Limetree Inc:

Security Breach Analysis and Recommendations

Jeremy Willett

Contents

[Introduction 3](#_Toc131357535)

[Security Breach 4](#_Toc131357536)

[Attack Location 4](#_Toc131357537)

[Attack Method and Type 5](#_Toc131357538)

[Vulnerabilities 6](#_Toc131357539)

[Incident Response 10](#_Toc131357540)

[Purpose 10](#_Toc131357541)

[Examples 11](#_Toc131357542)

[Roles and Responsibilities 13](#_Toc131357543)

[Current incident Response Process 15](#_Toc131357544)

[Actions and Business Continuity 16](#_Toc131357545)

[New Incident Response Process 17](#_Toc131357546)

[Impact 17](#_Toc131357547)

[Application 17](#_Toc131357548)

[Impact 19](#_Toc131357549)

[Financial and Legal Implications 20](#_Toc131357550)

[Security Test Plan 21](#_Toc131357551)

[Scope 21](#_Toc131357552)

[Resources 21](#_Toc131357553)

[Hardware and Software 22](#_Toc131357554)

[Tools 23](#_Toc131357555)

[Timeline and Benchmarks 24](#_Toc131357556)

[Approach 25](#_Toc131357557)

[Risk Remediation 26](#_Toc131357558)

[Security Controls 26](#_Toc131357559)

[Vulnerabilities 27](#_Toc131357560)

[Evaluation 29](#_Toc131357561)

[Conclusion 29](#_Toc131357562)

[Communication 29](#_Toc131357563)

[Organizational Culture 30](#_Toc131357564)

[Reputation 31](#_Toc131357565)

[Recommendations 31](#_Toc131357566)

[References 33](#_Toc131357567)

Introduction:

Limetree Inc. is a research and development firm specializing in healthcare and biotechnology, with extensive experience in conducting research projects for both the federal government and private corporations. With a team of highly qualified and dedicated professionals, Limetree Inc. is committed to developing innovative solutions that advance the fields of healthcare and biotechnology.

In recent years, Limetree Inc. has established itself as a growing player in the research and development industry. The company's focus on healthcare and biotechnology has allowed it to build a strong reputation for producing cutting-edge research, with many of its projects having received industry recognition. Limetree Inc.'s team of experts includes research scientists, engineers, and healthcare professionals, all of whom are committed to pushing the boundaries of what is possible in their respective fields. The company's culture of collaboration and innovation is reflected in its work, with each project benefiting from the unique perspectives and expertise of its team members. One of Limetree Inc.'s key strengths is its ability to partner with both government agencies and private corporations. This has allowed the company to develop a diverse range of projects that have significant implications for the healthcare and biotechnology industries. By collaborating with a wide range of partners, Limetree Inc. can access cutting-edge technology and expertise, further enhancing its ability to deliver innovative solutions. Overall, Limetree Inc. is a dynamic and forward-thinking research and development firm that is dedicated to advancing the fields of healthcare and biotechnology. Its ability to produce groundbreaking research and collaborate with a range of partners makes it an ideal partner for anyone looking to advance innovation in these areas.

As a company that deals closely with healthcare providers, Limetree Inc. is subject to the same laws and regulations. Laws such as the Health Insurance Portability and Accountability Act of 1996, (HIPAA), and the Health Information Technology for Economic and Clinical Health Act (HITECH), are in place to ensure that companies handling sensitive information, such as patient health information (PHI), properly protect this information. “HIPAA meets this goal primarily through its privacy rule, security rule and breach notification rule. Covered Entities such as physicians, hospitals and insurers were initially the only entities required to comply with these rules. The increased use of digital media for storage and transmission of PHI led to the passage of the Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009. One effect of HITECH was the requirement that business associates of covered entities comply with many of the regulatory requirements that had generally only been applicable to covered entities, fully implemented by 2013. A business associate is defined by the U.S. Department of Health and Human Services as “a person or organization that conducts business with a covered entity that involves the use or disclosure of individually identifiable health information” (Ezold, 2019). While this is a broad definition, it does mean that Limetree Inc. is responsible for adhering to these laws and regulations and ensuring that this information is secure and protected.

Security Breach:

Attack Location:

Based on the provided scenario and the results of the interview with Limetree Inc’s security manager, Jack Sterling, it is suspected that the organization was breached through its network. The breach is suspected to have resulted in the theft of personal health information (PHI) that was used in a research study. Through the interview, it was revealed that Limetree operates a non-segmented network that allows incoming FTP and Telnet inbound connections. While the network is password protected, the password is handed out to visitors when they check in at the front the desk. The network is protected by a firewall with logging enabled, however the network switches do not log any information and the SQL database has logging enabled but with minimal disk space resulting in it being overwritten regularly as new log files are created. The information stored in the database is not encrypted. Remote employees access the network through a VPN but use laptops with unencrypted hard drives. Employees are also permitted to use personal devices on the network. These multiple issues lead to the belief that the attack took place through the company network as many different avenues onto the network were left open allowing access controls to be bypassed or simply passed as normal traffic.

Attack Method and Type:

The reasoning for the network being the suspected means of attack has been explained. The method of attack must be speculated but based on the provided information, there are three entry points that could have been the vector for attack.

First, the company does not segment their network and allows visitors to connect to it when they check in. This could indicate that the attacker initially entered the network by visiting the company and receiving the network log in information. From here, the attacker could have used an SQL injection. “Unmoderated user data inputs could place organizational networks at risk of SQL injection attacks. Under the network attack method, external parties manipulate forms by submitting malicious codes in place of expected data values. They compromise the network and access sensitive data such as user passwords. There are various SQL injection types, such as examining databases to retrieve details on their version and structure and subverting logic on the application layer, disrupting its logic sequences and function” (Forcepoint, 2023). Since the attacker would already be on the network using this method, they would have had ample opportunity to perform his attack on site, however, they could have also installed malware that allowed them remote access after they left. Since employees are only required to update their anti-virus/anti-malware software monthly, the attacker could have used a malware version that was new and not currently supported by the current version of McAfee they had installed on devices.

The second method of attack is like the first, however the malware could have been delivered through an employee device that was infected before being connected to the company network. This infection could have stemmed from a social engineering/phishing attempt that the employee fell for on their personal device. “According to ISACA’s State of Cybersecurity 2020 Report, social engineering is the most popular network attack method, with 15 percent of compromised parties reporting the technique as the vehicle of infiltration. Social engineering involves elaborate techniques in deception and trickery techniques — phishing — that leverage users’ trust and emotions to gain access to their private data” (Forcepoint, 2023).

The last potential method of attack could have been using Telnet or FTP. These protocols are not secure and should not be used. FTP and Telnet utilize plain text authentication meaning they transmit data in plaintext that can be intercepted. This could result in falling victim to a man-in-the-middle attack in which the attacker intercepts the traffic being transmitted and steals employee credentials, then using the stolen credentials to access and steal sensitive information.

Vulnerabilities:

Based on the speculation that the network was attacked through access gained by either visiting the company, an employee’s personal device or through an employee’s remote connection, there are a number of vulnerabilities that could have aided in the ability of the attacker to carry out the breach.

The first major vulnerability is the lack of network segmentation on the Limetree Inc. network. “Network segmentation is when different parts of a computer network, or network zones, are separated by devices like bridges, switches and routers” (Landsberger, 2020). By having a network set up in a way that keeps everything connected, instead of segmented into zones, the company is relying solely on its firewall and anti-malware software to protect it. But what happens when someone is already on the network, such as a visitor who was given access? “Firewalls have to do far too much these days: From real-time learning behavioral analytics all the way down to allowing necessary cookies for user experience. Firewalls are very strict and follow established firewall rules, but they don’t do everything to protect your digital assets. What’s more, they can quickly become an outdated generation firewall. Your static IP addresses deserve to be protected, and they need backup beyond the front lines. What happens when a threat actor penetrates the firewall via a phishing attempt, for example? Systems and services need to be isolated from one another to prevent a small breach from becoming a massive incident that leads to a data breach. It’s one thing to have your smart lighting system compromised, but it’s another to have your customer data stolen. These are both virtualized functions for many businesses, but they are not nearly the same in terms of risk and liability. If the business in the above example practices proper network segmentation and is hacked via their smart lighting system (this isn’t uncommon), the threat actor will find another obstacle. Basically, it’s like turning a corner within a hedge maze to find a dead end: the threat actor will have to work their way backward and attempt to find other access points to the systems and data they are attempting to compromise. At this point, most cybercriminals are going to get discouraged and look for an easier target” (Landsberger, 2020). Take for example the Home Depot hack of 2014. This data breach occurred because a hacker was able to access the point of sale terminals and steal information off the RAM of the computers used to process payments. The hackers gained access to the Home Depot network through a third party contractor’s credentials and because Home Depot failed to segment their network, were able to work their way through the network ending with a connection to the POS systems.

The second major vulnerability Limetree Inc. has is that they still use FTP and Telnet connections and allow these ports to remain open to inbound traffic. FTP and Telnet are referred to as “clear text” protocols. That means that these protocols transmit data in plain text and unencrypted. Utilizing these protocols to establish a remote connection, even if through a VPN, leaves the information open to interception and allows anyone viewing it to read it. This means any time an employee logs into the company network remotely, their log in information is transmitted in plain text for anyone to intercept and steal. This leaves the company open to man-in-the-middle attacks that could allow an attacker to steal employee credentials and gain access to the network, bypassing all firewalls, to steal whatever information they want from the company.

The third major vulnerability of Limetree Inc. is the failure to use any form of encryption on the storage media and SQL databases housing sensitive information. This is in direct violation of HIPAA law. “According to HIPAA, encryption software must meet minimum requirements relevant to the state of that information, whether it is at rest or in transit:

1. When data is **“at rest”**, it is inactive and stored in a digital medium such as a server hard drive or SSD. This can also mean that the data is sitting on a mobile device like a tablet or phone.

At rest, HIPAA defines valid protocols as consistent with [NIST Special Publication 800-111](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf), “Guide to Storage Encryption Technologies for End User Devices”. This publication outlines the proper technologies used for secure storage, including advanced cryptography, full-disk and virtual disk security, and the encryption of mobile devices.

1. When data is **“in transit”,** it is actively moving between a sender and a destination. This can include sharing PHI between two health care providers via [email](https://www.kiteworks.com/secure-email/hipaa-compliant-email/) or other software, transmitting to cloud storage, or transmitting between central servers and mobile devices.

In transit, HIPAA cites [NIST Special Publications 800-52](https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final) “Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations” and [800-77](https://csrc.nist.gov/publications/detail/sp/800-77/rev-1/final) “Guide to IPsec VPNs”. These publications outline proper procedures for securing data.

Through these guidelines, providers can make reasonable decisions about what kinds of security they should use” (Lau, 2021). Failure to meet this legal requirement left the company data out in the open and able to be stolen as it was taken in plain text form.

The final major vulnerability that could be attributed to causing this data breach was the allowance of personal devices to be used on the company network for conducting business. By allowing this, the company facilitated employees using unregulated and uncontrolled devices on the network exposing the network to any threats that were housed on these devices. Because these devices cannot be controlled by the company, these personal devices could have carried malware and other threats that allowed an attacker to gain access to the company network once the infected device was connected to the network. Through this, the attacker then had free reign over the system and combined with the other vulnerabilities, would have been able to take whatever they wanted off the network.

Incident Response:

Purpose:

An Incident Response Plan is intended as a guide and framework for how an organization prepares, detects, analyzes, contains, eliminates, and recovers from any computer incident that can occur. An Incident Response Plan serves to uphold the CIA triad of confidentiality, integrity, and availability of data and information. “The purpose of the CIRT plan is similar to the purpose of a disaster recovery plan (DRP). By taking the time to create a plan, critical thinking can be applied to potential problems, the advice of experts can be sought, and the best types of responses can be researched. However, if a plan is not in place, these benefits are not available to responders when the incident occurs, which leaves them no choice but to use trial-and-error techniques. These impromptu techniques may succeed, but, on the other hand, they may allow the attacker to continue and cause significantly more damage to the organization. A CIRT plan outlines the purpose of the response effort, which is, in general, to identify the incident as fully as possible and then contain it. Answering the five W’s is a good starting point. They are what, where, who, when, and why. For good measure, how it occurred can be added” (Gibson & Igonor, Managing Risk in Information Systems, 2022). By providing employees and security personnel a framework on how to prepare and respond to any incident that occurs, the guideline sets out a general procedure to be followed to direct staff through the process of incident response to resolve the issue, eliminate the threat, and recover any salvageable information that may have been lost or stolen. The Incident Response Plan serves as a preparation tool as much as it does a guideline during an event. Preparation for an event and learning from an event after they happen is crucial to combat future threats and limit potential damage to the company, whether financial or reputational.

Examples:

Gibson and Igonor define a computer incident as “a violation or imminent threat of a violation of a security policy or security practice. It includes any adverse event or activity that affects the security of computer systems or networks. These adverse events affect the organization’s security and may result in loss of confidentiality, integrity, or availability” (Gibson & Igonor, Managing Risk in Information Systems, 2022). It is important that an incident be defined by the company to allow team members to understand what is considered an incident. Failure to define this for employees can lead to relying on a vague understanding and potentially different definitions being thought to be the case, preventing everyone from properly identifying potentials incidents that need to be reported as every employee is vital in the identification of potential incidents and threats regardless of their department of specialty. An example of a computer incident is unauthorized access. “Unauthorized access occurs any time an attacker is able to access data without authorization. Unauthorized access can be gained from different types of social engineering attacks and from technical attacks used to gain access or control to systems. Unauthorized access often results in loss of confidentiality” (Gibson & Igonor, Managing Risk in Information Systems, 2022).

Unauthorized Access is a common occurrence in many industries and has been reported by multiple companies who have fallen victim to it. Unauthorized access can occur for many reasons, improperly configured security features such as firewalls, successful phishing attempts made against employees, poor information protection practices by employees or contracted partners. Attackers will use any avenue they find to access information they think they can reap for financial or causal gain.

Home Depot recently settled a lawsuit from a data breach they experienced in 2104. The attacker gained access to PII of customers through access gained from a 3rd party contractor. Home Depot failed to segment their store networks which allowed the attack to steal credit card information from their point-of-sale systems because the POS systems were connected to the same network the contractor had access too (Lukic, 2020). A similar breach occurred at Target in 2013, the attacker gained access through a 3rd party vendor and stole 40 million credit and debit records (Jones, 2021). Another example of unauthorized access is the Capital One data breach of 2019. From their website, disclosing information about the breach, Capital One states “On July 19, 2019, we determined that an outside individual gained unauthorized access and obtained certain types of personal information about Capital One credit card customers and individuals who had applied for our credit card products” (Capital One, 2021). First Financial Corporation was victim to one of the largest breaches in history in 2019. “This data breach was unique in the sense that there was not a breach in the company's servers, but an authentication error, meaning no authentication was required to view documents. There was a common web design error called Insecure Direct Object Reference (IDOR), which basically means that anyone who searches the direct link will have access to it. Once a single link is found, cyber criminals can use Advanced Persistent Bots (APBs) to collect and index the remaining documents. This error went undiscovered for years. The New York DFS alleges that First American failed to follow its own policies, neglecting to conduct a security review or a risk assessment of the flawed computer program” (Todd, 2022). A final example is the Equifax data breach of 2017. “In 2017, an application vulnerability in one of their websites lead to the breach. The breach went undiscovered for months. The company has been faulted for a number of security and response lapses, the application vulnerability being prime among them. Inadequate system segmentation made lateral movement easy for the attackers. The sensitivity of the compromised information of this data breach makes it particularly unique” (Todd, 2022).

Roles and Responsibilities:

The NIST identifies several team models for an Incident Response Team in their NIST SP 800-61 Rev. 2 publication. Of those identified, the Central Incident Response Team model is best for Limetree Inc. because they are a single location business and can benefit from the use of a single, centralized team. This will benefit Limetree by having on-sight team members that can support employees when questions arise or guidance on how to proceed with any suspected threats. This team should be comprised of individuals from multiple backgrounds to provide a broad skillset. Team members can fill multiple roles and may be likely given that Limetree is a relatively small company. The roles necessary for the team are that of Team Lead, Information Security specialists, Network Administrators, Physical Security, and then support from Legal and Human Resources should also be incorporated. The responsibilities of the Incident Response Team span a broad scope. They are responsible for every stage of incident response and as a result must continually prepare, monitor, and address potential threats brought to their attention. “Some of the primary responsibilities of the CIRT include:

* **Developing incident response procedures**—These procedures can be generic procedures to respond to any type of incident or detailed checklists for different types of incidents. For example, malware infections and DoS attacks may each have its own checklist.
* **Investigating incidents**—When an incident occurs, the CIRT is responsible for responding to and investigating it. Depending on the priority and impact of the incident, a single team member may respond. For high-priority, high-impact incidents, the entire team may respond.
* **Determining the cause of incidents**—One of the goals of an investigation is to determine the cause because, by understanding the cause, the CIRT is better able to determine the best response. For example, a user brings in an infected universal serial bus (USB) flash drive from home. After plugging it into the system, the antivirus software detects and quarantines it. Thus, the cause was from the user transferring the virus from home to the work computer via the USB drive. Luckily, the antivirus software detected it, but, unfortunately, some viruses bypass the antivirus software. This type of incident has caused many organizations to outlaw USB flash drives on their networks.
* **Recommending controls to prevent future incidents**—CIRT members often know the best solution to prevent the same incident again. Even if they don’t know it already, they have the expertise and experience to identify a control, which may be as simple as upgrading the security policy or more complex and require the purchase and installation of hardware or software. Either way, the CIRT members provide the recommendation.
* **Protecting collected evidence**—Evidence should not be modified when it’s collected. For example, police officers don’t walk through the blood at a crime scene because doing so would affect the evidence. Similarly, CIRT members should not modify the evidence, such as accessing files or turning off the computers, unless they’ve captured the RAM content if that is desired. They use bit copy tools to copy hard drives to get a complete copy without modifying the data.
* **Using a chain of custody**—CIRT members are responsible for managing the evidence as soon as they collect it. A chain of custody helps ensure that the evidence presented later is the same evidence that was originally collected. It should be established when evidence is seized and maintained throughout the life of the evidence. The chain of custody log documents who had the evidence at any moment and when the evidence has been secured in a semipermanent storage location.” (Gibson & Igonor, Managing Risk in Information Systems, 2022)

Current incident Response Process:

Limetree currently has no official documented process for incident response. The policy practice currently falls to system administrators to report incidents brought to their attention if deemed relevant. These reports go to the IT manager before being judged whether they are necessary to be forwarded to the security manager. Additionally, Limetree has no documentation of past events and any corrective measures taken in response to past events are not documented in any way. This entire process causes problems and fails to allow Limetree to prepare, identify, or respond to incidents as they occur. Under the current practice, the entire reporting process is subjective and as stated earlier, because an incident isn’t even defined in policy by the company, what qualifies as an incident is left to the opinion of whichever system admin receives a report from an employee. Because of this subjective nature for determining an incident, there is no consistency in what gets passed on to management as it is left up to different system admins each day.

To add to this, the lack of documentation makes it impossible for Limetree to properly learn from past incidents. Preparation is the first step of incident response, as part of preparation, this includes lessons learned from past events, which is the last step of incident response. Without properly documenting the incident response process, the company cannot learn and adapt to a changing threat landscape and the incident response cycle is broken before it ever begins.

Actions and Business Continuity:

Due to the lack of documentation, it can only be speculated that the security vulnerabilities that were disclosed as being the suspected cause of the recent data breach at Limetree were resolved as per the interview with Jack Sterling where he stated, “Corrective measures are taken immediately after an incident, though none of the measures was ever documented.” This is the only basis known for assuming that the vulnerability was resolved but because of the failure to have an implemented Incident Response Plan and policies surrounding Incident Response and proper documentation of events and actions taken, this information can only be inferred based on the interview and cannot be verified at this time. Implementation of an Incident Response Plan and policies is vital to create a paper trail of events and actions taken to remediate any causes identified as well as help to protect Limetree in the event of legal action taken against them for the loss of PII.

While it would seem the recent data breach did not inhibit normal operations at Limetree, the failures displayed by the company to address, resolve, and document the incident put the company in a position that fails to allow the company to protect itself in the event further action is taken against them, whether this comes from a regulatory body or further attack from bad actors. The need for documenting the process used to identify, contain, and resolve a breach is exacerbated by the fact that no previous incidents or resolutions can be referenced because of the lack of documentation by the company. While the company has not experienced a breach that has shut down their operations, the likelihood of this occurring if the current practices are not changed increases on a regular basis.

New Incident Response Process:

Impact:

Application:

Limetree Inc. has governmental and industry regulations it must adhere to within its given sector of business. Because Limetree works within the healthcare industry for its research and development work, the major law it falls under the jurisdiction of is the Health Information Portability and Accountability Act (HIPAA). “There are three major areas that HIPAA covers in terms of compliance: administrative (ways to protect patient data and ensure that it can be accessed only by authorized parties), physical (ways to prevent physical theft and unauthorized access to systems with protected data), and technical (using technology to protect computer networks and devices from threats)” (Gibson & Igonor, Managing Risk in Information Systems, 2022, p. 57). HIPAA will come into effect depending on the work Limetree is conducting at any given time and could have an impact depending on that work.

While falling under HIPAA as a healthcare provider is unlikely for Limetree, it is important to understand when it could have come into effect. More commonly, based on the work Limetree performs, they will fall under the Health Information Technology for Economic and Clinical Health Act, commonly referred to as the HITECH act. The HITECH act works in conjunction with HIPAA, “HITECH strengthened HIPAA in a number of ways. Most importantly, the reach of the HIPAA Security Rule was extended to Business Associates of Covered Entities, who also had to comply with certain Privacy Rule standards and the new Breach Notification Rule. The Act did not make compliance with HIPAA mandatory as this was already a requirement, but it introduced a new requirement for Covered Entities and Business Associates to report data breaches – which ultimately enabled the Department of Human Services´ Office for Civil Rights to step up enforcement action against non-compliant organizations.” (The HIPAA Journal, 2023).

The industry regulations Limetree needs to be concerned with are the standardization recommendations put out by entities for the promotion of protection, innovation, and to uphold the CIA triad. Special Publications put out by the National Institute of Standards and Technology in the U.S. are a major part of the IT industry and recommends the industry standard and recommended best practices for IT processes and procedures. A global entity of a similar nature is the International Organization for Standardization (ISO). The ISO also publishes standards that are recognized as industry standards such as ISO 27002 – Information Security Controls, ISO 31000 – Principles and Guidelines on Implementation, and ISO 73 - Risk Management.

Impact:

These regulations require careful consideration when they come into effect. For HIPAA, it has a certain time it must be considered for research organizations. “A researcher is a covered health care provider if he or she furnishes health care services to individuals, including the subjects of research, and transmits any health information in electronic form in connection with a transaction covered by the Transactions Rule. See 45 CFR 160.102, 160.103. For example, a researcher who conducts a clinical trial that involves the delivery of routine health care, such as an MRI or liver function test, and transmits health information in electronic form to a third-party payer for payment, would be a covered health care provider under the Privacy Rule. Researchers who provide health care to the subjects of research or other individuals would be covered health care providers even if they do not themselves electronically transmit information in connection with a HIPAA transaction, but have other entities, such as a hospital or billing service, conduct such electronic transactions on their behalf” (National Institutes of Health, 2007). This is an important rule because in conjunction with HITECH, those that fall under HIPAA authority were expanded to include business associates. “The HITECH Act of 2009 applied the HIPAA Security and Privacy Rules to Business Associates and made them directly liable for their own compliance with HIPAA. Business Associates now had to sign a Business Associate Agreement with the Covered Entity on whose behalf they were processing PHI and had the same legal requirements as the Covered Entity to protect PHI and prevent data breaches. Business Associates were also required to report data breaches to their Covered Entities.” (The HIPAA Journal, 2023)

Further, compliance with industry standards from NIST and ISO, while they have minor differences, is a road map that allows companies a pathway to improve their organizations reputation as trustworthy. The NIST does not offer any form of certification but serves as a cheaper beginning path to meet industry standards before further reaching for ISO certification that is offered through a third-party audit. “ISO 27001 accreditation certifies that your company follows information security best practices and provides an impartial, professional assessment of whether or not your personal and sensitive data is effectively safeguarded” (Siddiqui, 2023). Achieving accreditation through compliance and successful audit of ISO standards can serve to further Limetree’s reputation and overcome negative effects on reputation from prior security incidents.

Financial and Legal Implications:

The security breach of a business, such as Limetree, that handles protected health information (PHI) can have significant financial and legal implications under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Financial implications:

* The business may face fines, penalties, and legal fees. HIPAA noncompliance can result in fines ranging from $100 to $50,000 per violation, up to a maximum of $1.5 million per year. HITECH can add up to $1.5 million per incident. These fines can quickly add up, depending on the scope of the breach.
* The business may also face class action lawsuits by individuals affected by the breach. These lawsuits can result in large settlements, which can have a significant monetary impact on the business.

Legal implications:

* The business may have to report the breach to the Department of Health and Human Services (HHS) and notify affected individuals. Failure to report the breach can result in additional fines and penalties.
* The business may have to implement corrective action to prevent future breaches. The HHS may require the business to implement specific security measures, policies, and procedures to ensure compliance with HIPAA and HITECH regulations.
* The business may also face investigations by federal and state regulators. The investigation process can be time-consuming and costly, and the results can have a significant impact on the business's reputation and bottom line.

Security Test Plan:

Scope:

The scope of a risk assessment for Limetree Inc. should include the following:

1. Identify all types of data held by the company, including sensitive data such as personal health information (PHI) used in research studies and intellectual property related to the company's research and development projects.
2. Assess the potential impact of a security breach on the confidentiality, integrity, and availability of the company's data and systems. This includes evaluating the potential financial, legal, and reputational consequences of a breach.
3. Evaluate the current security posture of the company's systems and processes, including access controls, authentication mechanisms, network security, data encryption, and incident response procedures.
4. Assess the level of compliance of the company with established cybersecurity standards such as NIST, ISO 27001, and HIPAA, as well as any other relevant regulatory requirements that impact the company's operations.
5. Identify and prioritize the risks associated with the company's systems and processes, based on the likelihood and potential impact of each risk.
6. Develop a risk mitigation strategy that includes recommendations for addressing the identified risks, such as implementing new security controls, enhancing existing processes, or improving employee training programs.
7. Develop a risk management plan that includes regular monitoring and testing of the company's systems and processes to ensure ongoing compliance and effectiveness of the risk mitigation strategy.

Resources:

Based on the scope of the risk assessment outlined, the following resources will be required:

1. Information Security Experts: The risk assessment should be led by an experienced information security professional or team, who can conduct a thorough assessment of the company's systems, processes, and controls, and identify potential risks and vulnerabilities.
2. Data Classification Experts: The team should include experts in data classification and handling, who can identify the types of data held by the company, including sensitive data such as personal health information (PHI) used in research studies and intellectual property related to the company's research and development projects.
3. Technical Experts: The team should also include technical experts with knowledge of the company's infrastructure, network architecture, and systems, who can assess the technical risks associated with the company's operations.
4. Legal Experts: Legal experts with knowledge of the regulatory and compliance requirements that impact the company's operations, such as HIPAA and other relevant standards, should be included in the team to ensure that the risk assessment is comprehensive and meets all legal requirements.
5. Tools and Technology: The risk assessment team will require tools and technology to conduct vulnerability scans, penetration testing, and other assessments of the company's systems and processes. This may include network and application scanning tools, data encryption software, and intrusion detection and prevention systems.
6. Documentation: The team will require access to relevant documentation, such as policies, procedures, and other internal documents that describe the company's security controls, processes, and systems. The team should also document their findings and recommendations for risk mitigation.
7. Time and Budget: Conducting a comprehensive risk assessment requires significant time and resources. The team will need to allocate sufficient time and budget to conduct a thorough assessment, analyze findings, and develop a comprehensive risk mitigation strategy.

Hardware and Software:

The following is a list of the system hardware and software that should be included in the risk assessment:

1. Network Infrastructure: This includes routers, switches, firewalls, and other network devices that are used to connect the company's systems to the internet and to each other.
2. Servers: The company's servers should be evaluated, including both physical and virtual servers. This includes file servers, application servers, database servers, and any other servers that store and process company data.
3. Workstations: The company's workstations, including desktops and laptops, should be evaluated. This includes an assessment of the operating systems, software applications, and user accounts on each workstation.
4. Mobile Devices: The company's mobile devices, including smartphones and tablets, should be evaluated. This includes an assessment of the operating systems, applications, and security controls on each device.
5. Cloud Infrastructure: The company's cloud infrastructure, including any cloud-based servers, storage, or applications, should be evaluated.
6. Databases: The company's databases should be evaluated, including an assessment of the type of data stored in each database, the database management system (DBMS) used, and the security controls in place to protect the data.
7. Security Software: The company's security software, including antivirus, intrusion detection and prevention systems (IDS/IPS), and security information and event management (SIEM) systems, should be evaluated.
8. Backup and Recovery Systems: The company's backup and recovery systems, including both hardware and software solutions, should be evaluated to ensure that data can be recovered in the event of a security breach or other disaster.
9. Access Controls: The access control systems used by the company, including authentication mechanisms such as passwords and biometrics, should be evaluated.
10. Incident Response Systems: The company's incident response systems, including policies, procedures, and technologies used to detect and respond to security breaches, should be evaluated.

Tools:

There are several tools that will be necessary to conduct a risk assessment on Limetree’s systems. These tools will allow a full analysis of the network and systems configurations used by Limetree to allow it to address identified vulnerabilities and make necessary changes to improve its security posture. The following tools are recommended for conducting a comprehensive risk assessment:

1. Vulnerability scanning tools: These tools scan the network infrastructure, servers, workstations, and other devices to identify known vulnerabilities and misconfigurations that could be exploited by attackers.
2. Penetration testing tools: These tools simulate real-world attacks to identify vulnerabilities and weaknesses in the network and systems.
3. Network mapping and discovery tools: These tools help in identifying all devices and applications connected to the network, and their respective roles and interconnections.
4. Application security testing tools: These tools evaluate the security of software applications used by the company, including web applications and mobile applications, to identify any vulnerabilities that could be exploited by attackers.
5. Security information and event management (SIEM) tools: These tools collect and analyze security-related data from various sources to detect and respond to security incidents.
6. Firewall configuration analysis tools: These tools evaluate the firewall configuration settings and assess the security posture of the network perimeter.
7. Data loss prevention (DLP) tools: These tools monitor and protect sensitive data to prevent unauthorized access or leakage of information.
8. Identity and access management (IAM) tools: These tools manage and monitor access to critical systems, applications, and data by ensuring that only authorized users have access to them.
9. Backup and recovery testing tools: These tools verify the integrity and availability of backup data to ensure that critical systems and data can be recovered in case of a security breach or disaster.
10. Risk management and compliance tools: These tools provide a framework for managing risk and compliance related to cybersecurity, including mapping to industry standards and regulatory frameworks.

Timeline and Benchmarks:

1. **Day 1-7: Initial Assessment**

* Conduct a preliminary investigation to identify the type of breach and affected systems
* Compile a list of potential security incidents that may have led to the breach
* Initiate containment measures to prevent further damage or data loss
* Notify relevant stakeholders, including the executive team, IT department, and legal counsel

1. **Day 8-21: Investigation and Risk Assessment**

* Perform a comprehensive risk assessment of the systems and applications affected by the breach
* Analyze the data collected from various sources to identify the root cause of the breach
* Conduct forensic analysis to determine the extent of data loss and impact on the organization
* Identify and prioritize critical assets and data that need to be protected
* Develop and implement an incident response plan

1. **Day 22-30: Remediation and Recovery**

* Develop a plan for restoring affected systems and data
* Implement remediation measures to address identified vulnerabilities and risks
* Monitor systems and network traffic to detect any further signs of intrusion
* Conduct follow-up assessments to verify the effectiveness of remediation measures

1. **Day 31 onwards: Ongoing Monitoring and Maintenance**

* Establish ongoing monitoring and maintenance processes to maintain the security posture of the organization
* Conduct regular vulnerability assessments and penetration testing to identify potential security gaps
* Monitor network traffic and system logs for signs of suspicious activity
* Develop and implement security policies and procedures to promote a culture of security awareness and best practices among employees.

Benchmark data:

* Time to detect and contain incidents: According to a report by IBM Security, the average time to detect and contain a breach is around 280 days (IBM Security, 2021). Limetree Inc. should aim to reduce this time by implementing automated detection and response systems.
* Incident response plan effectiveness: The effectiveness of an incident response plan is measured by the time it takes to contain and remediate a security incident. The National Institute of Standards and Technology (NIST) recommends a maximum time to respond to a security incident of one hour and a maximum time to recover of 30 days (National Institute of Standards and Technology (NIST), 2018). Limetree Inc. should aim to reduce the time to resolution to less than 30 days.
* Vulnerability remediation: According to a report by the Ponemon Institute, the average time to remediate a vulnerability is around 60 days (Ponemon Institute, 2021). Limetree Inc. should aim to reduce this time by prioritizing critical vulnerabilities and implementing remediation measures promptly.

Approach:

My recommended approach would be to follow a risk management framework to identify, assess, and mitigate potential security risks. Specifically, I would use the NIST Cybersecurity Framework (NIST CSF) to guide the risk management process. The NIST CSF provides a flexible and customizable approach to cybersecurity risk management and is widely used by organizations of all sizes.

My approach would begin with a comprehensive risk assessment of the systems and applications affected by the breach. This assessment would identify critical assets and data that need to be protected and prioritize vulnerabilities and risks based on their potential impact on the organization. Using this information, I would work with the IT department to develop and implement an incident response plan that outlines procedures for containing and remedying security incidents.

In addition to the incident response plan, I would establish ongoing monitoring and maintenance processes to maintain the security posture of the organization. This would include regular vulnerability assessments and penetration testing to identify potential security gaps, as well as the implementation of security policies and procedures to promote a culture of security awareness among employees.

Throughout the risk management process, I would ensure compliance with relevant cybersecurity standards and regulations, such as HIPAA for healthcare organizations. I would also work closely with legal counsel to manage any legal or regulatory requirements resulting from the security breach.

Risk Remediation:

Security Controls:

1. Implement multi-factor authentication: Require all users to use multi-factor authentication when accessing sensitive systems or data. This would help prevent unauthorized access even if a user's credentials were compromised.
2. Conduct regular security awareness training: Train all employees on cybersecurity best practices and provide regular updates on the latest threats and attack vectors. This would help ensure that employees are aware of the risks and know how to avoid them.
3. Encrypt sensitive data: Implement encryption on sensitive data both in transit and at rest. This would help protect data in case of a breach and prevent attackers from accessing sensitive information.
4. Regularly patch and update systems: Ensure that all systems and applications are regularly patched and updated to address known vulnerabilities. This would help prevent attackers from exploiting known vulnerabilities to gain access to systems or data.
5. Perform regular security assessments: Conduct regular security assessments to identify and address potential security weaknesses before they can be exploited. This would help ensure that the organization's security posture is up-to-date and effective against the latest threats.

Vulnerabilities:

The security controls proposed can mitigate risks by reducing application, website, and network vulnerabilities. For instance, implementing multi-factor authentication can help prevent unauthorized access even if a user's credentials are compromised, thereby reducing the risk of data breaches through phishing attacks and other social engineering techniques. As noted by the National Institute of Standards and Technology (NIST), multi-factor authentication provides a higher level of security than traditional passwords and can significantly reduce the risk of unauthorized access (National Institute of Standards and Technology (NIST), 2017).

Conducting regular security awareness training can also mitigate risks by reducing the likelihood of human error and providing employees with the knowledge and tools needed to recognize and avoid potential threats. As noted by the National Cyber Security Alliance (NCSA), security awareness training is essential in helping employees understand their role in keeping sensitive data secure (National Cyber Security Alliance (NCSA), n.d.).

Encrypting sensitive data is also an effective way to reduce vulnerabilities, especially when data is stored or transmitted over public networks. By using strong encryption algorithms, attackers will find it difficult to decrypt the data, reducing the risk of data breaches. NIST recommends the use of strong encryption algorithms and keys to protect sensitive data at rest and in transit (National Institute of Standards and Technology (NIST), 2017).

Regularly patching and updating systems can help reduce vulnerabilities by ensuring that all known security flaws are addressed in a timely manner. This reduces the risk of exploits, malware infections, and other cyber threats that may take advantage of vulnerabilities in outdated software. NIST notes that organizations should implement a robust patch management system to ensure that all systems and software are up-to-date with the latest security patches (National Institute of Standards and Technology (NIST), 2019).

Finally, performing regular security assessments can help identify potential vulnerabilities and security weaknesses before they can be exploited. This can include penetration testing, vulnerability scanning, and other security testing techniques. By identifying and addressing vulnerabilities in a timely manner, organizations can reduce the risk of security incidents and minimize the impact of any breaches that do occur. NIST recommends regular security assessments as part of a comprehensive security program (National Institute of Standards and Technology (NIST), 2017).

Evaluation:

Measuring and evaluating security controls are important to ensure their effectiveness and to determine if they have been properly implemented. The criteria for measuring and evaluating security controls include four key factors: confidentiality, integrity, availability, and accountability (Junejo & Sahito, 2021). Confidentiality is the ability to prevent unauthorized access to sensitive information. Integrity is the ability to maintain the accuracy and completeness of data. Availability is the ability to ensure that information and systems are accessible when needed. Accountability is the ability to track and audit the actions of users and systems.

To ensure that security controls are properly implemented, it is important to establish performance metrics that can be used to evaluate the controls. Metrics can include factors such as the number of incidents or breaches, response time to incidents, and the effectiveness of the controls in preventing or mitigating incidents. Regular testing and auditing can also help to ensure that security controls are functioning as intended and that any vulnerabilities are identified and addressed (National Institute of Standards and Technology (NIST), 2018).

It is also important to establish roles and responsibilities for monitoring and evaluating security controls. This can include assigning specific individuals or teams to regularly review and test the controls and report on their effectiveness to management. Regular training and education on security best practices can also help to ensure that personnel understand their roles and responsibilities for maintaining security controls.

Conclusion:

Communication:

During the risk assessment process, the risk assessment team may encounter interpersonal communication issues that can hinder progress and negatively impact the team’s effectiveness. These issues can include poor listening skills, differences in communication style, and conflicts between team members (Hemmatian & Parsa, 2019). If not addressed, these issues can result in misunderstandings, delays, and inaccurate risk assessments.

To resolve interpersonal communication issues, the risk assessment team can implement various strategies. For example, the team can establish clear communication protocols, such as regular team meetings and progress reports, to ensure that all team members are informed and up to date on the assessment progress (Hemmatian & Parsa, 2019). Additionally, the team can provide training on effective communication skills and conflict resolution techniques, which can help to promote better communication and collaboration between team members (Layton & Smith, 2017).

Another strategy is to establish a team leader who can serve as a mediator and facilitate communication among team members. The team leader can help to resolve conflicts and ensure that all team members are heard, and their opinions are considered (Hemmatian & Parsa, 2019).

Organizational Culture:

A security breach can have a significant impact on the organizational culture of a company. One of the challenges that may arise is a loss of trust between employees and management, as employees may feel that management did not take the necessary steps to prevent the breach or adequately protect their data (Srivastava, Bhatnagar, & Sharma, 2017). This loss of trust can lead to a decrease in employee morale, job satisfaction, and engagement, which can ultimately impact productivity and performance.

Another challenge is a potential shift in the company's culture towards a more risk-averse and security-focused mindset. While this shift can be beneficial in terms of improving the company's security posture, it may also lead to a more rigid and inflexible organizational culture, which can hinder innovation and creativity (Cao, Wilkin, & Lim, 2018). Therefore, it is important for the company to strike a balance between security and flexibility to maintain a positive and innovative organizational culture.

Reputation:

A security breach can have a significant impact on the reputation of a business or organization. In addition to the financial costs associated with a breach, such as regulatory fines and legal fees, companies may also face reputational damage and loss of customer trust (Yeo & Huang, 2016). This can lead to a decrease in sales and revenue, as customers may be hesitant to continue doing business with the company following a breach.

Moreover, the impact of a security breach on the reputation of a business can extend beyond immediate financial losses. Negative publicity and media attention can lead to long-lasting reputational damage and loss of brand value (Moustakas, Katsikas, Kavakli, & Gritzalis, 2020). Therefore, it is critical for companies to prioritize information security and take proactive measures to prevent breaches and protect sensitive data.

Recommendations:

To reduce the impact of communication and organizational cultural issues in future risk assessments, it is important to establish clear communication channels and encourage open dialogue among all stakeholders. This includes ensuring that all team members have a clear understanding of their roles and responsibilities and are adequately trained in communication skills. It is also essential to establish a culture of trust and collaboration, where team members feel comfortable sharing their concerns and ideas without fear of retribution or criticism.

One effective way to reduce communication and cultural issues in risk assessments is to engage in regular team-building activities and training sessions. This can include activities such as team-building exercises, cross-functional training sessions, and communication workshops. These activities can help to foster a sense of teamwork and collaboration among team members, which can improve communication and reduce the likelihood of cultural misunderstandings.

Moreover, it is essential to establish a culture of continuous improvement and learning, where team members are encouraged to share feedback and suggestions for improving the risk assessment process. This can help to identify areas of improvement and ensure that the risk assessment process is continually evolving to meet the changing needs of the organization.

# References

Cao, J., Wilkin, C. L., & Lim, J. (2018). The Impact of Cybersecurity Breaches on the Performance of Breached Firms. *Journal of Management Information Systems, 35*, 1030-1061.

Capital One. (2021, February 22). *Information on the Capital One cyber incident*. Retrieved from Captial One: https://www.capitalone.com/digital/facts2019/

Ezold, C. (2019, June 5). *HIPAA’s Business Associate Traps for Biotech and Life Sciences*. Retrieved from Law: https://www.law.com/thelegalintelligencer/2019/06/05/hipaas-business-associate-traps-for-biotech-and-life-sciences/?slreturn=20230119180053

Forcepoint. (2023). *What is a Network Attack?* Retrieved from Forcepoint: https://www.forcepoint.com/cyber-edu/network-attack

Gibson, D., & Igonor, A. (2022). *Managing Risk in Information Systems.* Burlington: Jones & Bartlett Learning.

Gibson, D., & Igonor, A. (2022). *Managing Risk in Information Systems.* Burlington: Jones & Bartlett Learning, LLC.

Hemmatian, A., & Parsa, S. (2019). The role of leadership in managing and improving team communication. *Journal of Management Research in Iran, 23*, 165-186.

IBM Security. (2021). *Cost of a Data Breach Report 2021*. Retrieved from IBM Security: https://www.ibm.com/security/data-breach

Jones, C. (2021, October 26). *Warnings (& Lessons) of the 2013 Target Data Breach*. Retrieved from Red River: https://redriver.com/security/target-data-breach#:~:text=What%20Happened%20During%20the%20Target,was%20one%20of%20the%20largest.

Junejo, A. K., & Sahito, S. A. (2021). Security metrics evaluation framework for cyber security assessment. *Computers & Security, 107*.

Koester, R. J. (2017). *Risk assessment communication strategies: Best practices for success*. Retrieved from American Society of Safety Professionals: https://www.assp.org/docs/default-source/future-focused/feature-articles/risk-assessment-communication-strategies\_best-practices-for-success.pdf?sfvrsn=7b378647\_2

Landsberger, D. (2020, October 23). *What Is Network Segmentation and Why It Matters?* Retrieved from CompTIA: https://www.comptia.org/blog/security-awareness-training-network-segmentation

Lau, V. (2021, March 31). *HIPAA Encryption: Requirements, Best Practices & Software*. Retrieved from Kiteworks: https://www.kiteworks.com/hipaa-compliance/hipaa-encryption/#:~:text=Does%20HIPAA%20require%20encryption%3F,there%20are%20very%20specific%20exceptions.

Layton, R., & Smith, B. (2017). *Communication and interpersonal skills for risk management.* Palgrave Macmillan.

Lukic, D. (2020, December 18). *Home Depot Data Breach, How Did it Happen*. Retrieved from ID Strong: https://www.idstrong.com/sentinel/home-depot-could-data-breach/

Moustakas, E., Katsikas, S., Kavakli, E., & Gritzalis, S. (2020). Corporate reputation in the context of cybersecurity incidents. *International Journal of Information Management, 51*.

National Cyber Security Alliance (NCSA). (n.d.). *Security Awareness Training*. Retrieved from National Cyber Security Alliance (NCSA): https://staysafeonline.org/cybersecurity-awareness-training/

National Institute of Standards and Technology (NIST). (2017). *Cryptographic Standards and Guidelines*. Retrieved from National Institute of Standards and Technology (NIST): https://csrc.nist.gov/publications/detail/sp/800-175b/final

National Institute of Standards and Technology (NIST). (2017). *Multi-Factor Authentication (MFA) for E-Commerce*. Retrieved from National Institute of Standards and Technology (NIST): https://csrc.nist.gov/publications/detail/nistir/8144/draft

National Institute of Standards and Technology (NIST). (2017). *Security Assessment and Authorization*. Retrieved from National Institute of Standards and Technology (NIST): https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

National Institute of Standards and Technology (NIST). (2018). *NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.* Retrieved from National Institute of Standards and Technology (NIST): https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

National Institute of Standards and Technology (NIST). (2018). *Computer Security Incident Handling Guide*. Retrieved from National Institute of Standards and Technology (NIST): https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

National Institute of Standards and Technology (NIST). (2019). *Patching Enterprise Systems and Software*. Retrieved from National Institute of Standards and Technology (NIST): https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8267.pdf

National Institutes of Health. (2007, February 2). *Frequently Asked Questions - HIPAA Privacy Rule for Researchers*. Retrieved from National Institutes of Health: https://privacyruleandresearch.nih.gov/faq.asp#18

Ponemon Institute. (2021). *The Cost of Data Breach Report 2021*. Retrieved from Ponemon Institute: https://www.ibm.com/security/data-breach

Siddiqui, M. (2023). *NIST vs. ISO –What You Need To Know*. Retrieved from CyberSaint Security: https://www.cybersaint.io/blog/nist-vs.-iso-what-you-need-to-know

Srivastava, S. C., Bhatnagar, J., & Sharma, A. (2017). Impact of cyber security breaches on organizational performance: An empirical study. *Information Systems Frontiers, 19*, 225-238.

The HIPAA Journal. (2023). *What is the HITECH Act?* Retrieved from The HIPAA Journal: https://www.hipaajournal.com/what-is-the-hitech-act/

Todd, D. (2022, September 14). *Top 10 Data Breaches of All Time* . Retrieved from Secure World: https://www.secureworld.io/industry-news/top-10-data-breaches-of-all-time

Yeo, G. T., & Huang, W. (2016). The impact of data breaches on firm reputation and customer loyalty: A study of Australian companies. *Journal of Computer Information Systems, 56*, 85-94.

# 