Risk analysis: utah department of health

Health & Medicine

In March 2016 Utah Department ofHealthwas notified of a breach in their system. The current firewall had not been correctly set up to protect personal information. Intrusion Detection System was supposed to be turned on, but for some reason was off, and the remote access that medical staff use was not set up for restricted access segment in order to protect patient information.

THe Department ofTechnologyservices failed to complete their implementation of the security setup, which ultimately was the reason for the breach that has occured.

Network segmentation for security splits the network into zones that contain data with similar compliance requirements. By segmenting the network this way, you reduce the scope of compliance and simplify security policies. An accurate security policy involves segmenting the network into multiple zones with differing security requirements and enforcing a strict policy of what is allowed to move from one zone to another zone.

Anything designated in the PCI zone should be isolated from the rest of the network as much as possible. Utah Department of Health was set up with the firewall. A firewall generally establishes a barrier between a trusted internal network and an untrusted external network, like the internet.

Data Life Cycle:

Data life cycle is the sequence of stages that a particular unit of data goes through from its initial stage to its eventual archival and/or deletion at the end of its useful life. Proper oversight of data throughout its life cycle is

important to optimize its usefulness and to decrease the potential for errors as much as possible. Data life cycle management is a comprehensive approach to managing an organization's data, involving procedures and practices as well as applications.

Access:

The staff at the Utah Department of Health were not properly trained in utilizing the firewall, which is where the small hole occurred for this type of breach. The internal staff had not set up secure passwords which in turn allowed malware to enter into the system. Downloading items, searching the internet, and clicking on sites that may or may not be secure is where this began.

Thisfailureto follow through from DOT, as well as the internal staff that continued to pursue surfing the internet with known knowledge of malware and viruses that occur within IT just scratches the surface for the breach of information. The employees, such as nurses, doctors, and administrators are the main stakeholders of this issue and are the ones that will be associated with the risk analysis and mitigation.

It is important that they have access to the information that was associated with the breach because they need to be able to use this as identifiers when dealing with each patient to avoid providing the wrong treatment, and or medications. Each patient is to be identified using 3 identifiers, such as date of birth, first and last name, and either address or social security number.

The roles and responsibilities that the stakeholders will participate in will start with the importance of surfing the internet on a company based server that has personal information attached to it.

Next would be to train each individual in setting up their own unique personal ID and password associated with access controls to prevent any further breach. Further training on how these systems should be used and what is an inappropriate site to enter such associal media, which should be done on their own devices, and downloading of documents that pertain to the facility or medical references.

Rating:

This breach of personal and health information will have a huge impact on not just the patient but on the staff as well. While UDOH has the proper security as far as being in compliance goes, they did not have the barriers up and running. Failing to correctly configure and monitor the firewall, and having internal and external securities out of date fall through keeping the health information system in compliance with regulations.

With that being said, if all walls were up and running and everything was kept up to date, it would have been harder for the breach to have occurred, warning flags would have popped up that they were entering into an unsecure site for example. With this issue at hand lies a trust issue.

> *" By properly segregating the network, you are essentially minimizing the level of access to sensitive information for those*

applications, servers, and people who don’t need it, while enabling access for those that do (Reichenberg, March, 2014."

This breach will have the patients hesitant to provide the needed identification and information that is used to help the medical and administrative staff keep the patients safe. Patients will be reluctant to provide their identity for fear of that identity being stolen due to another possible breach.

" Many companies know their enterprise networks are not as secure as they would like. They have a perimeter firewall—and possibly other tools like Security Information and Event Management (SIEM), Intrusion Prevention System (IPS), Advanced Threat Detection (ATD) protecting the network perimeter, but behind that is the internal " trusted" network, with no standardized segmentation methodology. (E. Nelson, 2017)"

Conclusion:

In conclusion, patient privacy (AKA HIPAA) is to be protected at all costs. " The Health Insurance Portability andAccountabilityAct of 1996 (HIPAA) Rules contain privacy, security, and breach notification requirements that apply to individually identifiable health information created, received, maintained, or transmitted by health care providers who engage in certain electronic transactions, health transactions, health plans, health care clearinghouses, and their business associates (HHS, 2018)."

HIPAA violations (or breaches) unfortunately are an occurrence all over the nation. It is up to the medical staff to protect this information and trust what is instilled into the profession. Following policies and procedures are necessary in order to abide by regulations of privacy.