Security Assessment of Cloud-based Healthcare Applications

October 13, 2019

Jonathan C. Miller

IS 550: Information Systems Thesis/Project

Abstract:
Security assessment and analysis of healthcare software applications can offer an in-depth understanding of role-based access options, logging capabilities, and vulnerabilities at the network, application, database, and operating system level for each application. An assessment can become more complicated as cloud capabilities become leveraged. Healthcare information is governed by a higher standard set forth by the U.S. Department of Health & Human Services through the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA policies are to be strictly enforced from the creation, transmission, and storage of data as well as during the release and capture to the cloud provider. Vendor and software evaluation can be viewed strictly based on cost, rather than the dependability and security that a higher price can potentially offer. Through reviewing security standards based on NIST and SANS, with a crosswalk to HIPAA guidelines, an open standard assessment guide for cloud-based software could be created. An open assessment guide could offer healthcare providers and agencies a guided process to assess potential vulnerabilities that could have long-term liabilities.

Keywords:
Security, cloud computing, cloud security, privacy, HIPAA, NIST, SANS, cloud taxonym, cloud computing security, social engineering.

Security Assessment of Cloud-based Healthcare Applications 1

Introduction..... 5

Problem Statement 5

Goal 5

Background 6

Valuable Medical Record Data 9

Healthcare Social Engineering Tactics 14

Social Engineering Data 16

HIPAA Guidelines 19

OCR – Burden of Proof 20

NIST HIPAA Crosswalk 21

Security incident to breach 23

Ransomware Attack 25

Risk Management 27

Risk Framework 31

Risk Assessment Software 36

Higher Education Cloud Vendor Assessment Tool 37

Cloud threat assessment 38

Deployment: Control and Management 38

Proposed Solution 42

Conclusion 42

Future Research 43

Bibliography 44

Introduction

Applications and vendors come in all shapes and sizes. As applications and the devices, they interact with continue to evolve and expand, it is vital for companies implementing new software to complete a thorough security assessment. This assessment should become more stringent when dealing with medical record data, live patient data, and personal identifying information that is transmitted to a cloud system. A complete evaluation, including access control, logging capabilities, and encryption methods, must be considered. This evaluation must include an appraisal of the network, database, application, and operating system to be able to have a full understanding of the potential gaps and vulnerabilities. A flawed examination of a healthcare application put into production can have dire consequences to the business.

Problem Statement

An electronic technology assessment can be a daunting task, where the security of data and access can be easily overlooked. While technology continues to evolve, so do the threats, and healthcare software is not void of those threats but rather more susceptible. The existence of multiple security frameworks, a lack of highly trained security professionals and no standard healthcare-specific assessment model make it increasingly difficult to adequately assess the security and privacy of a cloud-based software solution.

Goal

The purpose of this document is to explore areas where increased awareness of HIPAA restrictions placed on vendors, physician providers, and healthcare agencies in regards to cloud-based software. This document will illustrate the potential threat vectors that exist, the potential path for data

compromise leading to a security breach, and the long-term impact. Lastly, this document will demonstrate why security in healthcare applications must be evaluated, monitored, and audited regularly.

Background

Cloud technology has become a growing trend, as well as a popular buzz word but has been a part of information technology well before the dot com bubble. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell & Grance, 2011). Cloud computing dates back to the 1950s, and over the years, it has evolved through many phases that were first pioneered by IBM, including grid, utility, and on-demand computing (Cloud computing: A complete guide, n.d.). Whether it is used to run applications that share photos to millions of mobile users or to support business-critical operations, a cloud services platform provides rapid access to flexible and low cost IT resources (What is Cloud Computing?, 2019). Cloud technology "is composed of five essential characteristics, three service models, and four deployment models" (Mell & Grance, 2011). Characteristics of cloud technology include on-demand self-service, broad network access, resource pooling, and rapid elasticity. Cloud platforms are commonly designed in the following three service models. Platform as a service (PaaS) which provides a cloud-based environment with everything required to support the complete lifecycle of building and delivering web-based applications without the cost and complexity of buying and managing the underlying hardware, software,

provisioning, and hosting (Cloud computing: A complete guide, n.d.). Infrastructure as a Service (IaaS) offers the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications (Mell & Grance, 2011). Software as a service (SaaS) offers the ability to Cloud-based applications on distant computers "in the cloud" that is owned and operated by others, and that connect to users' computers via the internet through a web browser (Cloud computing: A complete guide, n.d.). Other Cloud-based models are starting to become popular such as, Security as a Service where external security services are integrated into an existing infrastructure on a subscription-based service.

Each service model can be deployed in three different ways. Public clouds are owned and operated by companies that offer rapid access over a public network to affordable computing resources (Cloud computing: A complete guide, n.d.). A private cloud is where the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (Mell & Grance, 2011). A hybrid cloud uses a private cloud foundation combined with the strategic integration and use of public cloud services (Cloud computing: A complete guide, n.d.). Security for cloud deployment or integration falls both on the vendor and the customer to work to protect data and privacy. A cloud managed services provider should incorporate built-in security layers at every level, from the data center to the operating system with regular vulnerability scans performed by highly skilled specialists (Cloud computing: A complete guide, n.d.).

Built upon the flexibility and low-cost, cloud technology has been widely adopted. The HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules) establish essential protections for individually identifiable health information (protected health information or PHI when created, received, maintained, or transmitted by a HIPAA covered entity or business associate), including limitations on uses and disclosures of such information, safeguards against inappropriate uses and disclosures, and individuals' rights with respect to their health information (Guidance on HIPAA & Cloud Computing, 2017). HIPAA standards provide protection of health data, and any vendor working with a healthcare organization or business entity handling healthcare data must abide by the HIPAA privacy rules (HIPAA Compliant Cloud Storage Solutions, 2019). A covered entity is a health plan, a health care clearinghouse, or a health care provider who conducts billing and payment related transactions electronically, whereas a business associate is an entity or person, other than a member of the workforce of a covered entity, that performs functions or activities on behalf of, or provides certain services to, a covered entity that involves creating, receiving, maintaining, or transmitting PHI (Guidance on HIPAA & Cloud Computing, 2017). Being HIPAA compliant means implementing all of the rules and regulations that HIPAA proposes, and any vendor offering services that are subject to HIPAA must provide documentation as proof of their conformity (HIPAA Compliant Cloud Storage Solutions, 2019). When a covered entity engages the services of a Cloud service provider to create, receive, maintain, or transmit ePHI, on its behalf, the Cloud service provider is a business associate under HIPAA (Guidance on HIPAA & Cloud Computing, 2017).

Valuable Medical Record Data

The 2016 Healthcare Industry Cybersecurity Report illustrates the critical vulnerabilities that exist in healthcare agencies. The report listed that "out of 18 industry sectors reviewed, healthcare placed 15 as one whose employees are most susceptible to fall for socially engineered schemes, which suggests that there is a bigger security awareness problem among the personnel of healthcare organizations" (Yampolskiy, 2016). The report goes on to detail how the healthcare industry falls below the industry norm in six out of 10 critical security categories that are used by Security Scorecard. That in 2016, "63 percent of the 27 largest hospitals in the U.S. received a letter grade of C or lower for prompt patching of IT systems" (Yampolskiy, 2016). Further reading also identified IoT devices, primarily being patient medical devices demonstrate severe vulnerabilities to a malware infection. With many kinds of endpoints, "including the IoT devices, emanating signatures of malware because they were infected, attackers are going to compromise those devices more and more, and the healthcare sector is very much affected" (Yampolskiy, 2016). The combination of unpatched, unmanaged insecure network devices, along with a governmental push to migrate to an electronic health record system (EHRs) created massive opportunities for attackers and identity thieves.

Under "the HITECH Act it was mandated that Centers for Medicare and Medicaid Services (CMS) recipients to implement and use EHRs by 2015 in order to receive full reimbursements" (Kruse, Smith, Vanderlinden, & Nealand, 2017). Even though under the law, one of the meaningful use statements focuses on privacy and security, most migrations to an electronic

health record were focused on the migration, and little attention was given to overall security. Incentives were offered to providers who adopted EHRs prior to 2015 and penalties are imposed for those who do not beginning 2017 (Kruse, Smith, Vanderlinden, & Nealand, 2017). The incentives and penalties aspect of the Affordable Care Act motivated most healthcare agencies to migrate sooner, which left many gaps in security with their implementations. These gaps have been exploited by attackers to compromise sensitive PHI and PII data. In 2015, Accenture estimated that one in 13 patients, roughly 25 million people, will have personal information, such as social security or financial records, stolen from technology systems over the next five years (Francis, 2015). The forecast of data compromised has proved correct, as each month and year passes more providers are compromised. During 2014, approximately, "1.6 million people had their medical information stolen from healthcare providers last year, according to the U.S. Department of Health and Human Services Office for Civil Rights" (Francis, 2015). Identity or patient data theft differs as compared to a credit card provider. Unlike credit card identity theft, where the card provider generally has a legal responsibility for account holders' losses above $50, victims of medical identity theft often have no automatic right to recover their losses (Francis, 2015). Though through the Office of Civil Rights, medical providers can be fined, and victims can be compensated, but being proactive could prove more beneficial. Addressing cybersecurity proactively can improve a provider’s ability to thwart attacks by an average of 53 percent (Francis, 2015). Medical identity theft is often not immediately identified by a patient or their

provider, giving criminals years to milk such credentials which makes medical data more valuable than credit cards, which tend to be quickly canceled by banks once fraud is detected (Humer & Finkle, 2014). These stolen credentials can be used for months and sometimes years to fraudulently bill insurance providers, Medicare and/or Medicaid. One example of this type of fraud is a case in 2014, where a patient learned that his records at a major hospital chain were compromised after he started receiving bills related to a heart procedure he had not undergone and then being billed for the purchase of a mobility scooter and several pieces of medical equipment, racking up tens of thousands of dollars in total fraud (Humer & Finkle, 2014). Given the potential level of fraud that can be gained from stolen medical data, threats still exist. There are many threats to the privacy of a patient's information, and one of the largest threats is social engineering (Cazier & Medlin, 2010). While social engineering may be covered in an online video or quiz to remind the healthcare staff, most still adhere to old and sometimes bad habits. Unfortunately, the most significant threat to a health care agency's security may not be outsiders, but rather their own employees (Cazier & Medlin, 2010). With a badge and a little knowledge, can be very dangerous to the organization. Inside employees actually can pose the largest threat to the security and privacy of information as they can exploit the trust of their co-workers, and they generally are the individuals who have or have had authorized access to the organization's network and who are familiar with its internal policies, procedures, and technologies (Cazier & Medlin, 2010). Even though HIPAA has enacted the following requirements; these are not always followed or enforced at the facility level:

Security Management Process [161.308(a)(1)]: Healthcare organizations must show that they have a consistent set of internal processes, with implementation that is widespread and institutionalized. Processes range from establishing criteria for who has access to what, and who can request certain resources; to ensuring that access rights are revoked immediately upon employee termination.

Security Awareness and Training [161.308(a)(5)]: HIPAA requires that staff members be trained and educated concerning the proper handling of PHI. This basic-level security training should include measures such as password management.

Access Control [161.312(a)]: HIPAA security regulations require a definition of who has access to PHI within the organization, as well as the rules determining an individual's right of access, and the reasons for denying access to some individuals.

Organizations and individuals should, therefore, be made well aware of those factors that may compromise password or system management and the resulting risks attached to such a compromise (Cazier & Medlin, 2010). Any healthcare or provider system should strive to maintain HIPAA compliance. But employees and agencies should do everything possible to protect a patient's sensitive data. It is also imperative that "employees be knowledgeable about the techniques used by individuals to gain information" (Cazier & Medlin, 2010).

Social engineering is typically overlooked as company plans and develops its facility and information security policy. One of the reasons social engineers are so successful is because of their personalities; they are trying to hack humans into telling them the information they want to know,

they are expert flirters, charismatic suck-ups, and confident intimidators (Barney, 9 Ways To Social Engineer A Hospital, 2015). Most companies have a focus on customer relation, as well as the typical human nature to want to help, which allows most tactics to be successful. It takes only a few moments with an employee over the phone, via email, or in-person to determine that they are not adequately trained to protect the business, and sensitive data against a social engineering attack and then the social engineer flips the proverbial switch, and the attack begins using charm, whit, questioning, leading the attackee, and more (Barney, Healthcare: Recognize Social Engineering Techniques, 2015). Social engineers know how to act the part, by not appearing sneaky or timid, but these engineers use a person's weaknesses to their advantage. Social engineering is hard to identify, especially in larger organizations where workforce members don't always know their coworkers, especially everyone in IT, or janitorial, or maybe outsourced third-party vendors (Barney, Healthcare: Recognize Social Engineering Techniques, 2015). Healthcare employees are typically more trusting, but most humans have an "innocent until proven guilty" mindset. Sometimes this naive human quality is what a social engineer relies on to slip past a few employees who could have otherwise easily stopped him (Barney, Healthcare: Recognize Social Engineering Techniques, 2015). Serving patients, aiding in their recovery as well as becoming close to the patient's family, it's a natural transition to want to help any and all that are crossed through a day. Good people look out for each other, especially in the healthcare environment, who wouldn't want to help someone who has a quick question, or open the door for someone who forgot their ID badge (Barney,

Healthcare: Recognize Social Engineering Techniques, 2015)? Another concern or weakness is the inevitable need not to look stupid. Someone working in a large healthcare environment could only know a small percentage of staff, including vendors, contractors, students, volunteers. The unknown mixed with the lack of challenge can easily allow an attacker to access a secure area, hook or plug unknown devices into computers or network devices. Fear is a universal emotion that attackers' prey upon. Employees don't want to cause trouble or challenge the wrong person. The fear of stopping a or questioning a person and their access could turn out to be an executive or a provider, and that fear may allow an attacker to gain access. These 'human flaws' are some of the most challenging aspects when training employees on detecting social engineering, because the end goal is to now train people out of the way they naturally think (Barney, Healthcare: Recognize Social Engineering Techniques, 2015). There are countless ways hospitals and even smaller covered entities can be socially engineered, but they all revolve around five big issues that most entities have (Barney, 9 Ways To Social Engineer A Hospital, 2015):

- Unaware staff
- No policies regarding request verification
- Lack of reporting suspicious people or situations
- Minimal physical security
- Lack of communication between departments

Healthcare Social Engineering Tactics

Social engineering methods can vary from in-person, on-site attacks, phone or email attacks, while healthcare can be run like any other business, it is also very exploitable. Methods or tactics to consider as a threat vector:

- The Dumpster Dive, this is where an attacker goes through any publicly placed garbage to gather any knowledge of possible advantage. If the hospital receives invoices and

doesn't shred them, a social engineer could go through that trash and find sensitive information about new hospital computers (Barney, 9 Ways To Social Engineer A Hospital, 2015).

- The Password Change is when an attacker poses as an employee or a co-worker and contacts the helpdesk to reset the password of an employee in hopes of gaining system access. A password change can "be a huge problem, but it can and does happen in organizations all the time especially if your help desk doesn't have a solid policy for non-face-to-face password resets, and if they get swamped" (Barney, 9 Ways To Social Engineer A Hospital, 2015). The change could allow the attached access to PHI or PII data under a different user's accounts, making it even harder to trace.
- The Name-Drop tactic occurs when an attacker poses under the guise of being sent with orders from a manager or executive to have access created or modified. By using a supervisor's name, and a bit of urgency an attacker now could have potential access to PHI data (Barney, 9 Ways To Social Engineer A Hospital, 2015).
- The Walk-In requires the attacker to be on-site and show their face. Under this scenario, the attacker, "enters into the hospital, dressed up in a suit, looking very official, picks up a patient record and starts looking through it and within five minutes, he takes several photos of the data, and leaves" (Barney, 9 Ways To Social Engineer A Hospital, 2015). Even though the attacker may have only gotten access to one record, that may be the cornerstone of an attack that leads to the rest of the MRN records in the system.
- The Unlocked Computer is an all too common threat vector in any workplace but does require the attacker to come on-site and show their face. An attacker confidently goes into an office that is unlocked and sits down at an unlocked computer and begins copying over data or installs a piece of malware for use later (Barney, 9 Ways To Social Engineer A Hospital, 2015).
- The Relaxing Conversation, this is another on-site attacker where a social engineer uses charm, whit, and conversation to gather information such as a username, supervisor, or even system access.
- The Fake IT Guy method is where the attacker calls a potential victim, identified as someone within the IT department and ask for their credentials. The person in question then gives the information out, and the attacker now has access to the network as well as making them untraceable (Barney, 9 Ways To Social Engineer A Hospital, 2015).
- The Pointed Question attack can be used over the phone or in person. In

this tactic the "social engineer asks a staff member pointed questions, masking them as casual inquiries while the staff member unwittingly gives her valuable information, such as his supervisor's name, his username, the supervisor of the department" (Barney, 9 Ways To Social Engineer A Hospital, 2015). This attack may not grant system access but maybe a foothold for another offense such as The Name Drop.

- The Device Walk Out does require being on-site, and considering site security could be more dangerous but also offers high rewards. Through this attack, the social engineer poses as an employee, contractor, or provider and attempts to exit the building with a company device such as an iPad, laptop, computer tower or even external storage drive. The staff 'doesn't notice the device is missing until later and by then, the social engineer potentially has access to information, PHI, data, etc. (Barney, 9 Ways To Social Engineer A Hospital, 2015).

Healthcare systems can combat these attacks through various methods. The first may be to hire an outside consultant to conduct a security audit and offer specific areas to focus on for improvement. One area which will always be ongoing is to train staff members to verify requests. Staff members should check with supervisors when someone claims they have arrived to work on hospital devices, network systems, or software (Barney, 9 Ways To Social Engineer A Hospital, 2015). Although training can be costly to time and resources, it could be the difference between a security breach or a security incident that ended with a failed attack.

Social Engineering Data

Attacker access can be gained, through a phishing attack, malicious code injected into a website or through a social engineering attack. Rather than exfiltrating data and cleaning up after the attack, hackers have adjusted their attacks to fetch a higher price tag on the dark web. Threat researchers have seen an uptick on a unique variation of health care data for sale, rather than selling databases containing patient

data or forged insurance cards, cybercriminals are auctioning admin access to health care portals (Maor, 2019). As healthcare providers move more applications to the cloud, this will increase the likelihood of data being sold in this manner. Health care organizations are now facing a growing number of attacks and threats while also having to keep in line with different regulatory compliances such as HIPAA (Maor, 2019). With a current cloud application vendor providing services, a healthcare provider may want to review and even test the processes and security mechanisms the vendor has in place. An annual security audit performed by a healthcare entity based in northeast Tennessee analyzed the responses to cloud application vendors. The review consisted of contacted technical support of the vendor, in attempt to gain user account information, and administrative account information over the phone under the simple guise of being a replacement IT analyst for the organization. The Vendor Audit, performed by a healthcare entities IT Security team, selects ten random vendors each quarter to assess the likelihood of an outside attacker compromising their cloud-based applications. Date that is requested is a list of all healthcare entity-specific associated logins, data and time of the last login, and administrative accounts identified (vendor names have been deidentified for this research paper but demonstrate the potential threat) (Haney, Oliver, & Birchfield, 2019):

- Vendor A provided the account executive contact information to help resolve the request.
- Vendor B emailed all data without question or verification, as well as verbally provided the administrative accounts.
- Vendor C opened up a service ticket, and the data was never provided.

- Vendor D could not reach anyone at the vendor's service desk.
- Vendor E opened up a service ticket, and the data was never provided.
- Vendor F provided a screenshot from the service desk portal view of all accounts, and email address.
- Vendor G verbally provided the only log in on the account.
- Vendor H provided the account executive contact information to help resolve the request.
- Vendor I said the service desk was unable to pull that report but created an administrative account and granted access to pull the data requested.
- Vendor J escalated the request to another team, and a week later, the data was provided via email.

The concern lies in the fact that none of the vendors contacted verified the request with any known point of contact within the healthcare facility prior to completing the request (Haney, Oliver, & Birchfield, 2019). This access offers the attacker the potential for a master key to all data related to the targeted facility (Maor, 2019). The subtle effort by the attacker and the potential prize by a social engineering attack, which demonstrates that technology can only prevent human error to an extent. Security awareness training must be integrated with a company's long term. Many security companies offer training tools that can assist with phishing, social engineering, and social media attacks. One company, "KnowBe4 offers a Social Media Phishing Test is a complimentary IT security tool that helps you identify which users in your organization are vulnerable to these types of phishing attacks that could put your users and organization at risk" (What is social engineering?, n.d.). KnowBe4 focuses on training end users to be more aware of potential attacks. KnowBe4 educates users through a, "Awareness Training Program provides you with a comprehensive new-school approach that integrates baseline testing using mock attacks, engaging

interactive web-based training, and continuous assessment through simulated phishing, vishing and smishing attacks to build a more resilient and secure organization" (What is social engineering?, n.d.). This form of training can exceed what most organization's offer employees in the form of a yearly review or quiz.

HIPAA Guidelines

The Office for Civil Rights (OCR) that falls under the U.S. Department of Health and Human Services (HHS), role is to enforce federal civil rights laws, conscience and religious freedom laws, the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules, and the Patient Safety Act and Rule. Between the years of 2008 and 2015, OCR had imposed on average four HIPPA penalties a year. In 2016, there was a significant increase in HIPAA fines and settlements compared to the previous year which included one civil monetary penalty was issued by OCR and 12 settlements were agreed with HIPAA covered entities and their business associates (Summary of 2018 HIPAA Fines and Settlements, 2019). Through 2017-2018, OCR continued with a large number of HIPPA penalties, and with these, the fines grew based on the breach size and reason behind the breach. While 2018 was not a record-breaking year in terms of the number of financial penalties for HIPAA violations, it was a record-breaker in terms of the total penalty amounts paid where OCR received $28,683,400 in financial penalties in 2018 (Summary of 2018 HIPAA Fines and Settlements, 2019). During 2018 OCR levied high fines to various institutions for an array of reasons due to HIPPA violations. Top of OCR fines for 2018 include: (Summary of 2018 HIPAA Fines and Settlements, 2019):

- Fresenius Medical Care North America, $3,500,000 settlement for

"Risk analysis failures, impermissible disclosure of ePHI; Lack of policies covering electronic devices; Lack of encryption; Insufficient security policies; Insufficient physical safeguards."

- University of Texas MD Anderson Cancer Center, $4,348,000 Civil Monetary Penalty for "Impermissible disclosure of ePHI; No Encryption."
- Massachusetts General Hospital, $515,000 settlement for “Filming patients without consent."
- Anthem Inc, $16,000,000 settlement, for "Risk Analysis failures; Insufficient reviews of system activity; Failure related to response to a detected breach; Insufficient technical controls to prevent unauthorized ePHI access."
- Cottage Health, $3,000,000 settlement for "Risk analysis failure; Risk management failure; No BAA."
- Advanced Care Hospitalists, $500,000 settlement for "Impermissible PHI Disclosure; No BAA; Insufficient security measures; No HIPAA compliance efforts prior to April 1, 2014."

Each of these examples may be taken under advisement by healthcare systems to help promote better system security and firm adherence to HIPPA guidelines.

OCR – Burden of Proof

In 2013, an omnibus law that was passed to strengthen the Affordable Care Act but also had a tremendous impact on security regarding HIPPA. Under the law it "reaffirms that, in the case of an impermissible use or disclosure of PHI, it is the covered entity or the business associate, as applicable, that has the burden of demonstrating that all notifications were provided or, in the alternative, that an impermissible use or disclosure did not constitute a breach, and of maintaining documentation as necessary to meet this burden" (Breach Notification Standard Changed by HIPAA Omnibus Final Rule, 2013). Covered entities have the burden of demonstrating that they satisfied the specific notice obligations following a “breach” as defined by the law, or if notice is not made following an unauthorized use or disclosure, that the unauthorized use or

disclosure did not constitute a "breach" (Omnibus Rule Revises What Constitutes a "Breach" , 2013). The shift is the complete opposite of what a person would have to demonstrate in court, where the burden of proof lies on the accuser. It is critically essential that covered entities and business associates have appropriate policies and procedures in place to detect and respond to a potential breach (Breach Notification Standard Changed by HIPAA Omnibus Final Rule, 2013). If the information is not PHI, there is no breach, also including de-identified information and employment records held by a covered entity in its role as an employer is not PHI (Omnibus Rule Revises What Constitutes a "Breach" , 2013). The specifics of what is classified as PHI and what is not is essential depending on the system that was breached or compromised. Even though it may be an application in a healthcare system, it may not contain any PHI due to the nature of its processes.

NIST HIPAA Crosswalk

The National Institute of Standards and Technology (NIST) have developed the NIST Cybersecurity Framework to assist in the guidance of cybersecurity. Through the NIST Cybersecurity Framework, there has been a correlation to HIPPA compliance to assist healthcare systems, agencies, and providers in understanding cybersecurity better and assist to protect their patients data better. Under the NIST HIPPA crosswalk, is broke down into twenty-one categories and a total of ninety-seven sub-categories (HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework):

- Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
- Business Environment (ID.BE): The organization's mission, objectives,

stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

- Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
- Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
- Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
- Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
- Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security related duties and responsibilities consistent with related policies, procedures, and agreements.
- Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
- Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
- Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
- Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.
- Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
- Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
- Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
- Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

- Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.
- Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
- Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
- Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
- Communications (RC.CO): Restoration: activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

Under each sub-category, there is a correlation provided to HIPPA guidelines and the NIST Cybersecurity framework that allows for a deeper understanding.

Currently, there are many types of incidents that could lead to a security breach. What may be considered an incident for one organization might not be as critical for another. The following are a few examples of common incidents that can have a negative impact on businesses (Rouse, 2019):

- A distributed denial of service (DDoS) attack against critical cloud services.
- A malware or ransomware infection that has encrypted essential files of business across the corporate network.
- A successful phishing attempt that has led to the exposure of personally identifiable information (PII) of customers or protected health information (PHI).
- An unencrypted laptop is known to have sensitive customer/patient records that have gone missing.

Security incident to breach

Security incidents that could lead to a potential breach should be treated as critical and be remediated as soon as possible. Due to the nature of the urgency and the impact of the system, the mitigation must be done in an attempt to lessen the threat and the reach of the situation. Another important aspect of understanding incident response is defining the difference between threats and

vulnerabilities. A threat is considered an indication of a criminal hacker or dishonest employee that is intending to exploit a vulnerability for a malicious or financial gain, whereas vulnerability is a weakness in a computer system, business process or user that can be easily exploited (Rouse, 2019). Understanding the difference allows for better communication. Threats exploit vulnerabilities which, in turn, create business risk leading to potential consequences that include unauthorized access to sensitive information assets, identity theft, systems taken offline and legal and compliance violations (Rouse, 2019).

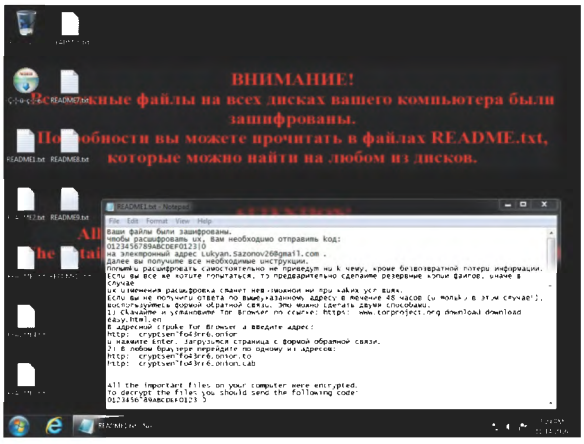
It has become an all to a common part of life, the various attempts of malware, viruses, and phishing, where most people become numb to the attempts. But "as cyberattacks against organizations have steadily worsened, consumer-targeted ransomware attacks have declined by 33 percent since last year" (Davis, 2019). It has become more lucrative for attackers to go after larger companies in an attempt to steal personal information, health information and also proprietary information. An FBI report also found that healthcare-related crimes schemes attempting to defraud private or government healthcare programs, typically health providers, companies, or individuals saw a total of $4.5 million in losses from 337 victims (Davis, 2019). The rise in losses can attribute to spikes in the cost of healthcare, but many times it can force providers to shut the doors. For businesses, detection of malware attacks continued to skyrocket across the board since last year, while hijacker malware was the only variant that has seen a steady decline in attacks and that the increase in ransomware is due to a massive Troldesh ransomware attack against US organizations (Davis, 2019).

Ransomware Attack

The concept behind ransomware is easily comparable to a kidnapping. It can start, typically with a phishing email or visiting an infected site that will give the infection access to the computer. From there, the software starts to encrypt all the data on the computer in a fashion that makes it next to impossible without the encryption key. Then the group running the campaign will have an image locked to the computers screen explaining how to make payment and receive the encryption key.

Ransom.Troldesh, aka Shade, is still an active form of malware and has experienced a sharp increase in detections from in the last two quarters between 2018 and 2019. An increase or spike in detection indicates that there is currently an active campaign and that it is becoming successful. Troldesh, which has been around since 2014, is typically spread by malspam (specifically malicious email attachments), the attachments are usually zip files presented to the receiver as something to be opened quickly (Arntz, 2019). Keen eyes will ignore the sender or the language in the email and only want to attempt to respond to urgency. The extracted zip is a JavaScript that downloads the malicious payload (aka the ransomware itself) that is often hosted on sites with a compromised Content Management System (CMS) (Arntz, 2019). A common CMS platform that can be compromised is WordPress, that when not

properly managed and updated can play host to ransomware, while some attackers just stand up a quick page to resemble other content such as a Microsoft Live login page or Google Drive login page. As the sender in Troldesh emails is commonly spoofed, it can be surmised that the threat actors behind this campaign are phishing, hoping to pull the wool over users' eyes in order to get them to open the attachment (Arntz, 2019). Based on the ransom notes that are left on a computer after the encryption process is complete, it is believed that the origin behind Troldesh is Russian.



Troldesh uses AES256 encryption, and there are currently some free decryption tools available on the Internet. Victims of Troldesh are provided with a unique code, an email address, and a URL to an Onion address. They are asked to contact the email address mentioning their code or go to the Onion site for further instructions (Arntz, 2019). Some victims have chosen to pay the attackers, while some will get the access code needed, many do not, but paying the ransom should not be an option due to the fact that it only aides in financing the next attack by the attacker. What sets Troldesh apart from other ransomware variants is the huge number of readme#.txt files with the ransom note dropped on the affected system, and the contact by email with the threat actor but it employs a classic attack vector that relies heavily on tricking uninformed victims (Arntz, 2019). This current attack in the last six months has

been quite successful, but devasting to end users and businesses.

Risk Management

To understand risk management, one must first understand risk. Risk is the possibility of threat, danger, injury or liability. What risk is per se can vary from field to field. For instance, in the food industry, a risk could be considered food contamination or cross contamination. Whereas in finance, a risk would look much differently which could stem from economics, politics or natural circumstances. Risk can come from "both internal and external sources, whereas external risks are those that are not in direct control of the management" (The Importance of Risk Management In An Organisation, 2013). Risk is the unknown, the probability of what could happen and the potential impact it could have on a business.

Risk Management allows an organization to identify the risk, the probability of the risk, and the impact. The ability to manage risk will help companies act more confidently on future business decisions, and their knowledge of the risks they are facing will give them various options on how to deal with potential problems (The Importance of Risk Management In An Organisation, 2013). Though risk management has been standard in the business sector, IT Risk Management is a growing field and an asset to any company. The heart of any cyber risk management program is an ongoing process of risk assessment, that involves an understanding of risk tolerance, knowledge of likely risks and threats, measured assessments of established controls, and executed plans to address identified vulnerabilities (Yildirim, 2016). Effective IT risk management covers all areas of IT and subdisciplines, and each

area has its area of potential risk. Examples of potential risk based on subdisciplines (Bevan, Ganguly, Rezek, & Kaminski, 2016):

- Information and Cybersecurity:
  - Leakage of confidential customer and internal data, blackmail, hacktivism
- Disaster Recovery:
  - Recurring or prolonged interruptions of IT services supporting critical processes
- Third-party management:
  - Not delivering reliable and secure services
- Project and change management:
  - Projects not following the schedule, budget or quality
- Infrastructure Development and testing:
  - Systems not being designed to provide long-term affordable, reliable and maintainable service to the enterprise
- Data governance
  - Legal, regulatory issues, missing or inaccurate data
- IT compliance
  - Noncompliance of IT systems and processes with regulations

Within each area of IT, risk can be assessed and processes designed to control or mitigate those risk.

Processes within risk management can vary slightly from model to model and from framework to framework. Risk management is fundamentally about making decisions – decisions about which risk issues are most critical (prioritization), which risk issues are not worth worrying about (risk acceptance), and how much to spend on the risk issues that need to be dealt with (budgeting) (Risk Taxonomy , 2009). But overall each model has at its core the following steps:

- Identify Risks
- Measure Risks
- Examine Solutions
- Implement Solution
- Monitor Results

These steps hold for risk assessment within financial, operational and hazard risks. Being able to identify what types of risk you have is vital to the risk management process, an organization can identify their

risks through experience and internal history, consulting with industry professionals, and external research (Rowe, 2018). Organizations could go further when identifying risk, by having group brainstorming sessions utilizing inside and outside people to aid in assessment. Environments change over time, identifying and assessing risks should be done in a regular and routine basis as an organization moves forward.

When all potential risks are identified, next the frequency and severity of the risk must be assessed — knowing the frequency and severity of your risks will show you where to spend your time and money and allow your team to prioritize their resources (Rowe, 2018). During the measuring phase, organizations can score or rank risks in "quantitative, semiquantitative or qualitative terms based on the probability of occurrence and the possible consequence" (A Risk Management Standard, 2002). Effective assessment and measuring will guide the effectiveness and potential for solutions. To be consistently effective in making these decisions, we need to be able to compare the issues themselves, as well as the options and solutions that are available (Risk Taxonomy , 2009). Depending upon the identified risks, solutions can vary in size and in cost and time to implement.

In dealing with risks, organizations have the four following options:

- Accepting
- Avoiding
- Controlling
- Transferring

Accepting the risk, "means deciding that some risks are inherent in doing business and that the benefits of an activity outweigh the potential risks" (Rowe, 2018). Accepting the risk can be a "a good strategy to use for very small risks – risks that won't have much of an impact on a project or organization if

they happen whereas, it could take a lot of time to put together an alternative risk management strategy or take action to deal with the risk, so it's often a better use of your resources to do nothing for small risks (5 Ways To Manage Risk, 2014). The avoiding option, allows an organization to not allow or participate in an activity that would allow that particular risk. The avoiding option could be as simple as changing plans to avoid the risk, "this is a good strategy for when a risk has a potentially large impact on an organization" (5 Ways To Manage Risk, 2014). Another option would be controlling or mitigating the risk, and this is the most common and used option. What mitigation means is that you limit the impact of a risk, so that if it does occur, the problem it creates is smaller and easier to fix (5 Ways To Manage Risk, 2014). Through controlling, there is the possibility of preventing the risk, but "reducing the likelihood that the risk will occur" (Rowe, 2018). Strategies to control or mitigate risks can vary greatly including the cost of the control. Lastly, transferring the risk. Although transference isn't used as often, it will entail utilizing another party such as another department or an outside contractor. For example, a third party could be contracted to write software code, the risk of potential errors in the code could be transferred over to them, and they would then be responsible for managing this risk (5 Ways To Manage Risk, 2014). Transferring risk typically would require a formal written agreement and planning but allows for the organization to remove the risk from their assessment.

As solutions are identified and implemented for each potential risk, the last phase is to monitor results. Even though monitoring is the last phase, it is the last phase in a cyclical process. As risks change or new solutions identified each time results to

those risks must be analyzed. Determine whether the initiatives are effective and whether changes or updates are required, the team may have to start over with a new process if the implemented strategy is not effective (Rowe, 2018). During the monitoring and reviewing process the following should be determined (A Risk Management Standard, 2002):

- did the measures adopted resulted in what was intended
- the procedures adopted, and information gathered for undertaken the assessment were appropriate
- improved knowledge would have helped to reach better decisions and identify what lessons could be learned for future assessments and management of risks

Throughout the monitoring phase, the implemented controls should assure that they match the organization's activities. Risk management for IT is a comprehensive solution that requires each step in each process to be well thought out and finely executed.

Risk Framework

It can be easy for a company to see a blatant risk and implement control or mitigation, but to execute a thorough assessment that includes assessing and mitigation is another thing. Risk is a natural part of the business landscape; if left unmanaged, the uncertainty can spread like weeds (Risk IT Framework for Management of IT Related Business Risks , n.d.). If managed effectively, losses can be avoided, and benefits obtained. To better understand why risk management is important is to understand the failures that come from it or the lack of risk management. What began in 2011, Wells Fargo has paid $185 million in penalties and led to 5,300 employees having been fired as a direct result of failure for risk management (Minksy, 2016). Wells Fargo management had set out unobtainable sales quotas and no internal auditing to show evidence of governance within the

organization. Effective risk management does not provide a guarantee against failure; companies with the best risk management systems and expertise can experience large losses (Stulz, 2009). But in the IT world, a data breach can draw large media attention but have become more all too common. The fast-food chain Wendy's dealt with a data breach in 2015. The problem was however that hackers continued to access data undetected at more than 1,000 franchisee-owned locations for over a year after banks and credit unions and others disputed the size of the problem that Wendy's was forced to reopen their investigations and uncover the full extent of the breach (Minksy, 2016). This isn't failed cybersecurity, it's a failure of vendor and third-party management, while Wendy's maintained its cybersecurity processes it failed to ensure that all locations maintained the same standards (Minksy, 2016). Even though risk management directly may not have prevented a breach, at the bare minimum it may have prevented the court cost and litigation claims. Too often, companies react by purchasing a new system solution which is effectively a band-aid, instead of ramping up risk assessments to identify potential future issues and identify the root causes of the problem (Minksy, 2016). During a risk management assessment, the team could have assessed the following:

- Does the organization rely on third parties?
- What standards do the third parties follow?
- Can the third parties demonstrate proof of standards?
- Would that proof hold up in a court case?
- What data is flowing to our third-party vendors?
- Can we track and document that data?
- What encryption and protocols do they follow?
- Is our vendor transmitting our data to another party?
- Outside of our organization, who has access to our data?

- Is it logged who accessed our data and when?

Risk management failures can result from using a risk metric that answers the wrong question, such as: transmitting sensitive data outside of the network, but only documenting where it goes and not the time or the amount of data (Stulz, 2009). It's just as important in choosing the right risk metrics as it is asking the correct questions. Risk management failures will fall into one or more categories (Ten Common Risk Management Failures and How to Avoid Them, 2008):

- Poor governance and “tone at the top.”
- Reckless risk-taking
- Inability to implement enterprise risk management
- Nonexistent, ineffective or inefficient risk assessment
- Falling prey to a “herd mentality.”
- Misunderstanding the “If you can’t measure it, you can’t manage it!” mindset
- Accepting a lack of transparency in high-risk areas
- Not integrating risk management with strategy-setting and performance management
- Ignoring the dysfunctionalities and “blind spots” of the organization’s culture
- Not involving the board promptly

Each area can be avoided when risk management is properly organized and implemented based on the risk framework chosen and the governance methods selected.

Multiple frameworks exist to guide any organization in risk management. Business risks, such as market risks, credit risk, and operational risks have long been incorporated into the corporate decision-making processes, whereas IT risk has been relegated to technical specialists outside the boardroom, despite falling under the same ‘umbrella’ risk category as other business risks (Risk IT Framework for Management of IT Related Business Risks , n.d.). The FAIR institute has developed the FAIR model.

Factor Analysis of Information Risk (FAIR) is the only international standard quantitative model for information security and operational risk (Freund & Jones, 2015). The FAIR model is a scalable risk framework developed to simplify information risk management, with the purpose of developing better assessments which leads to greater mitigations while reducing the potential for unknown risks. FAIR follows the following definitions (Freund & Jones, 2015):

- Threat
    - Anything acting in a manner that can harm
- Vulnerability
    - A value of the potential for risk
- Risk
    - The probable frequency and probable magnitude of future loss

The FAIR model was intended to be able to communicate technical, informational risk to stakeholders effectively.

Through 2002 the Federal Information Security Modernization Act (FISMA), and the National Institute of Standards and Technology (NIST) developed the Risk Management Framework (RMF) to make informed judgments and investments in the mitigation of risks. NIST's RMF model is a holistic and comprehensive risk management process that integrates the framework into the system development lifecycle and provides processes (tasks) for each of the six steps in the RMF at the system level (Risk Management Framework, 2019). The NIST RMF can differ from the FAIR model, based on the initial definition : "Risk is a function of the likelihood of a given threat source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization" (Stoneburner, Goguen, & Feringa, 2003). The methodology focuses on the systems that by identifying those risk, it lessens the risk to business processes and further on to lessen the risk to the

organization. By identifying security issues under the Federal Information Processing Standard (FIPS) 199 standard, an impact level of Low, Moderate and High can be assigned (Risk Management Framework, 2019). A key aspect of the RMF is that controls are planned during the development phase of an Software Development Life Cycle (SDLC). An implementation may include:

- Writing and following policies, plans, and operational procedures
- Configuring settings in operating systems and applications
- Installing tools/software to automate control implementation
- Training

The NIST RMF model is focused on qualitative whereas the FAIR model produces quantitative data; each model can serve a purpose in securing and identifying risks in information systems. The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities whereas a quantitative impact analysis is that it provides a measurement of the impacts' magnitude, which can be used in the cost-benefit analysis of recommended controls. (Stoneburner, Goguen, & Feringa, 2003). An alternative view held by some is that "exposure" should be the focus of our attention rather than "risk" and that the argument put forward here is that they consider "risk" to be the inherent worst case condition, and "exposure" represents the residual risk after controls were applied (Risk Taxonomy , 2009). The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of any recommended controls difficult, as compared to depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear,

requiring the result to be interpreted in a qualitative manner (Stoneburner, Goguen, & Feringa, 2003). Through the FAIR model the same information that is gathered and analyzed in the NIST RMF model, can be communicated to anyone outside of the IT area.

Risk Assessment Software

Risk software can be a valuable tool in collecting risk data, analyzing and producing reports to help guide the next steps. Nehemiah Security has developed RQ: Risk Quantified as a platform to automatically measure and deliver business analytics about your cyber risks. RQ allows the use of existing data on the business assets and IT systems to map an inside-out, unified view of the risk environment, which can model probable attack scenarios against key areas of exposures to predict business outcomes and stay ahead of unacceptable losses (RQ: Risk Quantifier, n.d.). The use of such software can help produce more valuable and in-depth information, that could take longer to calculate and assess manually. RQ can quantify and monitor potential financial impacts of cyber risks over time, by using metrics like business disruption, reputational damage, and legal fines, leaders can proactively escalate security initiatives (RQ: Risk Quantifier, n.d.). A product of this nature may not be suitable for smaller companies but possibly used by a contractor to do a risk analysis.

The FAIR Institute has developed a web application known as FAIR-U. RiskLens which host the free FAIR-U web application has created an enterprise-grade version for cyber risk assessment and management platform based on the FAIR model. RiskLens allows risk analysts to assess, manage and report on cyber risk across the enterprise in financial terms, in a consistent and scalable way (RiskLens, n.d.). The platform is

designed to produce information that can be utilized by board executives, security officers, and risk analyst. RiskLens gives the ability to drive security investments by demonstrating their impact against risk and risk changes over time as well as meet growing regulatory pressures (RiskLens, n.d.). RiskLens is a SaaS platform utilized by many in the financial and healthcare industry to asses risk. Each tool could be a valuable asset depending on the organization size, budget and number of information systems utilized.

Higher Education Cloud Vendor Assessment Tool

The Higher Education Cloud Vendor Assessment Tool (HECVAT) was developed to help post-secondary education institutions standardize security assessments. The HECVAT is a mere 284 questions and includes qualifying items for HIPAA and PCI based in the following areas (Higher Education Cloud Vendor Assessment Tool, 2019):

- Application/Service Security
- Authentication, Authorization, and Accounting
- Business Continuity Plan
- Change Management
- Data
- Database
- Datacenter
- Disaster Recovery Plan
- Firewalls, IDS, IPS, and Networking
- Mobile Applications
- Physical Security
- Policies, Procedures, and Processes
- Product Evaluation
- Quality Assurance
- Systems Management & Configuration
- Vulnerability Scanning

The HECVAT provides many benefits to both the college, and vendors can complete the HECVAT a single time and share it with any school that uses the HECVAT (HECVAT, n.d.). The HECVAT attempts to generalize higher education information security and data protection questions and issues regarding cloud services for consistency and

ease of use (Higher Education Cloud Vendor Assessment Tool, 2019). By having a standard platform for software evaluations, it leads to a more efficient and secure path to deployment.

Cloud threat assessment

Vulnerability scanning is critical when knowing potential unknown or unassessed vulnerabilities. When deploying a cloud solution for an enterprise that is handling sensitive data, a vulnerability scanning solution can aid in remediation. Potential solutions could include:

- Tenable.IO: Has continuous visibility and assessment into public cloud environments through our Amazon Web Services, Microsoft Azure, and Google Cloud Platform Connectors (tenable-io, n.d.).
- Qualys Cloud: Existing agreements and integrations with main public cloud platform providers, including Amazon, Microsoft, and Google, simplify protection (Qualys Cloud Platform, n.d.).
- Fortify On-Demand: Dynamic assessments, powered by Web Inspect, mimic real-world hacking techniques and attacks. It uses automated, interactive, and manual techniques to provide a comprehensive analysis of complex web applications and services (Fortify on Demand, n.d.).

Deployment: Control and Management

User access control and management can vary greatly based upon the business, the responsibilities of the users and the platform being utilized. A challenging concept to application security is effectively regulating and maintaining user access. However, “the business needs of all organizations evolve, and security changes may need to be made to accommodate them” (Parisian). But regardless of the system in place, the best way to protect data is to control how the data is stored and who has access to the data.

A typical cloud system can apply access control through a Role-Based process or Role

Based Access Control (RBAC), which allows for specific settings or enhancements per a specific user or group. This model allows for the definition of permissions, roles, users, and constraints. Permission allows for the access to one or more modules and processes within the system. Permission meanings can vary per system but, "most refer to the rights such as select, update, delete, or insert a record" (Thuraisingham & She). A role is a named job function within the organization typically in a hierarchical fashion. A user is a person who would be assigned one or more roles similar to a user in Microsoft Active Directory. In a system with only one administrator, the constraints may be meaningless. But, if the administration is decentralized, "meaning there are several administrators, the constraints will be used by the senior administrator to restrict the junior administrator's right to grant/deny the permissions" (Thuraisingham & She). It is critical to examine the business and plan the design of user roles and groups accordingly.

A common point of contention is how to segregate conflicting duties from the business organization to the cloud system. Roles need to be "aligned with business processes rather than specific users or jobs, as this will make it easier to ensure that appropriate access is granted to all users" (Ward, 2017). Cloud vendors may offer a solution, assistance or documentation for the Segregation of Duties (SoD) to help with the implementation of a cloud deployment. Poorly designed roles may lead to access issues such as too much or too little access being granted and will also make it more difficult to manage and report on the SoD" (Ward, 2017). Roles and permissions can cause cross issues either through design or planning. For example, giving a user "the ability to "Inquiry" may inadvertently gain

access to Add, Change and Delete to the database" (Ward, 2017). Hackers seek out design flaws and failures, which can only be found by digging deep into the details.

Another point of discord is the use of generic user accounts. These accounts typically have a bland username and a simple password if there is even one set. For full accountability during a security audit, “discourage the use of shared accounts or generic user accounts” (Ward, 2017). It is tempting for an organization to create generic accounts especially when multiple users share the same role or access, but this can have long-term effects. Tracking who used these accounts can be difficult to follow which removes the lack of accountability. Some organizations also fall under Data Protection laws that require audits that may leave a company fined for having such accounts or not being able to properly account for user logins.

Privileged user accounts such as super users, power users or administrator accounts hold an extraordinary amount of risk. These types of accounts typically have high to full access to most if not all data and modules. Based on the business size, "the same person will also be the database administrator and operating system administrator, which increases the level of risk even further" (Ward, 2017). Under this scenario, if that account was compromised, all users could be locked out and an attacker could hold the company at ransom. With privileged accounts, it is vital for processes and policies to be in place to document how these accounts are accessed and managed. It is good security practice to, "to avoid granting anyone full access to everything, but if you can’t avoid it you need to put compensating controls in place to monitor their activity" (Ward, 2017). This may be a difficult task, but consulting the vendor or a

security consultant may be necessary when internal knowledge is lacking.

Based on the company size and staff knowledge an easy area to be overlooked is establishing a regular process to do a user account audit. Having this process in place "ensures that appropriate business managers review and verify their users' access privileges and identify any changes that are needed, such as removing redundant access when responsibilities have changed" (Ward, 2017). Users can get assigned access or roles that may change over time or may have never needed in the first place. A periodic access review "can be a tedious and cumbersome process, but the review can assist to resolve risks associated with inappropriate access" (Ward, 2017). A standard review should provide a way of checking the integrity, as well as keeping the account database clean and free of errors. If thorough security measures and control processes are not in place, "updates and changes made to the organization's environment over time are likely to cause conflicts, which can pose varying levels of risk to the business and may ultimately force the organization to revisit its security design" (Parisian). Areas that can always be examined first include users with no roles or privileges, roles with no access or security records and enabled users that should be deleted.

Monitoring the user activity of an account with access can be a difficult task but is imperative. Most application systems do not have "real-time monitoring and alerting capability, because access control and monitoring is managed separately for each application or system, it is close to impossible to monitor individuals as a practical matter" (Oracle, 2015). Having a comprehensive activity logging process in place will better protect an organization.

Due to a compromise companies typically end up having to over-compensate in identity theft protection for victims as well as the cost to recoup any funds possible. Performing an internal audit can seem inefficient because, "it requires manual information-gathering, analysis, and reporting, as well as correlation when multiple applications and systems are involved" (Oracle, 2015). Some application systems have built special tools to analyze this data into a centralized location to help identify an issue before it can be used as a weakness. A criminal that exploits an application system can cost the company and the consumers when information is transmitted and left unsecured, when internal users have more access than needed or when accounts are left vulnerable. While compliance and data security can prove to be a difficult challenge, if organizations are proactive it can help to protect the company and the consumer.

Proposed Solution

As healthcare entities start to understand the potential threats associated with cloud applications, a standard document could be designed and shared. The HECVAT could be the foundation to the standard document, and then HIPAA related content could be added. Vendors could complete the documents and upload to a neutral online repository and update as needed. A central repository would allow healthcare entities to review the security of each potential applications before contacting the vendors for demonstrations and completing an entity-specific questionnaire.

Conclusion

The potential consequences can be detrimental to using a cloud-based application for healthcare that has not been

adequately vetted. A thorough investigation can allow the healthcare entity to identify any possible vulnerabilities prior to deployment. HIPAA guidelines aim to protect valuable patient data and hold healthcare agencies accountable for insufficient security controls, impermissible disclosure of PHI, or failure to manage risk. An open standard security guide for software assessment would allow all healthcare entities to be current to technology and HIPAA standards while analyzing cloud-based applications.

Future Research

Research in the future could be focused on the development of a standard security guide to assist healthcare agencies. Stakeholders and interested parties could be interviewed to gain valuable insight into the creation of a security guide. Over time, vendors could be asked to provide insight into the use and the potential for acceptance.

Bibliography

5 Ways To Manage Risk. (2014, July 4). Retrieved from DBP Project Managment: http://www.dbpmanagement.com/15/5-ways-to-manage-risk

A Risk Management Standard. (2002). Retrieved from The Institute of Risk Management: https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf

Arntz, P. (2019, March 6). *Spotlight on Troldesh ransomware, aka 'Shade'*. Retrieved from Malware Bytes: Blog: https://blog.malwarebytes.com/threat-analysis/2019/03/spotlight-troldesh-ransomware-aka-shade/

Barney, B. (2015, October 12). *9 Ways To Social Engineer A Hospital.* Retrieved from Security Metrics: https://www.securitymetrics.com/blog/9-ways-social-engineer-hospital

Barney, B. (2015, August 24). *Healthcare: Recognize Social Engineering Techniques.* Retrieved from Security Metrics: https://www.securitymetrics.com/blog/healthcare-recognize-social-engineering-techniques

Bevan, O., Ganguly, S., Rezek, C., & Kaminski, P. (2016, July). *The ghost in the machine': Managing technology risk*. Retrieved from McKinsey: https://www.mckinsey.com/business-functions/risk/our-insights/the-ghost-in-the-machine-managing-technology-risk

Breach Notification Standard Changed by HIPAA Omnibus Final Rule. (2013, January 22). Retrieved from McGuire Woods: https://www.mcguirewoods.com/Client-

Resources/Alerts/2013/1/Breach-Notification-Changed-HIPAA-Omnibus-Final-Rule-Risk-Harm.aspx

Cazier, J. A., & Medlin, B. D. (2010, September). Analyzing the Vulnerability of U.S. Hospitals to Social Engineering Attacks. *International Journal of Information Security and Privacy, 2*(3), 71-83.

Cloud computing: A complete guide. (n.d.). Retrieved from IBM: https://www.ibm.com/cloud/learn/cloud-computing

Davis, J. (2019, April 26). *Ransomware Attacks on Business Targets Increase by 195% in Q1.* Retrieved from CyberSecurity News: https://healthitsecurity.com/news/ransomware-attacks-on-business-targets-increase-by-195-in-q1

Fortify on Demand. (n.d.). Retrieved from Micro FOCUS: https://www.microfocus.com/en-us/products/application-security-testing/how-it-works

Francis, J. (2015, 10 14). *Cyberattacks Will Cost U.S. Health Systems $305 Billion Over Five Years.* Retrieved from Accenture: https://newsroom.accenture.com/news/cyberattacks-will-cost-us-health-systems-305-billion-over-five-years-accenture-forecasts.htm

Freund, J., & Jones, J. (2015). *Measuring and Managing Information Risk: A FAIR Approach.* Waltham, WA: Elsevier.

Guidance on HIPAA & Cloud Computing. (2017, June 6). Retrieved from U.S. Department of Health & Human Services: https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

Haney, G., Oliver, A., & Birchfield, M. (2019). *Vendor Audit.* IT Security. Johnson City: Ballad Health.

HECVAT. (n.d.). Retrieved from CalPoly: Security: https://security.calpoly.edu/ICT/hecvat

Higher Education Cloud Vendor Assessment Tool. (2019, May 24). Retrieved from Educause: https://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool

HIPAA Compliant Cloud Storage Solutions. (2019, February 19). Retrieved from Phoenix NAP: https://phoenixnap.com/blog/hipaa-compliant-cloud-storage

Humer, C., & Finkle, J. (2014, September 14). *Your medical record is worth more to hackers than your credit card.* Retrieved from Reuters: https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017, July 21). Security Techniques for the Electronic Health Records. *Journal of Medical Systems, 41*(8), 127. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5522514/

Maor, E. (2019, September 13). *Cybercriminals are Auctioning "Master Keys" for Admin Access to Health Care Portals*. Retrieved from IntSights:

https://intsights.com/blog/cybercriminals-are-auctioning-master-keys-for-admin-access-to-health-care-portals

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing.* Retrieved from National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Minksy, S. (2016, September 20). *The Wells Fargo Scandal is a Failure in Risk Management*. Retrieved from Logic Manager: https://www.logicmanager.com/erm-software/2016/09/20/wells-fargo-scandal-risk-management/

Omnibus Rule Revises What Constitutes a "Breach" . (2013, May). Retrieved from Silverstone Group: https://www.silverstonegroup.com/wp-content/uploads/2012/12/May-2013-Omnibus-Rule-Revises-What-Constitutes-Breach.pdf

Oracle. (2015, July). *Sustainable Compliance for the Payment Card Industry Data Security Standard (White Paper).* Retrieved from Oracle: http://www.oracle.com/assets/security-pci-dss-wp-078843.pdf

Parisian, A. (n.d.). *Oracle Security in the Cloud (White Paper).* Fastpath. Retrieved 2018

Qualys Cloud Platform. (n.d.). Retrieved from Qualys: https://www.qualys.com/cloud-platform/

Risk IT Framework for Management of IT Related Business Risks . (n.d.). Retrieved from ISACA: http://www.isaca.org/knowledge-center/risk-it-it-risk-management/pages/default.aspx

Risk Management Framework. (2019, April). Retrieved from NIST: https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview

Risk Taxonomy . (2009, January). Retrieved from The Open Group: http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf

RiskLens. (n.d.). Retrieved from RiskLens: https://www.risklens.com

Rouse, M. (2019, June). *incident response*. Retrieved June 2019, from TechTarget: Search Security: https://searchsecurity.techtarget.com/definition/incident-response

Rowe, C. (2018, June 20). *The 5 Step Risk Management Process*. Retrieved from Clear Risk: https://www.clearrisk.com/risk-management-blog/bid/47395/the-risk-management-process-in-5-steps

RQ: Risk Quantifier. (n.d.). Retrieved from Nehemiah Security: https://nehemiahsecurity.com/solutions/rq/

Stoneburner, G., Goguen, A., & Feringa, A. (2003, July). *Risk Management Guide for Information Technology Systems.* Retrieved from U.S. Dept of Health and Human Services: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf

Stulz, R. M. (2009). *Risk Management Failures - What are they and why do they happen?* Retrieved from Cornerstone Research: https://www.cornerstone.com/Publications/Research/Risk-Management-Failures

Summary of 2018 HIPAA Fines and Settlements. (2019, January 3). Retrieved from HIPAA Journal: https://www.hipaajournal.com/summary-2018-hipaa-fines-and-settlements/

Ten Common Risk Management Failures and How to Avoid Them. (2008, Ocotober). Retrieved from Protiviti: https://www.protiviti.com/US-en/insights/ten-common-risk-management-failures-and-how-avoid-them

tenable-io. (n.d.). Retrieved from Tenable: https://www.tenable.com/products/tenable-io

The Importance of Risk Management In An Organisation. (2013, August 15). Retrieved from CareersinAudit: https://www.careersinaudit.com/article/the-importance-of-risk-management-in-an-organisation/

Thuraisingham, B., & She, W. (n.d.). *Security for Enterprise Resource Planning Systems (White Paper).* Retrieved from University of Texas at Dallas: https://www.utdallas.edu/~bxt043000/Publications/Journal-Papers/DAS/J46_Security_for_Enterprise_Resource_Planning_Systems.pdf

van Oosten, C. (2015, March 24). *Verizon 2015 PCI Compliance Report.* Retrieved from Verizon Enterprise.

Ward, M. (2017, Septemeber 20). *ERP Audit Access Management Controls*. Retrieved from Q Software: http://www.qsoftware.com/audit-reporting/erp-audit-access-management-controls/

What is Cloud Computing? (2019). Retrieved from Amazon: https://aws.amazon.com/what-is-cloud-computing/

What is social engineering? (n.d.). Retrieved from KnowBe4: https://www.knowbe4.com/what-is-social-engineering/

Yampolskiy, A. (2016, October 27). *Healthcare Sector Among Most at Risk from Social Engineering.* Retrieved from Bank Info Security: https://www.bankinfosecurity.com/interviews/healthcare-sector-among-most-at-risk-from-social-engineering-i-3370

Yildirim, E. Y. (2016, November). *The Importance of Risk Management in Information Security.* Retrieved from World Search Library: http://www.worldresearchlibrary.org/up_proc/pdf/543-14829057935-8.pdf