Security Breach Analysis and Recommendations

Brett Logan

Southern New Hampshire University: Global Campus

ISE 510: Security Risk Analysis & Planning

Instructor: Dr. Errol Waithe

September 24, 2021

Table of Contents

Security Breach Analysis and Recommendations

I. Introduction

Limetree Inc. (henceforth referred to as Limetree) is a rapidly growing research and development firm focused on healthcare, biotechnology, and other cutting-edge industries. Working alongside such partners as the federal government and private organizations, Limetree seeks to implement a strong and vigorous information security program in order to enhance its reputation and maintain regulatory compliance. While surging growth indicates a successful operation, it has also led to an increase in security vulnerabilities, and recently Limetree fell victim to a security breach. The breach is thought to have included confidential data related to research studies, including personal health information (PHI). In an effort to learn from this event, and prevent a recurrence, this security assessment has been commissioned.

II. Security Breach

Security Breach: Attack Location

The security breach occurred in Limetree's open-space office environment. While this type of environment is meant to encourage healthy and collaborative work among employees, it also presents unique security challenges: "having an open floor plan tips the balance between private and public and this shift majorly affects how proprietary and sensitive company information is protected" (Ponemon 2014). The workspace areas where Limetree employees are working on research and development projects, often consisting of sensitive information, lack of any kind of partitions or cubicles, offering direct line of sight to documents and computer screens.

Surrounding these workstations, the management and executive offices are located around the perimeter of the space, with glass doors again offering line-of-site opportunity.

Security Breach: Attack Method and Type

It is believed that the attacker successfully took advantage of the poor security awareness of Limetree Inc. employees in several ways. The most plausible method is that a visitor to the office was able to access an employee's unattended laptop or open computer workstation, logging in to a database with a password that had been recorded in a journal that was left open on a desk. Once in the system, the attacker could then have accessed the unencrypted files containing personal health information, and downloaded them to a removal storage device. This theft was enabled by the fact that there is no logging of network activity on any switches, and no encryption for sensitive data at rest within the SQL server environment.

Security Breach: Vulnerabilities

Numerous vulnerabilities in Limetree's operating environment contributed to the security breach and continue to create an increased threat level. These vulnerabilities can be broken down into categories as follows: systems security, personnel and administrative security, and physical security.

Systems security vulnerabilities include issues such as the lack of encryption or activity logging, which have been discovered when the breached data was leaked. Had Limetree utilized encryption or hashing for its SQL database, the attacker could have potentially only stolen unreadable data: "SQL server encryption is a process to encrypt connections (i.e. links), data and procedures that are stored in a database...the various areas that are needed to be covered to secure

SQL Server are the platform, authentication, objects mainly data and applications that access the system" (TechAffinity 2020). Information garnered in the interview with security manager jack Sterling has also revealed vulnerabilities such as:

- MS Edge browser security settings set to low.
- Lack of logical separation between environments (public-facing web server is part of the local area network (LAN).
- Use of FTP instead of SFTP.
- Reliance on only firewalls rather than an intrusion detection and prevention system.
- Wireless network using clearly advertised SSID on LAN (it would be more secure to create a dedicated guest network).
- No baseline from which to compare anomalous/malicious network activity.

This access could not have occurred as it did without the poor security awareness of the personnel, leading to personnel and administrative vulnerabilities such as passwords being written down and left out in the open. This too was made worse by the overall design of Limetree's environment, being open enough that a visitor could scan it in its entirety looking for potential weakness, "visual hacking, or the act of viewing or capturing sensitive, confidential and private information for unauthorized use, is a major data security risk in the age of the open-office floor plan" (Ponemon 2014). Users were also in charge of updating their own virus software rather than having this task carried out by the network administrator.

Finally, physical vulnerabilities such as portable hardware being left unattended and computer terminals left running and unlocked made the entire event successful. Having access to an unlocked workstation made the task of stealing data much quicker and easier for the attacker to

accomplish: “in the past few years, more than 250 million confidential business records were reported lost or stolen and those data losses did not all originate from external threats...whether knowingly or unknowingly, employees engage in behaviors that heighten the risk of data loss – and leaving your computer unlocked is one of them” (Jackson 2020). Keeping data backups on-site is also an additional vulnerability in the event of flood, fire or other disaster. In summary, among the many vulnerabilities that made the security breach possible are the open design of the office environment (lack of privacy precautions), passwords being written down and left in the open, computer workstations being left unlocked while unattended, lack of database encryption, poor network practices and configuration, lack of documentation policies, and lack of network activity monitoring.

III. Incident Response

Incident Response: Purpose

The purpose of the incident response plan is to ensure that Limetree Inc. can effectively deal with security threats by creating structure and guidance: “having an incident response plan means the right people, with the right skillsets and experience, know what procedures to follow to contain and remediate a cyber security threat” (Fox 2020). With procedures in place ahead of time, the organization assumes a proactive rather than reactive security posture, ensuring successful targeted response, investigation and remediation of threats.

Incident Response: Examples

One type of incident that may occur is unauthorized access. This occurs when someone without permission gains entry to Limetree's network, data, applications, devices, secured locations (e.g., server room), or anywhere else that is unintended by the organization. The risk of unauthorized access is considerable: "the most common threat in a networked system is unauthorized access to information and computer resources (information technology system)...this may cause the loss of confidentiality, integrity, and availability of the information technology assets" (Hau 2003). Causes of unauthorized access can include weak passwords, compromised accounts, insider threats, and malware. The following are examples of this type of incident:

- Tailgating. This is among the most common type of unauthorized access, and it occurs when an unauthorized person immediately follows an authorized person through a door and into an area they do not have permission to be in: "often the user will hold the door for an unauthorized individual out of common courtesy, unwittingly exposing the building to risk" (Laughlin 2015).
- Door Propping. At times doors are propped open to make access to different rooms easier and more convenient for building occupants, however this also enables access for anyone regardless of permission or credentials.
- Collusion. This is similar to tailgating, however the person being followed is purposely allowing it to happen, thereby granting access to a non-credentialed person.
- Compromised Password. Passwords that are improperly stored or easy to guess can give malicious actors access to networks and information they should not have access to. This can be seen in the evaluation if Limetree's physical environment in which passwords are left written on post-it notes. In addition, the current practice of

allowing employees to choose the length and complexity of their passwords increases the risk of this threat.

- Malware: “malware and viruses (viruses are a type of malware) are a set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer system or network without the permission of the owner” (NCSL 2020). Once inside the Limetree network, malware can access sensitive files and even encrypt, erase, or modify data.

Incident Response: Roles and Responsibilities

The stakeholders involved in a security incident are varied and diverse. As a company, Limetree must understand and embody the notion that it takes the actions of all to support and protect the organization. Each member has their own roles and responsibilities when faced with an incident and they can be described as follows:

- *Senior Management.* It is up to senior management (CEO, CISO, CIO, etc.) to coordinate and direct Limetree’s response to a security incident. This includes holding daily briefings in which progress is examined and input from various departments can be collated.
- *Limetree Inc. Employees.* As a primary line of defense, employees must be proactive and embody a “see something, say something” mindset. Reporting directly to system administrators, employees should not hesitate to immediately report any suspected incident, unusual/suspicious activity, or anything else they feel is atypical. Employees will have a participatory role in the incident response, as directed by the IT

manager. This may include pertinent actions such as unplugging devices from the network and awaiting further direction.

- *HR.* HR will act as directed by the security manager (Jack Sterling) and/or senior management team to utilize access controls in mitigating an incident. Network access may need to be restricted, passwords reset, or accounts frozen. Additionally, HR will be tasked with working in communication with law enforcement contacts.
- *Systems Administrators*. Provide analysis and technical advice. When notified by employees of a potential incident they must begin precautionary measures and immediately inform IT manager. Administrators may also be responsible for helping with investigation and/or remediation.
- *Network Administrator*. Responsible for daily data backups, an important factor in a data breach in which data is stolen or encrypted by ransomware. These backups must be protected and secure.
- *IT Manager*. The IT manager is responsible for reviewing all events reported by the administrators or employees. Using an incident triage matrix to determine the severity and impact of the incident, the IT manger then determines priority and escalates to, and works in conjunction with, the security manager.
- *Security Manager (Jack Sterling)*. Working alongside security personnel and in direct communication with senior management, Mr. Sterling is responsible for determining the incident response and directing execution.
- *Legal Counsel.* Once notified of an incident such as the data breach that occurred, "the first phone call made by an in-house counsel notified of a major data breach should be to outside counsel, who can better protect the integrity and confidentiality of the

incident response. Third-party experts, such as forensic examiners, should often be retained by outside counsel in order to follow court precedent regarding the scope of the attorney-client privilege during breach response" (Rogers and Singleton 2018). The Limetree team is responsible for ensuring laws and regulations are adhered to throughout the response process.

- *Marketing*. Any security incident has the potential to severely impact he brand and reputation of Limetree. The marketing department will work as directed by senior management to assist in the public response to the incident and help guide social media communications and community outreach.
- *Customer Service*. Customer service personnel must prepare to execute prepared responses to the incident when contacted by customers or members of the public. They should refrain from making statements prior to being briefed, and are responsible for coordinating with marketing to influence public opinion and guide the perception of the incident.
- *Security Incident Response Team (SIRT).* This newly developed team can consist of inside or outside individuals, and it will carry out the bulk of investigative, containment, eradication, and response efforts during an incident.

Law Enforcement Contacts. Depending on the type of incident and potential for laws to be broken, law enforcement contacts will need to be notified and included in the investigation process.

Incident Response: Current Incident Response Process

The current incident response process at Limetree consists of a simple notification chain and no documentation or reporting procedures. When an incident occurs, system administrators are notified, who then escalate to the IT manager. If the incident is deemed relevant, the IT manger then reports it to the security manager. Despite past incident occurrences, there is no previous documented history, and no record of corrective measures that were taken. This is an issue because without proper documentation of what works and what doesn't, administrators cannot learn from past occurrences and apply known effective mitigation techniques. This puts more strain on resources by necessitating more time and effort be taken in addressing critical security incidents rather than quickly applying corrective measures that were successful in the past. Additionally, having records and documentation will help Limetree Inc. maintain regulatory compliance and bolster potential legal defense. Current status quo is to take protective measures immediately after an incident, and this practice should undergo review to ensure that hasty actions are not preventing proper identification of attack methods, and/or impacting the collection of forensic evidence.

Incident Response: Actions

Several orchestrated actions must occur to effectively address and mitigate a security incident. In the previous breach, a Limetree employee suspected that their workstation had been accessed while they were away. Notification of system administrators occurred, who then confirmed that the employee's username and password was utilized by an unknown actor. Immediately escalating to the IT manager with this information, the IT manager contacted Jack Sterling to direct incident response. Due to lack of current record keeping or documentation, it is unknown

what specific steps Sterling took in addressing the suspected breach, beyond asking HR to change passwords and informing legal of the breach.

Actions that *should* occur in the event of an incident:

- *Detection and Analysis.* At this phase the suspicious employee immediately contacts Limetree's IT Manager. Information gathered includes affected assets and systems, as well as the potential impact on Limetree's network and operations. The IT manager, using an incident triage matrix to determine priority, reports to Jack Sterling who initiates the next step to include activation of the security incident response team.
- *Containment.* Sterling enacts several processes to lessen the event impact. HR is notified to restrict access and reset passwords, and a briefing with all key stakeholders occurs.
- *Eradication.* Network administrators conduct forensics backup, while security personnel eliminate the cause of incident. Affected stakeholders are notified while administrators conduct new vulnerability analysis.
- *Recovery.* The system returns to normal.

Post-Incident Activity. Documentation and reports are finalized, with records being kept for future reference and employee training.

Incident Response: Business Continuity

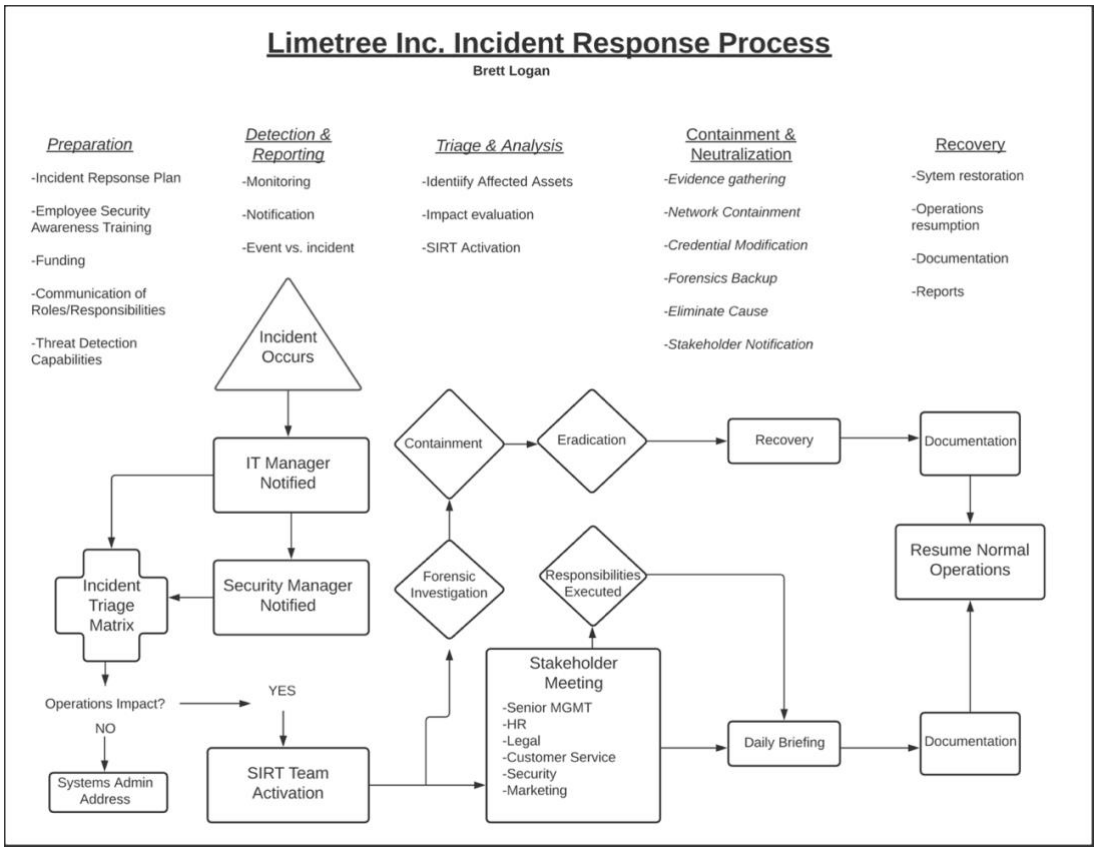
The resumption of business operations post-incident is of paramount importance. Without the ability to quickly pivot back to normal functions, Limetree Inc. faces a plethora of problems such as lost revenue, negative reputational impact, customer dissatisfaction, property damage, and more. The current incident response plan seeks to achieve business continuity by asking

employees to notify systems administrators of computer events, who then escalate to the IT manager. If the IT manager deems the event important enough, they notify the security manager. This process is inhibitive to business continuity due to the lengthy notification process and number of intermediary parties. In fact, this structure is detrimental to business continuity because it takes employees away from pertinent tasks. For example, when employees are notifying any/all systems administrators of all perceived incidents, the administrators must step away from their assigned security tasks. Furthermore, there is no contingency plan currently in place. To help decrease the time it takes to return to normal business operations, the SIRT team has been created. This team of experts will have pre-planned and practiced processes for addressing threats and will help ensure business continuity. Lack of network logging and intrusion prevention/detection systems is detrimental due to the fact that an attack could go undetected for lengthy periods of time, ultimately causing great harm and the potential for greater downtime or operations interruption, "breaches have gone undetected for weeks, months and sometimes years... the latest report from FireEye cites dwell time as 146 days on average globally" (Infocyte 2021). In the event of an incident limited in scope, or even during the remediation process, employees may still be able to work remotely via virtual private network, helping to continue operations.

One positive aspect of Limetree practices is the daily system backup conducted by the network administrator, allowing for a roll-back and data recovery if necessary. It should be noted, however, that these tapes are kept in the computer room, and in the event of a fire or disaster they could be compromised. It would be best to have encrypted copies securely stored offsite by a professional and insured third party. This would allow for the resumption of operations even in the event of disaster at the Limetree headquarters.

Incident Response: New Incident Response Process

The new incident response process utilizes the formation of a security incident response team (SIRT) and establishes an improved notification chain. The SIRT team will be tasked with carrying out the established incident response process once the security manager has deemed the impact on operations to be greater than zero. This team "must have the skills and experience to deal with a potentially high-stress situation... this will involve making key decisions, conducting an in-depth investigation, providing feedback to key stakeholders, and ultimately giving assurances to senior management that the situation is under control" (Fox 2020). The following flow chart illustrates this new incident response process in visual format:



IV. Impact

Impact: Application

The security breach that occurred involved the theft of confidential company data, as well as personal health information (PHI) that was used in a research study. This type of information is protected by industry regulations such as the health information portability and accountability act (HIPAA). Under HIPAA, organizations that retain PHI must take certain safeguards to protect it, and are required to notify individuals whose information may have been compromised during a breach. This regulation is especially relevant to Limetree Inc. because the lack of data encryption puts the company in violation of HIPAA and requires notifications to occur: "covered entities and business associates must only provide the required notifications if the breach involved unsecured protected health information...unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance" (HHS 2013).

Another relevant government regulation is the California Consumer Privacy Act (CCPA). The stolen PHI was part of a research study, making it likely that at least one study participant was a resident of the state of California: "California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or

reasonably believed to have been acquired, by an unauthorized person. (California Civil Code s. 1798.29(a)" (DOJ 2021).

Impact: Impact

Regulations such as these impact Limetree by requiring specific actions be taken in an effort to safeguard people's data. When a breach does occur, if it is found that these actions were missing or ignored, severe penalties can occur. Limetree must remain vigilant in adherence to all regulation, especially with regard to protected health information. An additional concern exists in any research projects undertaken in partnership with the federal government, as the information generated in these projects may be subject to further security standards, such as outlined in the NIST Publication 800-171, which provides requirements for protecting the confidentiality of controlled unclassified information. The ultimate impact is that Limetree must commit resources to meeting evolving regulations and ensuring that security practices are constantly up to date.

Impact: Financial and Legal Implications

A potential issue is the practice of Limetree employees using personal laptops for company work, which could include PHI. There is a higher degree of vulnerability in the theft/loss of these laptops when they leave the secure environment, which puts Limetree at great financial risk: "since 2010, federal HIPAA fines have ranged from $50,000 to more than $1.9 million for lost and stolen devices" (TMA 2019). In addition to HIPAA fines, violations of the CCPA can

also result in severe financial penalty: “CCPA fines start with civil penalties of up to $7,500 per violation. Statutory damages related to breaches range from $100 to $750 per consumer per incident or actual damages, whichever is greater... If 100,000 users within the database are impacted by a breach, for example, the total fine could reach $750 million” (Riskonnect 2021). In addition to California, each state can mandate its own data privacy regulations and levy fines if necessary. Such laws have gone into effect in states such as Nevada and New York in addition to California.

Legal implications of the data breach can be broken down into four areas:

- Notification, “In the United States, the attorney general of the appropriate state must be informed of a data breach incident. Other regulators include; the Federal Trade Commission (FTC), the Securities and Exchange Commission, the Federal Communications Commission (FCC), and the Consumer Financial Protection Bureau” (Taylor 2017).
- Response. How Limetree responds to a data breach affects the organization’s credibility, underscoring the importance of having a security incident response plan.
- Penalties. Penalties are dependent on the severity of the breach and jurisdiction, as well as demonstrated regulatory compliance.
- Litigation. Finally, litigation relating to the breach can occur if Limetree fails to:

“provide timely notice of the breach, as required by the data protection laws concerned; respond to the breach and endeavor to remedy or mitigate the damage caused; implement reasonable data security measures” (Taylor 2017).

V. Security Test Plan

Security Test Plan: Scope

This assessment is integral to Limetree's continued goal of monitoring and remaining compliant in any regulations impacting operations. Beyond this compliance, "risk assessments aren't only required under HIPAA (Health Insurance Portability and Accountability Act), but are also key in strengthening the IT team's and business leaders' knowledge of where the organization is most vulnerable, and what data is involved in higher-risk environments" (Furneaux 2021). Clearly stating the scope of this risk assessment is imperative because it serves many functions: "establishing the scope of the risk assessment helps organizations to determine: (i) what tiers are addressed in the assessment; (ii) what parts of organizations are affected by the assessment and how they are affected; (iii) what decisions the assessment results support; (iv) how long assessment results are relevant; and (v) what influences the need to update the assessment" (NIST 2012). For this assessment, the tiers addressed are two and three: business processes and information systems. This includes current practices relating to personnel/physical security, documentation, and network configuration. In terms of organizational applicability, the assessment will inform decisions related to information systems security and operational protocols. The results of this assessment shall remain valid until any changes are made to the Limetree network or employee security protocols, at which point a new assessment should be

conducted. Finally, the scope of this assessment can be defined in architectural/technical terms of protecting personal health information and preventing further data breaches.

Security Test Plan: Resources

The following resources will be required to carry out the risk assessment:

- NIST Special Publication 800-30: Guide for Conducting Risk Assessments.

This guide outlines the steps needed for a thorough and conclusive risk assessment, with multiple supporting appendices and graphics available for reference.

- Office of the National Coordinator for Health Information Technology (ONC) and HHS Office for Civil Rights (OCR) Security Risk Assessment Tool (SRA Tool).

Limetree operates in the healthcare industry and is subject to additional data safeguarding precautions. This tool has been designed to help ensure Limetree is conforming to industry standards and regulations: “the tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule and the Centers for Medicare and Medicaid Service (CMS) Electronic Health Record (EHR) Incentive Program” (HealthIT 2021)

- Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules.

These rules provide a framework to determine which information should be protected, therefor assisting in developing a threat/risk matrix.

- Team of certified IT professionals to carry out the assessment. Certifications might include Certified Penetration Tester, Certified Ethical Hacker, Security+, Certified Information Systems Security Professional (CISSP), or Certified Information Systems Auditor (CISA).

- Access to any logs, such as firewall logs.
- Security Manager Jack Sterling. It may be necessary to further interview or seek clarification from Mr. Sterling during the assessment. Additionally, his input and influence may be needed in achieving cooperation with employees and/or senior management.
- Assessment scales from NIST 800-30 as related to characteristics of adversary capability, intent, targeting, etc. These tables can be found in Appendix D.
- Common Vulnerabilities and Exposures (CVE) and National Vulnerability Database (NVD). These resources contain a large amount of information related to known threats and vulnerabilities and will be useful in considering if any of Limetree's applications contain vulnerabilities or weaknesses.
- Employee Interviews. These will be necessary to determine what security procedures are already in place, if they are followed correctly, and what the overall security culture at Limetree looks like.

NIST SP 800-171. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. This document outlines requirements for protecting information when working with the Federal Government.

Security Test Plan: Hardware and Software

The following hardware and software assets at Limetree are within target of the risk assessment:

<u>Hardware assets:</u>

- 3 web/applications servers
- 5 file and Printer Servers

- 2 proxy servers
- 7 Remotely manageable Cisco switches
- 250 Desktops
- 3 Firewall Devices
- 1 Router
- 3 wireless access points (WAP)

Software assets:

- MS Edge
- Firefox
- Google Chrome
- MS Office
- Adobe Flash
- Adobe Acrobat
- McAfee anti-virus deployed locally
- SQL Agent

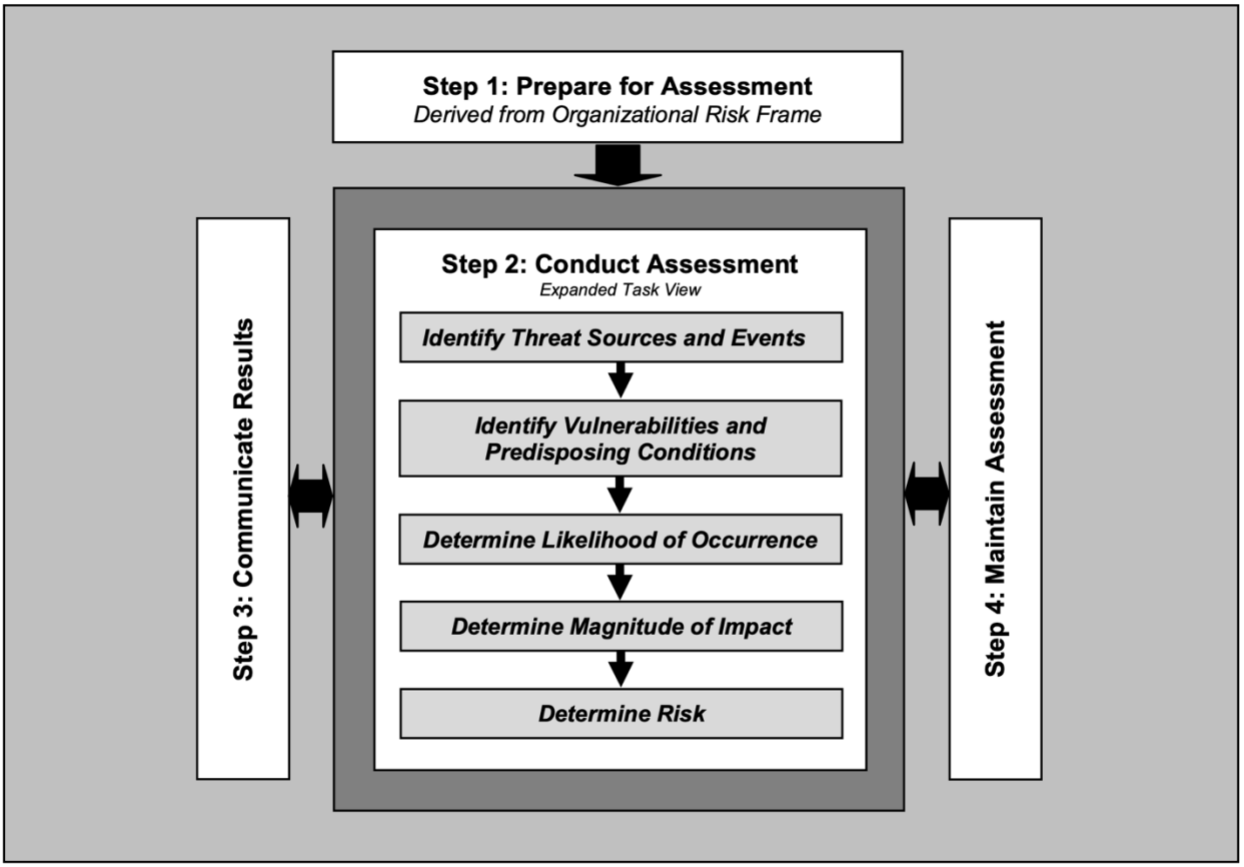
Tools

- Wireshark. This will be used to capture network traffic to determine access, communications, and vulnerabilities such as open ports.
- Kali Linux will be used for penetration testing and to ensure that any network configuration vulnerabilities are found and addressed to protect PHI.
- Risk Matrix

- Security Risk Assessment Tool (SRA), Department of Health and Human Services.

Security Test Plan: Timeline and Benchmarks

As per NIST 800-30 standards, the steps involved in the assessment will look as illustrated in the following graphic:



(NIST 2021)

- Step 1: Prepare for Assessment

Pre-assessment meeting to include non-disclosure agreement amongst participants.

Information Gathering.

- Step 2: Conduct the Assessment

Launch/execution of planned activities and testing.

Analysis.

Review/Compilation.

- Step 3: Communicate Results

Meeting with Assessment Team, Jack Sterling, and Management.

Includes reporting of results to board and necessary parties.

- Step 4: Maintain Assessment

This includes ongoing risk monitoring: “Risk monitoring provides organizations with the means to, on an ongoing basis: (i) determine the *effectiveness* of risk responses; (ii) identify risk-impacting *changes* to organizational information systems and the environments in which those systems operate;49 and (iii) verify *compliance*” (NIST 2021).

The total time allotted for steps one through three will be *30 days*, with step four requiring ongoing participation. As noted, any changes in the network infrastructure/configuration, or employee security processes necessitates the need for a new risk assessment. Benchmarking is important to ensure that Limetree stays on par or ahead of industry standards. We will look to current security statistics and metrics within the healthcare and biotechnology industries to maintain above -average results by consistently reviewing and comparing our performance to others in these industries. Also used will be the following:

- Center for Internet Security (CIS) Benchmarks: “CIS Benchmarks are frameworks for calibrating a range of IT services and products to ensure the highest standards of cybersecurity. They’re developed through a collaborative process with input

from experts within the cybersecurity community. There are more than 100 different benchmarks covering a range of well-known vendors and systems. CIS Benchmarks provide guidance for all areas of an IT network, including operating systems, server systems, office software and network devices (Nyhuis 2020)

- HIPAA Compliance. Working with PHI, it is imperative that Limetree meet or exceed benchmarks set by HIPAA, which will be achieved via adherence to HIPAA's five standards.

Security Test Plan: Approach

The approach to fulfilling the risk assessment will be attack-vector based. This is to take into account the overall lacking physical security protocols observed within the Limetree environment, as well as vulnerabilities identified in network configuration. This approach has been selected with consideration to the data breach that occurred, "from pre-exploitation (attack delivery via email, web or app), to exploitation (system compromise) to post-exploitation (e.g. lateral movement and data exfiltration) – challenging defenses deployed against each vector of the cyber-kill chain ensures you can defend against sophisticated cyber-attacks, such as advanced persistent threats (APTs)" (Wacshman 2019). Understanding the attack vector, or method, that the previous hackers have successfully utilized, will help Limetree eliminate vulnerabilities and reduce risk. It is important that this assessment be regarded by Limetree employees as a positive process to help enhance the security of their environment and processes, thus ensuring increased security culture and a demonstration of commitment to the highest standards. In an effort to better achieve this, all participants conducting the assessment will be instructed to approach the process with a positive and optimistic demeanor in all interactions.

Using the NIST special publication 800-30 as a guide, assessors will systematically examine the previously identified vulnerabilities in the Limetree environment and complete the following steps:

- Identify Threat Sources
- Identify Threat Events
- Identify Vulnerabilities and Predisposing Conditions
- Determine Likelihood
- Determine Impact
- Determine Risk

Once these steps have been fulfilled, communication of the results can occur and needed mitigation steps can be adopted.

VI. Risk Remediation

Risk Remediation: Security Controls

Future risks at Limetree can be mitigated via the adoption of security controls that help prevent a repeat security breach. There are three types of controls (physical, technical, and administrative) and three control functions: (preventative, detective, corrective), see figure below:

		CONTROL FUNCTIONS		
		Preventative	**Detective**	**Corrective**
CONTROL TYPES	**Physical**	Fences, gates, locks	CCTV and surveillance camera logs	Repair physical damage, re-issue access cards
	Technical	Firewall, IPS, MFA solution, antivirus software	Intrusion detection systems, honeypots	Patch a system, terminate a process, reboot a system, quarantine a virus
	Administrative	Hiring and termination policies, separation of duties, data classification	Review access rights, audit logs, and unauthorized changes	Implement a business continuity plan or incident response plan

(Walkowski 2019)

In order to mitigate future risks at Limetree and prevent a recurrent security breach, at minimum the following controls should be adopted:

- Implement an Access Control List (ACL): a table that tells the operating system which access rights each user has to a particular system object.
- Restrict Employee Software Downloads: downloads should be performed by the network administrator and pushed to employees.
- Employ Logical Separation Within Network: blocking traffic between different network segments to prevent unauthorized access or the dissemination of malware.
- Switch to Secure File Transfer Protocol (SFTP): ensures data/communications is encrypted and more secure.
- Create Separate Guest Network for Internet Access: can prevent malicious actors from accessing the Limetree LAN.

- Network Activity Logging: provides a baseline for network activity to help identify anomalous/suspicious behavior and assists in digital forensic investigation.
- Intrusion Detection and Prevention: to identify, log, stop, and report potential security incidents.
- Employee Security Training: to increase the overall security posture/culture at Limetree and address many vulnerabilities.
- Encryption: makes data unreadable to attackers.
- Documentation: helps in developing a security plan and assists in learning from previous incidents.

Risk Remediation: Vulnerabilities

As applied to the assessment of Limetree, these recommended security controls will address vulnerabilities in the following ways:

- Implement an Access Control List (ACL)
    - Currently employees have full access to the Limetree network, making it possible for anyone to access to the servers, (gateway) router, firewalls, switches, etc. Implementing an ACL will ensure that employees are only given sufficient access to those areas of the network that are necessary in completing their assigned duties/tasks, reducing the vulnerabilities of unauthorized access and disgruntled employee acting maliciously.
- Restrict Employee Software Downloads
    - Limetree uses the Microsoft Edge browser with low security settings, and remote downloads of applications is possible, making it vulnerable to allowing

malicious software downloads to occur. Creating a policy in which only the network administrator downloads software will lessen the likelihood of malware or viruses to making through our network defense through unintentional actions of employees.

- Employ Logical Separation Within Network
    - When the public facing web server is part of Limetree's local area network (LAN), and running File & Print services, Telnet, and IIS, it becomes vulnerable to hackers using techniques such as remote code execution and accessing unencrypted information. Separating these environments creates a security barrier between the public web server and the sensitive data that Limetree seeks to protect.
- Switch to Secure File Transfer Protocol (SFTP)
    - Limetree's current practice of using file transfer protocol (FTP) requires passwords for the transfer of data, which is typically transferred in clear text, making it vulnerable to an attacker's prying eyes. Additionally, data in transit can be intercepted. Switching to SFTP prevents this from happening by applying SHH2 Message Authentication Code (MAC) to hashed data payload packets which are encrypted in transit.
- Create Separate Guest Network for Internet Access
    - Creating segmentation between the guest wireless access and Limetree's LAN can help prevent unauthorized access from occurring.
- Network Activity Logging

- Logging network activity will create a baseline from which deviations from norm are exposed. This reduces the risk of a data breach by allowing for quick alert to suspected malicious activity or abnormal behavior.

- Intrusion Detection and Prevention
  - Another way to address the vulnerability of malicious activity going undetected and allowing for a breach or exfiltration of data, using an IDPS will block bad traffic ensure administrators are quickly alerted to potentially anomalous behavior.
- Employee Security Training
  - Perhaps among the most vital security controls needed, a new employee security training program at Limetree will help reduce a number of identified vulnerabilities. Enhanced training can address issues such as unlocked file cabinets, documents left on desks, unlocked workstations, poor password practices, phishing awareness, and more. Many physical vulnerabilities previously identified can be mitigated by proper employee training and adherence to policy.
- Encryption
  - Limetree currently utilizes unencrypted hard drives which increases the risk of data manipulation, theft, or destruction. All hard drives should be encrypted to address vulnerabilities relating to data breaches, as well as to adhere to regulatory compliance such as the Health Information Portability and Accountability Act (HIPAA)
- Documentation

- Proper documentation will mitigate risk by allowing Limetree to learn from previous security incidents and develop actions to prevent recurrence. Furthermore, a simplified template should be developed wherein Limetree employees can quickly and effectively document incidents.

Risk Remediation: Evaluation

Measuring and evaluating the effectiveness of the selected control methods should occur via regular audit and methodical procedure. While control self-assessments (CSA) can and should occur quarterly, a deeper understanding of effectiveness will occur if performance measures are developed specifically for each control. The following procedure has been developed for Limetree to carry out this task:

- Step 1: Establish a baseline in terms of overall functionality, operationality, behavioral norms, and activity at Limetree.

- Step 2: Prioritize the Control Measures
  - This can be accomplished via the creation of a matrix such as follows:

Consequence Level (of the risk)	Criticality of the Control	Assurance Priority	
Severe	3,4,5	1	It is critical that these controls are effective, therefore, they are the **number one priority** for the organisation's audit program. Where possible, external auditing should be utilised to provide further assurance
Major	4,5	2	It is important that these controls are effective, therefore, they are a **significant priority** for the organisation's audit program. Where possible, external auditing should be utilised to provide further assurance for the criticality 5 controls
Moderate	5	3	It is relatively important that these controls are effective. There is no requirement for external auditing.

(Paladin 2017)

- Step 3: Create a "Three Lines of Defense" System to determine whether the control method is effective at achieving the goal of mitigating risk, or if further audit/review is necessary to achieve this.

	1st Line of Defence	2nd Line of Defence	3rd Line of Defence
	Control self-assessment. This involves the control owner making a judgement in relation to the effectiveness of the control. It involves documenting the organisation's control processes with the aim of identifying suitable ways of measuring or testing each control. The actual testing of the controls is performed by staff whose day-to-day role is within the area of the organisation that is being examined as they have the greatest knowledge of how the processes operate	Line management review **or** Internal audit of controls against designated performance measures and key performance indicators. **Primary focus is on controls against risks with the highest level of consequence.** Outcomes of control audits provided to control owner. If any change to effectiveness the risk owner needs to be informed as this may change the level of the risk. Internal audit provides follow up to ensure that control improvements have been implemented within specified timeframes.	External audit conducted on specific controls. **Once again, the focus needs to be on controls against risks with the highest level of consequence.** Outcomes of audit findings are reported to the internal audit function for inclusion in reports to appropriate governance committees.
Assurance Priority	**Line of Defence to be engaged**		
Priority 1	x	x Internal Audit	x External Audit
Priority 2	x	x Internal Audit	x External Audit
Priority 3	x	x Line Management Review	x Internal Audit
All other controls	x		

(Paladin 2017)

- Step 4: Based upon the line of defense engaged, Limetree can determine whether or not the existing control is achieving success. For example, if the assessor (Jack Sterling) determines the control method 'Network Activity Monitoring' falls into assurance priority 2, and a CSA results in unsure judgement as to the effectiveness of this particular control, Sterling can escalate to the second line of defense and conduct a line

management review using performance measures and key performance indicators such as % of activity monitored, type of activity monitored, and number of malicious activity incidents detected. The most important part of evaluating the effectiveness of the controls is to create and update criteria and guidelines for what constitutes effectiveness or failure.

VII. Conclusion

Conclusion: Communication

The following interpersonal communication issues were encountered by the risk assessment team throughout the process of conducting the assessment:

- The prevailing attitude that information security is the sole concern of the IT department.
    - This was a common sentiment among Limetree employees, many of whom considered cyber security to be the domain of a single department within the organization. This is most likely related to the lack of security awareness training at Limetree and was resolved by conducting a townhall style meeting with the risk assessment team to educate, inform, and answer questions relating to the breach. Topics covered included phishing, physical security issues, and security vigilance.

- Failure to “see something, say something”

- Another communication issue observed was the tendency for employees to recognize potentially risky behavior (i.e., leaving workstations unlocked when away from desks), yet not raising any concerns with the workstation's owner or management. This was addressed by educating employees as to how the overall security at Limetree depends on its human assets and their choices/reactions, strengthening the "shared defense" mindset.

- Limetree employees afraid to communicate security concerns to "not rock the boat"
  - Employee interviews revealed that several practices and norms within the Limetree environment were concerning to employees, yet they did not feel confident or comfortable enough to communicate this to supervisors out of fear of being targeted or punished. This was resolved by developing an anonymous form which employees can now utilize to submit any concerns without fear of reprisal.

- The use of overly technical language when referring to/discussing cyber security and the breach that occurred.
  - Throughout the assessment it became clear that challenges and solutions were not being adequately communicated due to a tendency for IT and Security personnel to use language which other Limetree employees did not fully understand or grasp. This was remediated by reminding these departments that using specialized and technical language inhibits communication and special attention should be given to how IT concepts are communicated to other

departmental employees and management, emphasizing the "need to present technical security information to a variety of stakeholders, answer nontechnical questions, "translate" technical knowledge into business value, develop and write policies and build strong professional relationships" (Tollefson 2019).

- Lack of a defined process for communicating issues.
    - Limetree employees were instructed to notify system administrators of any issues, yet there was no prescribed way of doing so, leaving it up to individual employees. This was resolved with the creation of an incident report template that all employees will now use when raising concerns or reporting an incident.

Conclusion: Organizational Culture

The security breach led to several cultural challenges within Limetree that need to be addressed moving forward:

- Distrust
    - Data breaches damage trust within an organization, especially when potential vulnerabilities surrounding employee access to the breached data are revealed. This breach may have cause Limetree employees to become distrustful and/or suspicious of their fellow employees.
- Blame
    - Another negative emotional response to the breach is a tendency for employees and management to cast blame on others or other department for what

has occurred. This contributes to a deteriorating comradery within the organization and inhibits teamwork, cohesiveness, an job satisfaction.

- Shift from open-space working environment to a more private environment for security purposes.
    - As part of the remediation tactics aimed at preventing a recurrent breach at Limetree, the open-space office environment needs to be partially modified to enhance privacy, especially when displaying protected health information (PHI) on workstations. This alters the culture at Limetree by changing the prevailing carefree, easygoing attitude common amongst employees before the breach.

Conclusion: Reputation

Security breaches affect the reputation of organizations, often with lasting impact. At Limetree, this is especially important as the company works with the federal government and private corporations on a multitude of research projects, making maintaining a positive and reliable reputation extremely important to continue with these partnerships. A data breach that exposes PHI can result in research subjects withdrawing from the study or avoiding participation in future studies: “numbers highlight that consumers are not only skeptical of the organizations that have their sensitive information, but that they are willing to leave a company who goes through a data breach” (Neveux 2020). Additional effects include damage to the Limetree brand within the healthcare and biotechnology industries which it operates in: “a Forbes Insight report found that 46% of organizations had suffered reputational damage as a result of a data breach; 19% of organizations suffered reputation and brand damage as a result of a third-party security

breach. In other words, reputation is near impossible to fix once the public sees an organization in a bad light (Neveux 2020). Moving forward, the negative reputation impact of the data breach can even affect the ability for Lime tree to hire and retain top talent as individuals may be less likely to work for an organization who they consider to be "at risk" or potentially negative on their resume. Overall, the loss of trust and faith post-breach is deeply concerning and should be given special attention in remediation efforts.

Conclusion: Recommendations

The following recommendations have been devised to address the preceding communication and organizational culture issues by reducing their impact:

- Security Awareness Training
    - Aimed at addressing a variety of issues, properly implemented security awareness training can effectively change the attitudes and perceptions of Limetree employees regarding security responsibilities and communication of concerns. Trained employees are a better line of defense in preventing accidental errors that result in degraded security.

- Communication Processes Strategy/Policy
    - Aimed at enhancing the communication of complex problems and issues, developing a dedicated process for this will better enable employees and management to understand security risks and how their actions contribute or protect the organization from such risks. Enabling IT and Security personnel to

communicate better allows them to perform their work to greater effectiveness, bolstering the overall security culture at Limetree. Additionally, creating a template for reporting issues will result in streamlined evaluation and response to security incidents.

- Employee Empowerment Agenda
    - This agenda will result in employees who are not afraid to speak out when witnessing actions or behaviors detrimental to security at Limetree. The agenda will encourage employees to develop a pro-active and involved stake in the security of the Limetree environment and the protection of research subject data, based on the understanding that doing so results in a more successful operations to the benefit of all.

- Incident Response Plan
    - The development and implementation of an incident response plan will reduce the negative reputational impacts of security breaches by ensuring Limetree has an approved response timeline and tactics. Examples of the effectiveness at this in preventing reputational harm include the provision that Limetree should be the first to report/disclose a data breach to the public, something studies show to be extremely important in managing public opinion of a company post-breach: “The longer you wait to notify the appropriate people about the breach, the worse the consequences from consumers and authorities

may be. Uber, Equifax, and other high-profile data breaches suffered major criticism for the time they took to notify the public" (Hospelhorn 2020).

- Crisis Management Plan
    - As one of Limetree's major goals is to establish a strong reputation and robust information security program, developing a crisis management plan will help ensure that potentially influential occurrences such as the data breach are responded to and handled in ways that protect company reputation and ensure continued operations and profitability.

- Media training
    - It is recommended that a specific individual/s be tasked with coordinating media communications and the release of information in any future incident. This task must be undertaken with the understanding that all communications have the potential to either negatively or positively affect the public opinion, perception, reputation, and overall brand of Limetree. These key attributes can have a lasting impact on future operations, contracts, research partners, research studies, etc.

In closing, the data breach that occurred at Limetree Inc. proved to be a momentous event with high impact to the entire organization. The risk assessment that took place, and conclusions/recommendations generated, will serve to ensure this security incident provides a positive outcome for Limetree. The identification of vulnerabilities, analysis of their impact, and the creation of mitigation techniques and recommendations to address communication and

culture issues all come together to ensure a future in which Limetree achieves its goal of establishing strong industry reputation via the creation of a robust information security program. The first step in creating this program is to read, understand, and implement this document.

VIII. References

Department of Health and Human Services (HSS). 2013. HIPAA. Breach Notification Rule. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Furneaux, Allison. 2021. Cybersaint Security Blog. Tips For Your Next Risk Assessment Based On NIST 800-30. https://www.cybersaint.io/blog/risk-assessment-tips-based-on-nist-800-30

Fox, Neil. 2020. Varonis Data Security. What Is An Incident Response Plan and How To Create One. https://www.varonis.com/blog/incident-response-plan/

Hau, Dicky. 2003. SANS Institute. GSEC Practical Assignment, Version 1.4b, Option 1. Unauthorized Access- Threats, Risk, and Control. https://www.giac.org/paper/gsec/3161/unauthorized-access-threats-risk-control/105264

HealthIT. 2021. Security Risk Assessment Tool. https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

Hospelhorn, Sarah. 2020. Varonis Security. Analyzing Company Reputation After A Data Breach. https://www.varonis.com/blog/company-reputation-after-a-data-breach/

Infocyte, no author stated. 2021. Infocyte Blog. Breach Detection By The Numbers: Days, Weeks, or Years? https://www.infocyte.com/blog/2016/07/26/how-many-days-does-it-take-to-discover-a-breach-the-answer-may-shock-you/

Jackson, David. 2020. Net Standard. Why You Should Always Lock Your Computer. https://www.netstandard.com/always-lock-computer

Laughlin, Robert. 2015. Security Magazine. 5 Common Types of Unauthorized Access and How To Combat Them. https://www.securitymagazine.com/articles/86650-common-types-of-unauthorized-access-and-how-to-combat-them

National Conference of State Legislatures (NCSL). 2020. Computer Crime Statutes. https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx

National Institute of Standards and Technology (NIST). 2012. NIST Special Publication 800-30. Guide For Conducting Risk Assessments. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Neveux, Ellen. 2020. Secure Link. How Reputational Damage From A Data Breach Affects Customer Perception. https://www.securelink.com/blog/reputation-risks-how-cyberattacks-affect-consumer-perception/

Nyhuis, Michael. 2020. Diligent Insights. CIS Security Benchmarks and Compliance: What is CIS Compliance. https://insights.diligent.com/compliance/what-is-cis-compliance/

Paladin Risk Management. 2017. Risk Tip #2- How Do We Control Effectiveness? https://paladinrisk.com.au/risk-tip-2-measure-control-effectiveness/

Ponemon, Larry. 2014. CSO United States. Is The Open Floorplan Trend A Data Security Headache? https://www.csoonline.com/article/2597553/is-the-open-floor-plan-trend-a-data-security-headache.html

Riskonnect. 2021. Enforcement is Coming: How CCPA Fines Compare to GDPR. https://riskonnect.com/governance-risk-compliance/enforcement-is-coming-how-ccpa-fines-compare-to-gdpr/

Rogers, E. and Singleton, M. 2018. Access Data Group. Legal Team's Role In Investigating And Responding To Data Breach. https://www.michaelbest.com/portalresource/WPbreach

State of California Department of Justice (DOJ). 2021. Data Security Breach Reporting. https://oag.ca.gov/privacy/databreach/reporting

Taylor, Ben. 2017. The Data Privacy Group. https://thedataprivacygroup.com/blog/2019-9-17-data-breach-the-legal-implications/

TechAffinity. 2020. TechAffinity Blog. SQL Server Data Encryption At Rest- SQL Azure Database. https://techaffinity.com/blog/data-encryption-at-rest-sql-azure-db/

Tollefson, Rodika. 2010. InfoSec Research Institute. 5 Soft Skills You Need To Become A Successful Security Pro. https://resources.infosecinstitute.com/topic/security-pro-5-soft-skills/

Walkowski, Debbie. 2019. F5 Labs Application. What Are Security Controls? https://www.f5.com/labs/articles/education/what-are-security-controls

Waschman, Eyal. 2019. InfoSecurity Group. Building a Security Testing Plan. https://www.infosecurity-magazine.com/blogs/building-a-security-testing-plan/