical function that involves identifying and managing the data, devices, systems, and facilities that are essential to an organization's operations. Cybersecurity asset management focuses on maintaining an accurate inventory of all cyber-enabled technologies, which includes not only hardware and software but also people and processes within an organization that are susceptible to cyber threats. Asset management is foundational to cybersecurity as it helps organizations understand what assets they have, their importance, and how they would be protected, forming the basis for a robust cybersecurity posture.

4.2.5.1. Implementation

1. Asset Inventory:

- Conduct a Comprehensive Asset Inventory:
    - Begin by creating a detailed inventory of all assets within your healthcare organization. This includes physical assets (e.g., medical equipment, facilities, infrastructure) and digital assets (e.g., data, software, IT systems).
- Collaborate with Relevant Departments:
    - Work closely with departments across the organization to ensure that all types of assets are accounted for. This may involve collaboration with IT, operations, finance, and facility management teams.

2. Asset Classification:

- Identify Critical Assets:
    - Classify assets based on their criticality to the organization's operations. Focus on those assets that, if compromised, would have a significant impact on patient care, regulatory compliance, or overall business continuity.
- Consider Data Sensitivity:
    - For digital assets, consider the sensitivity of the data they hold. Identify assets that store or process sensitive patient information, ensuring compliance with healthcare regulations (e.g., HIPAA).

3. Documentation and Asset Profiles:

- Create Asset Profiles:
    - Develop detailed profiles for each identified asset. Include information such as asset type, location, owner, dependencies, and criticality. Use a standardized format for consistency.
- Maintain Documentation:
    - Establish a system for regularly updating and maintaining asset documentation. This ensures that changes in asset status or criticality are reflected in the asset management system.

4.2.6. Risk Management

Risk management in the cybersecurity framework involves a set of best practices that standardize the management of cybersecurity risks. It helps organizations in identifying, assessing, mitigating, and monitoring cyber risks, and in defining security processes and procedures to address them. Frameworks like the NIST Cybersecurity Framework map core functions of cybersecurity risk management, including protection, detection, identification, response, and recovery, and can be applied throughout the vendor lifecycle. Such frameworks can also benefit from automation tools like SOAR (Security Orchestration, Automation and Response) to efficiently handle cybersecurity risks and related decision-making.

4.2.6.1. Implementation

- Strategy and planning
    - HIPAA: Compliance with privacy and security rules regarding the protection of personal health information.
    - ISO/IEC 27001: Establishment and maintenance of an information security management System (ISMS), including the development of information security policies.
    - Implementation: Formulate information security policies and clarify guidelines and procedures for data protection, access control, risk management, etc.
- Technical control and tool implementation
    - NIST SP 800-53: Implements NIST recommended security controls, including encryption, access control, and security monitoring.
    - CIS Controls: Deploy basic and advanced security controls such as firewalls, IDS/IPS and SIEM systems.
    - Implementation: Install and configure network security equipment and software for data encryption and enhanced authentication.
- Staff training and awareness raising
    - HIPAA training requirements: Ensure that all employees receive training on protecting personal health information.
    - ISO/IEC 27002: Raising employee awareness of information security best practices.

    - Implementation: Regular cybersecurity and compliance training sessions are held, including simulated phishing attacks and security awareness campaigns.
- Compliance and standard compliance
    - HITRUST CSF: combines the requirements of HIPAA and other standards (such as NIST, ISO) to develop industry-specific security controls.
    - Implementation: Periodically audit and evaluate the effectiveness of existing security controls to ensure compliance with multiple standards and regulations.
- Continuous review and improvement
    - ISO/IEC 27001: Perform regular internal and external audits to assess the effectiveness of the information security management system.
    - NIST Cybersecurity Framework: Continuous improvement of security measures based on the framework for identification, protection, detection, response and recovery.
    - Implementation: Conduct regular security assessments and risk analysis and adjust and improve security policies and controls based on audit results.
- Emergency preparedness and response
    - HIPAA Emergency preparedness requirements: Ensure that emergency response and notification processes are in place in the event of a data breach or other security incident.
    - Implementation: Develop an emergency response plan, including incident detection, response, recovery and notification procedures, and conduct regular drills and tests.
- Document and record
    - ISO/IEC 27001: Maintaining detailed records of information security policies, risk assessment reports and training materials.
    - HIPAA documentation requirements: Maintain all compliance documentation related to the protection of personal health information.
    - Implementation: Establish a document management system to ensure that all safety policies, procedures and training records are properly archived and updated.

4.2.7. Third-party Relationships

Managing third-party relationships is crucial due to the potential risks these external entities can introduce. A third-party cybersecurity framework provides a structured process and procedure for organizations to assess, monitor, and mitigate risks within their vendor ecosystems. This framework is developed to set standards across the organization, focusing on third parties that pose the greatest risks. It encompasses a comprehensive approach to analyze, control, monitor, and mitigate cyber risks associated with third-party vendors, suppliers, and service providers. A robust risk assessment framework is key to enhancing organizational cybersecurity through third-party risk management. This framework should take into account the criticality of each third-party relationship, their cybersecurity practices, and their history of security incidents.

4.2.7.1. Implementation

Third-party Relationships partially belong to business continuity management. So, integrating third-party relationship considerations into your Business Continuity Management (BCM) plan is crucial.

1. Third-Party Dependency Analysis:

- Identify Critical Third Parties:
  - Conduct a comprehensive analysis to identify third-party suppliers and service providers critical to your healthcare operations. This includes vendors for medical supplies, IT services, pharmaceuticals, and any other essential partners.
- Assess Dependency Risks:
  - Evaluate the potential risks associated with each third-party dependency, considering their impact on your organization's ability to deliver healthcare services.

2. Integration into BIA and Risk Assessment:

- Include Third-Party Dependencies in BIA:

- Integrate third-party dependencies into the Business Impact Analysis (BIA) to understand their role in critical functions and assess the impact of disruptions.

- Risk Assessment for Third Parties:
  - Assess the risks posed by third-party providers, considering factors such as financial stability, geographical location, and the robustness of their own BCM programs.

3. Collaborative Planning with Third Parties:

- Establish Communication Protocols:
  - Develop communication protocols with critical third-party partners to ensure coordination and information sharing during disruptions.
- Joint Planning Exercises:

o Conduct joint planning exercises with key third parties to test the effectiveness of collaborative response and recovery efforts

4.2.8. Cryptography/Key Management

The purpose of cryptography is to ensure proper and effective use of cryptography to protect the confidentiality, authenticity, integrity, non-repudiation, and authentication of information. Cryptography and Key Management play a crucial role in a cybersecurity framework, ensuring the secure storage and transmission of sensitive information. Effective key management includes handling the entire lifecycle of cryptographic keys, from their generation, distribution, and usage to their eventual destruction or retirement. This lifecycle management is essential for ensuring that the keys remain secure throughout their use. It also includes provisions for key compromise recovery and secure key storage. In summary, cryptography and key management are essential components of a cybersecuritfrom their generation, distribution, and usage digital communications and protecting sensitive data.

4.2.8.1. Implementation

We recommend implementing key management by looking at these aspects (following NIST SP 800-57 PART 1 REV. 5 and ISO/IEC 27002:2013 Cryptographic Controls):

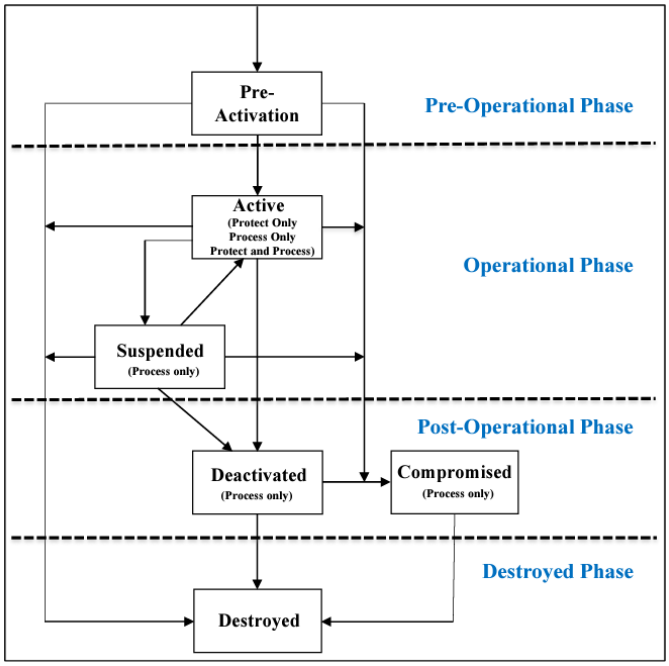

Figure 3. Cryptographic key-management lifecycle (NIST SP 800-57 PART 1 REV. 5)

We can also divide the cryptographic key-management lifecycle into four phrases (see Figure 3).

1. **Pre-Operational Phase:** Keying material is not yet ready for regular cryptographic operations. Keys may not have been generated or are in a pre-activation state. Additionally, system or enterprise attributes are established during this phase.
    - Key Generation:
        - Specify the methods and algorithms for generating cryptographic keys; Creating a key through the output of a Random Bit Generator (RBG), deriving a key from another key, deriving a key from a password, and executing key agreement between two entities using an approved key-agreement scheme (see Barker EB, Roginsky AL (2019)).
2. **Operational Phase**: Keying material is available and actively used. Keys can be in an active or suspended state, with active keys designated as protect-only, process-only, or both protect and process. Suspended keys are solely available for processing.
    - Key Distribution:
        - Define secure channels and protocols for distributing keys to authorized entities.

  - The encryption standards mandated by HIPAA represent the minimum AES 128-bit encryption requirements recommended by the NIST for safeguarding electronic Protected Health Information (ePHI) both at rest and in transit. We consider dealing with highly sensitive information, choosing to use 192-bit or 256-bit key lengths for added security.
  - Keys exclusively designated for storing information (i.e., data or keying material) shall not be distributed unless for backup purposes or to other authorized entities requiring access to the stored information protected by the keys.
  - Passwords are permitted to be distributed, but their level of protection during distribution must align with the security requirements mandated for their use. For example, if a password is intended for accessing cryptographic keys that deliver a security strength of 128 bits when safeguarding data, the password itself should be endowed with at least 128 bits of protection (see NIST SP 800-57 PART 1 REV. 5 8.1.5.3.8 Passwords)
- Key Storage:
  - Consider key types, type of security service that is provided by the key in conjunction with a cryptographic technique, the level of safeguarding needed for the key (i.e., confidentiality, integrity, and/or availability), and the length of time that the integrity and/or confidentiality of the key need to be maintained. For example, symmetric keys and private keys shall be rendered unusable upon completion of their protection period.
- Key Usage:
  - Clearly define the purpose and scope of each cryptographic key.
  - Specify the cryptographic algorithms and key lengths to be used for specific applications.
- Key Rotation and Refresh:

- Establish guidelines for regular key rotation to mitigate the impact of key compromise.
- Define procedures for updating cryptographic algorithms and key lengths as technology evolves

3. **Post-Operational Phase:** Keying material is no longer actively used, but access to it is possible, allowing for processing protected information. Keys are in deactivated or compromised states and may be archived.
    - Key Backup and Recovery:
        - Describe processes for securely backing up cryptographic keys.
        - Define recovery procedures in the event of key loss or compromise.
4. **Destroyed Phase**: Keys are permanently unavailable. Records of their existence may or may not have been deleted. Keys are in the destroyed state. Even if the keys themselves have been destroyed, metadata such as key name, type, cryptoperiod, and usage period may still be retained.
    - Key Retirement and Deletion:
        - Specify procedures for retiring keys that are no longer needed.
        - Ensure secure deletion processes for cryptographic keys that are no longer in use.

4.2.9. Security Controls

Security controls in a cybersecurity framework are essential measures and mechanisms put in place to protect information systems and organizations from a wide array of threats and risks. These risks can range from hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, to privacy risks. The purpose of these controls is to safeguard organizational operations, assets, individuals, and other organizations. In summary, security controls in a cybersecurity framework are a critical aspect of safeguarding an organization's digital assets and operations. These controls, guided by frameworks like the NIST Cybersecurity Framework, encompass a range of measures and practices designed to protect against various cyber threats and risks, ensuring the continuity and integrity of organizational processes and data.

4.1.9.1 Security Controls Implementation

To implement security controls, we can possibly utilize the following steps:

1. **Selection of Controls:** Based on the risk assessment, select appropriate security controls. These can be physical (like locks and surveillance), technical (like firewalls and antivirus software), or administrative (like policies and training).
2. **Implementation:** Deploy the selected controls. This could involve installing hardware or software, changing processes, or training employees.
3. **Testing and Evaluation:** After implementation, it's crucial to test the controls to ensure they are functioning as intended. This might involve penetration testing, security audits, or compliance checks.
4. **Maintenance and Continuous Monitoring:** Security is not a one-time task. Regularly review and update the controls to adapt to new threats, technological changes, or business developments. Continuous monitoring can help detect and respond to security incidents in real time

4.2.10. Physical and Environmental Security

The purpose of physical and environmental security is to prevent unauthorized physical access, damage, and interference to the organization's information and information processing facilities. Physical and Environmental Security in a cybersecurity framework encompasses measures designed to protect systems, buildings, and related supporting infrastructure against threats stemming from their physical environment. Physical and environmental security in a cybersecurity framework is not just about implementing barriers or locks but also a multifaceted discipline that requires a comprehensive approach, integrating with cybersecurity measures and continual assessment and improvement. This integration ensures that all aspects of an organization's security — both physical and digital — are robust, aligned, and responsive to the evolving threat landscape.

4.2.10.1. Implementation

When implementing physical and environmental security measures, several aspects must be considered to ensure the organization's safety. Based on visitor security, laptop control, cameras, alarms, security, secure entrances, racks and cages, environmental control, electrical grounding, and fire suppression systems, we can give:

- Visitor Security
    - Compliance with ISO/IEC 27001 requirements for physical access control.
    - Implementation: Implement visitor registration and identity verification procedures, provide visitor badges, and ensure that employees accompany visitors in sensitive areas.
- Laptop Control
    - Compliance with HIPAA and ISO/IEC 27001 security requirements for mobile devices and remote working.
    - Implementation: Check all incoming and outgoing laptops to ensure security configuration, use encryption and strong passwords.
- Camera
    - Compliance with ISO/IEC 27001 physical and environmental safety standards.
    - Implementation: Monitoring cameras are installed in key areas for real-time monitoring and video storage.
- Alarms
    - Compliance with local regulatory requirements for safety alarm systems.
    - Implementation: Install an intrusion detection alert system and connect with local law enforcement agencies.
- Guards
    - Compliance with ISO/IEC 27001 guidelines on physical access control.
    - Implementation: Security personnel are deployed to monitor key entrances and sensitive areas for patrolling and emergency response.
- Secured Entry
    - Compliance with ISO/IEC 27001 physical entry control requirements.
    - Implementation: Use electronic locks, biometrics, or other security mechanisms to control access to critical entry points.
- Racks and Cages
    - Compliance with ISO/IEC 27002 requirements for the protection of information processing facilities.
    - Implementation: Use locked racks and cages in data centers to protect critical equipment and servers.

- Environmental Controls
    - Compliance with ISO/IEC 27001 requirements for the management of environmental risks.
    - Implementation: Install the temperature and humidity control system to ensure that the equipment is in the appropriate environmental condition.
- Electrical Grounding
    - Compliance with local electrical safety standards and regulations.
    - Implementation: Ensure that all electrical systems and equipment are properly grounded to prevent electrical failures and fire risks.
- Fire Suppression
    - Compliance with local fire codes and ISO/IEC 27001 requirements for fire prevention.
    - Implementation: Install an automatic fire extinguishing system, smoke detector, and regular maintenance and testing.

4.2.11. Access Controls

Access controls are a fundamental component of cybersecurity frameworks. They are the methods and technologies used to manage and regulate who or what can view or use resources in a computing environment. Access controls are essential for ensuring that sensitive information, such as personal data, financial records, and intellectual property, is only accessible to authorized individuals. This helps prevent data breaches and information theft. Moreover, implementing access controls according to the principle of least privilege ensures that individuals have only the access necessary to perform their jobs, reducing the risk of accidental or deliberate misuse of information.

4.2.11.1. Implementation

We mainly followed the guidelines from NIST SP 800-162 and NIST SP 800-53. The key components for access controls are:

- **Access Control Policy and Procedures:**
    - Establishing and maintaining an access control policy that defines the rules and procedures for granting and managing access to information systems.

- **Account Management:**
    - Managing and controlling user accounts, including the creation, modification, and termination of accounts, as well as ensuring the validity of users' access credentials.
    - Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service.
- **Access Enforcement:**
    - Implementing mechanisms to ensure that access control policies are enforced, including the use of access control lists, authentication, and authorization mechanisms.
    - Control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems (NIST SP 800-53 AC-3).
        - Attribute-Based Access Control (ABAC):
            - In a healthcare setting, access to patient records may be determined not only by the user's role (doctor, nurse, administrator) but also by attributes like the patient's medical condition, the sensitivity of the data, or the location of the user. ABAC allows for fine-grained control over who can access what information based on a variety of attributes.
    - The minimum password length with special characters (10 characters), validation time window for time synchronous one-time tokens (e.g. 30 seconds), and number of allowed rejections (e.g. 4 times) during the verification stage of biometric authentication.
- **Separation of Duties:**
    - Preventing conflicts of interest and minimizing opportunities for unauthorized access by dividing tasks and responsibilities among different individuals or systems.
    - The separation of mission or business functions and support functions among distinct individuals or roles. It includes the delegation of system support functions to different individuals.

  - Ensuring that security personnel responsible for administering access control functions do not concurrently administer audit functions.

- **Least Privilege:**
  - Providing individuals with the minimum levels of access or permissions necessary to perform their job functions and responsibilities.
  - Role-Based Access: Define distinct roles within the organization based on job responsibilities and assign the minimum necessary permissions to each role to perform required tasks. Users are then assigned to roles based on their job functions
  - Need-to-Know Basis: Implement a "need-to-know" policy, where access to sensitive information is granted only to individuals who require it for their specific roles.
- **Access Control for Mobile Devices and Removable Media:**
  - Implementing access controls specific to mobile devices and removable media to protect sensitive information and prevent unauthorized access.
  - Device Authentication: Require strong authentication methods such as PINs, passwords, biometrics, or multi-factor authentication to unlock mobile devices. Enforce policies for regular password updates and discourage the use of easily guessable passwords

4.2.12. Monitoring/Audit Logging

Monitoring and audit logging in a cybersecurity framework are critical components for ensuring the security and integrity of information systems. According to the CIS Critical Security Control, organizations should collect, alert, review, and retain audit logs of events that could help in detecting, understanding, or recovering from an attack. This control emphasizes the importance of maintaining detailed records of security events to facilitate prompt and effective responses to cyber threats and incidents. In summary, monitoring and audit logging are fundamental to any cybersecurity framework. They enable organizations to track, analyze, and respond to security incidents and anomalies effectively. By implementing best practices in log management, organizations can enhance their ability to detect and respond to cyber threats, thereby strengthening their overall cybersecurity posture.

4.2.12.1. Implementation

We followed the guidelines from NIST 800-92 Guide to Computer Security Log Management. A log management infrastructure is structured into three tiers:

1. Log Generation
2. Log Analysis and Storage
3. Log Monitoring

The first tier involves hosts that produce log data, with some using logging client applications or services to share logs through networks to log servers in the second tier. Log servers in the second tier receive log data in real-time, near-real-time, or occasional batches, acting as collectors or aggregators for multiple log generators. Log data may be stored on these servers or on separate database servers. The third tier comprises consoles used to monitor, review, and generate reports on log data and automated analysis results.

Log management infrastructures are designed to execute various functions that facilitate the storage, analysis, and disposal of log data while maintaining the integrity of the original logs. These functions are typically carried out in a non-intrusive manner to preserve the authenticity and accuracy of the original log entries.

In our case, when choosing infrastructure, Security Information and Event Management (SIEM) software is a recommended choice. It typically utilizes proprietary data formats in its operations unlike syslog-based logging (NIST 800-92). These SIEM products feature centralized servers dedicated to log analysis and separate database servers for log storage. In many cases, SIEM implementations involve the installation of agents on each host generating logs. These agents play a crucial role in filtering, aggregating, and normalizing log data specific to their log types. Moreover, agents are responsible for the real-time or near-real-time transfer of log data from individual hosts to a centralized SIEM server.

5. Cost-Benefit Analysis

5.1. What each component requires

To better analyze the case, here are the elements of the costs and benefits of each part of our cybersecurity framework.

In the practice of cyber security, the personnel training and compliance component is fundamental, which includes the necessary training costs and the cost of compliance with various regulations. Despite the large initial investment, this helps to secure data, increase legal protection, improve customer trust, and give companies a competitive advantage, while improving efficiency and productivity, and significantly reducing the risk of fines for violations.

Risk management is about identifying threats and vulnerabilities and multiplying them with asset values to calculate overall risk. Factors to consider include organizational size, culture, industry verticals, regulatory requirements, and customer requirements. From the cost side, we need to calculate the cost of human resources, technical tools (e.g., SIEM, IDS/IPS), compliance costs, training and education costs, risk mitigation measures, and monitoring and response (e.g., SOC Operations centers). The benefits of these costs are reduced risk of data breaches, enhanced corporate reputation, compliance, reduced downtime, and increased productivity.

In terms of physical and environmental security, we need to understand the security of an organization's important physical locations, as well as the infrastructure and potential risks that exist within that area. Costs include security equipment and facility investments, human resources training and recruitment, environmental monitoring equipment, physical security audit and compliance costs, data center and backup equipment investments, and disaster recovery plans. The benefits of these investments are enhanced physical security, improved business continuity, compliance requirements, and a sense of security for employees and visitors, while helping to reduce insurance costs.

Encryption and key management are strategic investments. According to Gartner, by 2023, 40 percent of organizations will implement a hybrid and multi-cloud data encryption strategy across multiple storage areas. By 2024, 35% of organizations will utilize key and encryption orchestration platforms for various encryption tasks. Costs include staff expenses, policy development, compliance costs, training and awareness raising, risk assessment and audit, incident response and recovery, data classification and inventory. The benefits are reflected in enhanced data protection, regulatory compliance, reduced risk of data breaches, increased accountability and transparency, enhanced customer trust and confidence, improved incident response efficiency and brand protection.

The cost-benefit analysis of monitoring and auditing logs focuses on the costs of storage and infrastructure, compliance reporting, incident response, and investigation. The benefits are reflected in preventive measures, forensic analysis, auditing and reporting, and security incident detection.

For access control, key factors include business requirements for access control, user access management, user responsibilities, and system and application access control. Costs involve investments in hardware (such as access cards, biometric scanners) and software (such as access management platforms), compliance costs, and personnel expenses. The benefits include protection of sensitive information, reduced risk of unauthorized activity, improved security posture, and increased accountability.

The benefits of asset management are reduced downtime and costs, leveraging industry expertise, unifying asset management processes, extending asset life, and optimizing maintenance processes. The return on investment of real-time tracking systems (RTLS) is typically based on three cost-saving areas of improved clinical efficiency, increased utilization reduction, and reduced loss.

The benefits of security controls are to protect confidential information, prevent unauthorized access, avoid financial losses, maintain business operations, and maintain trust and reputation. The cost includes procurement cost, implementation cost and training cost.

System lifecycle benefits include improved quality, cost efficiency, effective risk management, flexibility and adaptability, and enhanced project management. Costs relate to initial investment, training and development, long time to market, maintenance costs and end-of-life costs.

Finally, the benefits of third-party relationship management and business continuity management lie in ensuring patient safety, data protection as a top priority, reduced risk of data breaches, reduced downtime, risk reduction, data protection, customer, and stakeholder confidence. The hidden annual costs of these management actions far outweigh the direct costs of data breaches, but with the right investments, these hidden costs can be significantly reduced.

To better calculate these costs, we divided the input into five parts: capital expenses, external resources, operations and control, training and education, and internal construction.

In terms of benefits, we integrate direct benefits and indirect benefits into two categories.

The following is our specific analysis of the costs and benefits.

5.2. Costs

Foundations:

- Risk Analysis and Monitoring Tools:
    - RiskLens platform: $15,000/year.
    - Security Information and Event Management (SIEM) tools: $15,000 (purchase and maintenance).
- Physical Security Systems
    - Access control systems (card or biometric): $30,000.
    - Surveillance cameras (CCTV (Closed circuit television) system): $10,000.
    - Climate control system: $15,000.
    - Fire protection system (smoke detectors and sprinklers): $20,000.
- Network and Information Security
    - Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS): $45,000.
    - Antivirus software: $3,500/year (for 100 devices, $35/device/year).
    - Firewalls (including basic and advanced options): $500 – $20,000.
    - Security compliance management: $10,000 – $100,000 (customized according to needs).
    - Hardware Security Modules (HSMs) or key management services: $20,000/year.
    - Encryption software and related hardware: $25,000/year.
- Hardware, Storage, and Networking Equipment
    - Servers and storage: $8,000. (optional)
    - Network equipment: $5,000. (optional)
    - Storage and infrastructure (including log collection and storage): $30,000.
    - Hardware (including 2 firewalls): $5,000.

- Software Procurement and Implementation Costs
    - Purchase, configuration, and integration of business continuity management software and hardware: $10,000.
    - Asset management software: $10,000.
- Technical Support and Services
    - Technical support contract for business continuity management system: $2,000/year.
- Reduced Potential Losses:
    - Real-time monitoring and intrusion detection: reducing potential losses by $7,000 annually.
- Contract Management:
    - Implementation of contract management system: $15,000.

External Sources:

- Consulting and Professional Services:
    - Annual risk assessments by external experts such as Deloitte or PwC: $20,000.
    - Security consulting (assuming a range of hours; this will be an estimate): If we assume a minimum of 10 hours of consulting at $100/hour, that is $1,000. If we assume a maximum of 20 hours at $500/hour, that is $10,000. Therefore, the range is $1,000 to $10,000 annually.
- Compliance and Auditing:
    - External compliance audits: $8,000 per year.
    - Legal and compliance fees (which may include legal counsel and compliance audits): Assuming the legal counsel fee is a separate expense, it is $10,000. The compliance audit fees are provided twice, at $15,000 and $10,000. If we assume the $15,000 includes the $10,000, then we will use the higher figure of $15,000 for a regular compliance audit.
    - Purchase of compliance tools: $7,000 (this is a one-time cost, but without specific indication, we will consider it as an annual expense for this calculation).
- Testing and Exercises:

  - Penetration testing: $20,000 every 2 years, which averages to $10,000 per year.
  - Full business continuity drill: $4,000 per year.
- Contractual Costs:
  - Contract negotiation fee: $5,000 (It is not clear if this is an annual fee or a one-time fee. If it is for ongoing negotiations, it could recur annually. For this calculation, we will consider it a one-time fee).
- Audit Costs:
  - Regular audit fee: $10,000 (Assuming this is an annual audit separate from the compliance audit).

Operating Maintenance:

- Team Operations Cost: $100,000 annually for the internal risk management team, including compensation and other expenses.
- Property and Equipment Insurance: $5,000 annual premium for protection against damage from fire, flood, or other natural disasters.
- System Maintenance and Monitoring: $10,000 annual operating costs, including regular inspections and maintenance of security systems.
- Encryption System Maintenance and Management: $5,000 per year, covering regular key changes and software updates.
- Backup and Recovery: $6,000 per year for a comprehensive data backup and disaster recovery plan, including backup software and remote backup sites.
- Ongoing Maintenance and Storage: $8,000 per year covering regular maintenance, storage, and management of log data.
- Contract Monitoring Costs: $10,000 for setting up and maintaining the monitoring mechanism.
- Updates, Patches, and System Check-ups:
  - Hardware: 15% - 25% of the initial purchase cost per year.
  - Software Subscription Renewals: Often 20% - 30% of the initial software cost annually.
- Asset Database Maintenance: $2,000 per year.

- Monitoring and Response: $6,000 to monitor asset security incidents.
- Data Storage Maintenance: Purchase enough storage for $5,000.
- Backup and Recovery: Set up a data backup and emergency recovery plan for $3,000.

Training:

- Risk Management Training Estimated Cost: $10,000.
- Business Continuity, Cybersecurity, and Safety Training Estimated Cost: $5,000.
- In-house Staff Training Cost: $5,000.
- Continuous Staff Training Cost: Per employee, $500 - $5,000 annually.
- Asset Managers Training Cost: $5,000.
- HIPAA Compliance Training Cost: $3,000.

Internal establishment of positions (personnel):

- Security Manager: $80,000
- Business Continuity Management Specialist: $60,000
- Cyber Security personnel (3): $180,000
- System monitoring and maintenance: $10,000.

To calculate total expenses for a year, we will combine all annual expenses and one-time expenses. Note that some costs give ranges rather than fixed values, and for these I will use the lowest value of the range to make the calculation to provide a conservative estimate.

Annual Recurring Costs:

- - RiskLens platform: $15,000
- - Antivirus software: $3,500
- - Hardware security module or key management service: $20,000
- - Encryption software and related hardware: $25,000
- - Technical Support contract: $2,000
- - Regular audit fee: $10,000
- - Risk assessments: $20,000
- - Security consulting: Assume an average of $5,500 (if this is an annual expense)
- - Compliance audits: $8,000

- - Legal and compliance fees: $10,000
- - Compliance audit fee: $15,000
- - Compliance tools: $7,000
- - Penetration testing (annualized): $10,000
- - Business continuity drill: $4,000
- - Team Operations Cost: $100,000
- - Property and Equipment Insurance: $5,000
- - System Maintenance and Monitoring: $10,000
- - Encryption System Maintenance and Management: $5,000
- - Backup and Recovery: $6,000
- - Ongoing Maintenance and Storage: $8,000
- - Contract Monitoring Costs: $10,000
- - Asset Database Maintenance: $2,000
- - Monitoring and Response: $6,000
- - Data Storage Maintenance: $5,000
- - Backup and Recovery (setup): $3,000
- - Continuous Staff Training: Assuming $2,500 average per employee (specific number of employees consider to be 100)
- - Staff Salaries:
    - Security Manager: $80,000
    - Business Continuity Management Specialist: $60,000
    - Asset Management personnel (3): $180,000
- System monitoring and maintenance: $10,000

Subtotal: $895000

One-Time Costs:

- - Access control system: $30,000
- - Security camera system: $10,000
- - Climate control system: $15,000
- - Fire protection system: $20,000
- - IDS/IPS: $45,000

- - Firewall: $500 (using minimum value)
- - Security Compliance Management: $10,000 (using minimum value)
- Optional- Server and storage: $8,000 (Not counted this time)
- Optional- Network equipment: $5,000 (Not counted this time)
- - Log Storage: $30,000
- - Business continuity management software and hardware: $10,000
- - Asset Management software: $10,000
- - SIEM Tool: $15,000
- - Contract Management System: $15,000
- - Contract negotiation fee: $5,000
- - Risk Management Training: $10,000
- - Business Continuity, Cybersecurity, and Safety Training: $5,000
- - In-house Staff Training: $5,000
- - Asset Managers Training: $5,000
- - HIPAA Compliance Training: $3,000

Subtotal: $243,500

Variable Costs:

- Hardware (15%-25% of initial purchase cost)
- Software Subscription Renewals (20%-30% of initial software cost)

COSTS :

Total Annual Cost = 895,000

Total One-Time Costs = 243500

5.3. Benefits

We separated the benefits into direct benefits, indirect benefits and potential penalties. Direct benefits refer to the tangible and measurable advantages that directly result from implementing a security framework. On the other hand, indirect benefits are positive outcomes that are not immediately measurable but contribute to the overall well-being and resilience of the organization. Another aspect is the potential penalties for non-compliance.

Non-compliance with security standards and regulations can result in various penalties, both financial and non-financial. This is considered as a benefit because unlike costs that are able to measure and can either annually or once-time. Using a regulatory-compliant framework mitigates potential penalties, turning regulatory compliance into a benefit that addresses underlying risks.

Direct Benefits:

- Accidental Losses: Mitigated losses of $50,000.
- Insurance Cost Reduction: Risk transfer savings of $5,000.
- Compliance Advantage: Penalty avoidance savings of $20,000.
- Asset Protection: Avoided losses of $25,000.
- Lower Insurance Rates: Premium reduction savings of $1,000.
- Efficient Incident Response: Lower impact costs, saving $5,000.
    - Impact and response costs of data breaches would be lower, resulting in a savings of $5,000
- Business Opportunities and Market Share: Increased revenue of $500,000.
- Overall Risk Reduction: Probability and loss reduction, saving $800,000.

Indirect Benefits:

- Enhanced Reputation: Positive influence on long-term value.
- Market Confidence: Increased confidence leading to potential new business.
- Investor and Customer Confidence: Enhanced confidence attracting new business.
- Employee Satisfaction: Safer environment boosting satisfaction and productivity.
- Customer Trust and Reputation
- Improved Security Measures: Potential cost and disruption risk reduction.
- Efficiency and Optimization
- Accountability, Transparency, and Trust: Reduced costs and enhanced reputation.

Potential penalties (Not included into total annual benefits):

- Data Breach Prevention:
    - The global average cost per mid-sized company per data breach was $4.45 million in 2023

- Regulatory Compliance: Fines avoidance and legal risk reduction.
    - CPRA (California Privacy Rights Act)
        - Fines of up to $7,500 for each intentional violation and up to $2,500 for each unintentional violation
    - General Data Protection Regulation (GDPR)
        - Fines of up to €20 million or 4% of the company's global annual turnover
    - HL7 Fast Healthcare Interoperability Resources (FHIR)
- Reputation Damage

Subtotal

Total Annual Benefits: $1,411,000

5.4. Analysis

Now, in the annual quantitative part, based on our total benefits and total costs, we can find the **Annual Net Benefits = Total Annual Benefits – Total Annual Costs = $516000**

This implies a positive outcome from implementing our cybersecurity framework. Even though there is a **$243,500** one-time cost in the set-up stage, after the first year's operation, the company will earn back the set-up fee and gain **$272,500** in revenue.

6. Summary

In the end, as a conclusion, this document outlines a comprehensive cybersecurity framework designed by a consultancy for Y-GWASH Inc., a healthcare company. The consultancy, with expertise in IT and cybersecurity, aims to address the significant cybersecurity risks in the healthcare industry, including data breaches, ransomware, phishing, and DDoS attacks. The framework stresses the importance of cybersecurity in protecting patient data, ensuring medical device security, maintaining operational continuity, managing financial implications, and complying with regulatory standards.

Our key components of the framework include:

1. Strategic Aspect: Focuses on business continuity, data lifecycle, compliance, and human training.

2. Managerial Aspect: Deals with asset management, risk management, and third-party relationships.
3. Technical Aspect: Covers cryptography/key management, security controls, physical and environmental security, access controls, and monitoring logging.

Our framework emphasizes the need for business continuity management, data lifecycle management, compliance with cybersecurity laws and regulations, and thorough human training. It also outlines detailed implementation strategies for each component, including asset management, risk management, cryptography, and key management, among others.

Additionally, we present a cost-benefit analysis of the proposed framework, highlighting the substantial initial and recurring costs against the significant benefits, including mitigated losses, compliance savings, asset protection, and overall risk reduction. The framework is expected to yield a positive return on investment, enhancing Y-GWASH Inc.'s overall cybersecurity posture and reducing its vulnerability to cyber threats. By implementing this framework, Y-GWASH Inc. is better able to protect its critical medical data and devices while also meeting increasingly stringent compliance requirements.

As technology evolves and cyber threats continue to evolve, Y-GWASH Inc. Cybersecurity policies need to be continuously monitored and updated. By implementing our proposed cybersecurity framework, Y-GWASH Inc. will be able to effectively protect its critical assets while preparing for security challenges that may arise in the future. This is not only an investment in technology, but also in the long-term success and sustainability of the company.

7. Reference

Gartner (2020): Develop an Enterprise wide Encryption Key Management Strategy or Lose the Data, https://www.gartner.com/document/3991120

Kost, E. (2023). *Biggest cyber threats in healthcare (updated for 2023): Upguard*. Biggest Cyber Threats in Healthcare (Updated for 2023). https://www.upguard.com/blog/biggest-cyber-threats-in-healthcare

Hyde, J. (n.d.). *Why Healthcare Orgs must prioritize 3rd-Party Risk Management*. Bank Information Security. https://www.bankinfosecurity.com/blogs/healthcare-orgs-must-prioritize-3rd-party-risk-management-p-3364

Security Magazine. (2019, July 10). *Third-party risk costs the healthcare industry $23.7 billion a year*. Security Magazine RSS. https://www.securitymagazine.com/articles/90499-third-party-risk-costs-the-healthcare-industry-237-billion-a-year

R., M. (2022, October 24). *How much should a business spend on disaster recovery?*. WheelHouse IT. https://www.wheelhouseit.com/how-much-should-your-business-spend-on-disaster-recovery-and-business-continuity/

Fragala, W. by M. (n.d.). *How to calculate the ROI of Healthcare Asset Tracking*. Joerns Healthcare Icon. https://blog.joerns.com/how-to-calculate-the-roi-of-healthcare-asset-tracking

Glassdoor (2023), https://www.glassdoor.com/Career/security-manager-career_KO0,16.htm

The HIPAA Journal. (n.d.). *Healthcare Data Breach Statistics - HIPAA Journal*.https://www.hipaajournal.com/healthcare-data-breach-statistics/

Han, J. Y., & Liss , S. (2023, February 28). *Hacking healthcare: With 385m patient records exposed, cybersecurity experts sound alarm on breach surge*. https://www.healthcaredive.com/news/cybersecurity-hacking-healthcare-breaches/643821/

Healthcare Cyber Security Market Size Report 2030. (2021). https://www.grandviewresearch.com/industry-analysis/healthcare-cyber-security-market#:~:text=How%20big%20is%20the%20healthcare,USD%2017.3%20billion%20in%202023

CheckPoint (2022), *Why Healthcare is a Leading Target for Cybercriminals*, https://www.checkpoint.com/cyber-hub/cyber-security/what-is-healthcare-cyber-security/cyberattacks-on-the-healthcare-sector/#:~:text=Common%20Cyber%20Threats%20For%20the%20Healthcare%20industry&text=Data%20Breaches%3A%20Healthcare%20organizations%20store,of%20attackers%20targeting%20healthcare%20organizations.

Barker EB, Roginsky AL (2019) Recommendation for Cryptographic Key Generation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-133, Rev. 1. https://doi.org/10.6028/NIST.SP.800-133r1

Hu, V. C., Kuhn, R., & Yaga, D. (2017). Verification and test methods for access control policies/models. *NIST Special Publication*, *800*, 192.

Barker, E., & Barker, W. (2018). *Recommendation for key management, part 2: best practices for key management organization* (No. NIST Special Publication (SP) 800-57 Part 2 Rev. 1 (Draft)). National Institute of Standards and Technology.

Kent, K. A., & Souppaya, M. (2006). Guide to Computer Security Log Management:.