

rISK ANALYSIS

Final Project



August 7, 2022

Guysell Dixson

Dr. Stuart McCubbrey

**Information Technology Structure**

ABC Healthcare is a startup company with 50 employees. Currently they have a Chief Information Officer (CIO), a newly hired IT network security officer and a network administrator. Their server contains patients’ health records which contains PHI, PII, billings, finances, and forms. Upon on looking at their information technology structure, I see that the network has been configured in a star topography running on a single switch. The router appears to be connected to wide area network (WAN) bringing the internet into the company’s local area network (LAN), but I do not see a firewall on the network between the WAN nor the LAN. From the switch it provides traffic control for ABC’s healthcare data server, the WIFI access point, the desktops for bookkeeping, HR management and the health records staff. The WIFI access point can be easily compromised because visitors and staff both use the same access points. Which can be assumed that it is not configured to deter any unauthorized users from attempting to gain access to the company’s network to cause damage. The data server is not protected from any unauthorized access. It should be placed in a DMZ to prevent data compromise.

**Cyberlaws and Ethics Regulations**

Even though ABC Healthcare is a startup company they must keep in mind that there are laws and regulations that they must abide by. Being in healthcare they automatically full under the laws of HIPPA, health insurance portability and accountability act. This law federally regulates the creation of a national standard to protect sensitive patient health information from being disclosed (HIPPA, 2002). This law helps to lower the chance of identity theft. Along with HIPPA, comes HITECH. HITECH is the health information technology for economic and clinical health act. This law ensures the privacy and security risk associated with electronic transmission of health information. Knowing that ABC Healthcare provides billing, it is safe to assume that they might have to handle patient’s credit cards. With that in mind ABC Healthcare will have to also follow the PCI DSS law or Payment Card Industry Data Security Standard was developed to minimize fraud and improve transaction security for the payment card industry (Woock, 2022). Lastly, for laws that should be followed, ISO/IEC 27001. This is the standards for all cyber active company to follow. The list of regulations covers acceptable use policies, asset inventory, asset configurations, patch configurations, password usage, clean desk/clean screen policy and help companies develop guidelines and procedures when it comes to information security (Williams, 2010).

When it comes to ethic regulations, ABC Healthcare should consider eHealth codes of ethics which are candor, honesty, quality, informed consent, privacy, professionalism in online healthcare, responsible partnering, and accountability (Mack, 2004).

**Organizational Ethics Violations**

ABC Healthcare is in violation of multiple violations that ranges from personal to professional. If not addressed these violations will lead to severe impact and consequences.

|  |  |  |  |
| --- | --- | --- | --- |
| **Violation (Personal/ Professional)** | **Code Broken** | **Regulation Governs** | **Impact to ABC Healthcare** |
| Lack of Firewall on network (professional) | ISO/IEC 27001  A.11.4.5 | Defines the requirement that perimeter firewalls must be installed between any wireless network and other networks containing sensitive data. | * Without the use of a firewall malware can easily spread throughout the network cause a total collapse of the network. This in terms means a loss of money and resources. |

|  |  |  |  |
| --- | --- | --- | --- |
| Non-sperate WIFI access point (professional) | ISO/IEC A.9.2.1  ISO/IEC A.10.1.2 | Governs how physical access to WIFI access point is appropriately restricted | * If left were visitors can access the same WIFI access point, hackers can gain access to the network and cause havoc or plant a bot to retrieve data without detection. |
| Improper disposal of PHI, PII (professional) | HIPAA Standard  164.310 (d)(2)(i) | Describes the formal procedures that safely and securely dispose of media that are no longer required. | * If sensitive data is not properly disposed of, like in the instant of documents left on the printer, patient’s PHI and PII will be exposed, and identity theft will happen. Alone with a lawsuit against ABC Healthcare. |
| Use of web for personal use (personal) | ISO/IEC 27001 A.7.1.3  A.15.1.2 | Appropriate and non-appropriate use of email and related resources | * Phishing scam * Download of viruses * Leak of company Data * PHI/PII exposed |
| Network using default settings (professional) | NIST SP 800-53 | Defines the requirement and procedures that must be followed to configure newly installed network components securely | * If devices are in default user mode, this makes it extremely easy for a hacker to look up the manufactures setting and gain access to ABC Healthcare network. Once inside the nightmares are endless. |
| Non-Acceptable use policy (professional) | ISO/IEC 27001 A.6.1.5 | Acceptable use Policy: what is acceptable and nonacceptable behaviors when using company’s resources. | * Viruses may be introduced unknowingly or maliciously. * Loss of employee. |

|  |  |  |  |
| --- | --- | --- | --- |
| Patient’s Information being overheard (professional) | HIPPA Privacy  164.528(a)(1) | Describes the incidental disclosure of patient’s PHI/PII | * Without a divider between departments, others can easily overhear private information about patients without their consent. This can lead to lawsuits or fines. |

|  |  |  |  |
| --- | --- | --- | --- |
| Video monitoring without staff knowledge(professional) | ISO/IEC 27001 A.9.1.5 | Describes use of video monitoring and access control.  Even though it is not required by the state to inform staff of monitoring, on an ethical level, staff should be informed to prevent self-incrimination. | * By allowing staff to know they have a chance to ensure that their actions are professional and compliant with company’s policies. This also creates a transparency within the company that hopefully the staff will understand what is private and non-private. |
| Non-BYOD policy (professional) | ISO/IEC 27001  A.9.1.5  HIPAA Standard  164.310(c) | Describes any policy and guidelines designed and implemented for working in areas that can access sensitive information. | * The impact on ABC Healthcare is patients’ PHI or PII can be removed from the property and disclosed to an unauthorized person. |
| Open cubicles | ISO/IEC 27001  A.9.1.3  HIPPA Standard  164.310(b) | Describes the appropriate use of workstations and the appropriate physical surroundings and physical safeguards of workstations that can access sensitive information. | * Runs the risk of shoulder surfing. * Actors gaining access to open computer screens. * Company could be fined if data is leaked containing PHI or PII. |

|  |  |  |
| --- | --- | --- |
| Cyberlaw Noncompliance | | |
| **Regulation** | **Example** | **Impact for noncompliance** |
| HIPPA: Protection of PHI  Protected health information. This contains individual identifiable heath information, name, SSN, demographic, insurance data, health information and address.  This dictates how this information should be destroyed, transmitted, and protected. | ABC Healthcare is in noncompliance by leaving patient’s information visible. By allowing documents to sit in an open area to be seen by everyone is a violation. The printer should be in a secure area and away from public eyes. Documents containing sensitive information should be always protected by the company. In accordance with HIPPA Security Rule system output displays rather it be printed pages, computer screens or other output devices should protect against shoulder surfing, visible displays and easily seen output. | If not mitigated or regulated to become compliance, as a government operated healthcare, ABC could lose all federal funding. They could also face a civil lawsuit or penalty up to $50,000 with an annual penalty cap of $1,500,000. |
| Training and Awareness.  Lack of training and awareness falls under Security Rule AT-2. It states that security training should meet applicable laws, directives, regulations, and policies. | Quoting,” there are no policies or guidelines for employees’ usage of the computers and network”. It can safely be said that security training and awareness is not a priority within ABC Healthcare and therefore, is not in compliance of even best practices within the information security, let alone within HIPPA, NIST, or FISMA. | Without a training and awareness program, ABC Healthcare will fall victim to data leakage, data loss and even worst system compromise and hacking. As a result, there will be fines, loss of reputation and lawsuits. |

|  |  |  |
| --- | --- | --- |
| Acceptable Use Policy  Without a guideline base to regulate use of company’s assets, team members will incidentally invite a virus or create a backdoor for attacks. According to ISO/IEC 27001, describes the appropriate and non-appropriate use of company’s resource. | Without any acceptable use policy, company resources can be exploited and misused. Team members can accidentally or incidentally download sensitive information to their devices and transport it off company’s property. Team members could use company WIFI to access personal emails or cloud-based data storage and inadvertently download malware or DOS. | Without the regulation of what is acceptable usage of company’s asset could be a high risk. Patients’ data could be leaked, and lawsuits could be filed. With HIPPA fines of up to $50,000 with an annual penalty cap of $1,500,000. |

|  |  |  |
| --- | --- | --- |
| Quality System Regulation  This requirement aims to reduce the risk of operational shutdown due to system compromise. It implements the use of authentication and encrypting any patients’ data stored on devices for stronger data protection. | Since ABC Healthcare team members tends to bring their own devices, this regulation helps to safeguard patient’s data against weak passwords and soft encryptions. ABC Healthcare suffers from a hardened security information system. | All medical device manufacturers must comply with this FDA mandate. Noncompliance ranges from warning letters to fines up to $500,000 for corporations to criminal prosecution. |

|  |  |  |
| --- | --- | --- |
| Security Rule/ HIPPA  Baseline Configuration  This regulates the configuration for system and system components including connectivity, operational ad communications aspects of systems. It creates documents on procedures, controls, network topology and logical placement. | This regulation is noncompliance within ABC Healthcare because all programs are currently using default usernames and passwords. This puts the company at risk because attackers with default equipment knowledge can easily compromise ABC’s network. | ABC Healthcare could face HIPPA fines of up to $50,000 with an annual penalty cap of $1,500,000. |

**Acceptable Use of Technology Policies**

ABC Healthcare currently does not have an acceptable use policy. While researching different AUPs, I read the AUPs of both Pennsylvania College and Einstein Medical. Pennsylvania College and Einstein Medical does a good job at identify what resources are covered and clearly outlines the acceptable and nonacceptable uses of their resources. Both AUPs puts in place the use of strong passwords and keeping credentials confident. Consequences for falling to comply with these policies are present and clearly stated. Within these policies prohibited conducts follows NIST and ISO/IEC recommendations. Looking at both policies, I would implement the following into ABC Healthcare AUP: no hacking, no child pornography, failure to abide by third party website policies, false pretenses, harmful content, defamation, failure to safeguard accounts, use of personal email on company network, gaining access by using someone else credentials and a provision put in place stating that if the company feels that staff is using resources inappropriately, network traffic to and from said device will be monitored and if justified the device will be disconnected from the network and actions will be taken. I would also add to ABC Healthcare, that use of x rate websites is prohibited, along with an email policy, bring your own device policy and a clean desk/screen policy. With an acceptable use policy in place, ABC Healthcare should be able to put better controls in place to safeguard its assets.

**Codes of Ethics**

ABC Healthcare would benefit from implementing codes of ethics. When researching World Wide Technology, Inc. (WWT) and AT&T Inc the similarities are as follows, honesty and ethical practice in fair dealing and handling of conflicts of interest. Both companies agree with complying with applicable laws, governmental rules, regulations, and accounting standards. WWT and AT&T both implements a gift policy and anti-corruption policy. This is referred to as a conflict-of-interest clause. The interesting part is that both companies also have a board for ethics where members can meet and discuss ethic violations and how to handle them. The difference between the two are, WWT word their document in a straightforward manner, as for AT&T word their document in a more legal wordage. AT&T goes into a full breakdown of what being within compliance entails and how to report any discrepancies and accountabilities. WWT does a good job of acquiring a signature of its team member to ensure that they understand and agree with terms of ethic. Within both codes of ethics, I would implement into ABC Healthcare the following:

1. Conflict of Interest which entails not getting involved in any activities that compromises the company, its employees or its stakeholders.
2. Do not misrepresent the company or yourself.
3. Adhering to applicable laws, governmental rules, regulations and industries standards.
4. Report proper and correct reporting to SEC.
5. Report any unethical or illegal conduct to management.
6. Integrity, honesty and full disclosure.

By implementing these codes of ethics, ABC Healthcare will establish a strong basis for their own ethical practices and guidelines. Without some type of ethical direction ABC Healthcare will eventually find themselves in legal lawsuits and their reputation completely left in shambles.

References

Chipeta, C., 2022. *Top 8 Healthcare Cybersecurity Regulations and Frameworks | UpGuard*. [online] Upguard.com. Available at: <https://www.upguard.com/blog/cybersecurity-regulations-and-frameworks-healthcare> [Accessed 1 August 2022].

Einsteinmedical.com. 2014. *Acceptable Use Policy*. [online] Available at: <https://www.einsteinmedical.com/acceptable-use> [Accessed 2 August 2022].

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. 2020. *Security and Privacy Controls for Information Systems and Organizations*.

Pennsylvania College of Technology. 2022. *IT Resources Acceptable Use Policy*. [online] Available at: <https://www.pct.edu/student-life/information-technology-services/it-resources-acceptable-use-policy> [Accessed 2 August 2022].

2022. [online] Available at: <https://www.nstec.com/technology/information-technology/what-is-an-information-technology-structure/> [Accessed 18 July 2022].

Mack, J., 2004. *Beyond HIPAA: Ethics in the e-Health Arena*. [online] Account.ache.org. Available at: <https://account.ache.org/iweb/upload/Nelson%20Excerpt-2c5f3570.pdf> [Accessed 18 July 2022].

Williams, B., 2010. *Information security policy development for compliance*. 2nd ed. Aurbach Publication.

Woock, K., 2022. *What Is PCI Compliance? 12 Requirements & Guide - NerdWallet*. [online] NerdWallet. Available at: <https://www.nerdwallet.com/article/small-business/pci-compliance> [Accessed 18 July 2022].

www.hhs.gov. 2002. *HIPPA*. [online] Available at: <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/incidentalu&d.pdf> [Accessed 18 July 2022].