2018

Exploring the Implementation of Cloud Security to Minimize Electronic Health Records Cyberattacks

Lamonte Bryant Tyler
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Lamonte Bryant Tyler

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Jon McKeeby, Committee Chairperson, Information Technology Faculty
Dr. Timothy Perez, Committee Member, Information Technology Faculty
Dr. Steven Case, University Reviewer, Information Technology Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2018

Abstract

Exploring the Implementation of Cloud Security to Minimize Electronic Health Records Cyberattacks

by

Lamonte Bryant Tyler

MS, Walden University, 2016

MLS, North Carolina Central University, 2001

MIS, North Carolina Central University, 2000

MA, North Carolina Central University, 1999

BA, Fayetteville State University, 1997

AA, Fayetteville Technical Community College, 1996

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

May 2018

Abstract

Health care leaders lack the strategies to implement cloud security for electronic medical records to prevent a breach of patient data. The purpose of this qualitative case study was to explore strategies senior information technology leaders in the healthcare industry use to implement cloud security to minimize electronic health record cyberattacks. The theory supporting this study was routine activities theory. Routine activities theory is a theory of criminal events that can be applied to technology. The study's population consisted of senior information technology leaders from a medical facility in a large northeastern city. Data collection included semistructured interviews, phone interviews, and analysis of organizational documents. The use of member checking and methodological triangulation increased the validity of this study's findings among all participants. There were 5 major themes that emerged from the study (a) requirement of coordination with the electronic health record vendor and the private cloud vendor, (b) protection of the organization, (c) requirements based on government and organizational regulations, (d) access management, (e) a focus on continuous improvement. The results of this study may create awareness of the necessity to secure electronic health records in the cloud to minimize cyberattacks. Cloud security is essential because of its social impact on the ability to protect confidential data and information. The results of this study will further serve as a foundation for positive social change by increasing awareness in support of the implementation of electronic health record cloud security.

Exploring the Implementation of Cloud Security to Minimize Electronic Health Records Cyberattacks

by

Lamonte Bryant Tyler

MS, Walden University, 2016

MLS, North Carolina Central University, 2001

MIS, North Carolina Central University, 2000

MA, North Carolina Central University, 1999

BA, Fayetteville State University, 1997

AA, Fayetteville Technical Community College, 1996

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

May 2018

Acknowledgments

Since 2000, my aunt Adelaide Davis has been in my ear about obtaining my doctorate. She never pushed but would always hint around. Thank you for your continuous encouragement. I would like to extend my gratitude to my committee, committee chair Dr. Jon McKeeby, my second committee member, Dr. Timothy Perez, and my university research reviewer (URR), Dr. Steven Case. Your continuous feedback has prepared me to this point, and now, I have a better understanding of how to scholarly write.

Dedication

I am dedicating this study to my family, friends, fraternity, martial arts family, and my late siblings (Andre Tyler and Tiffani Taft). Throughout this process, you all have been there with me. You all have been my primary support, and this is our study. After completing, my associate degree, my cousin Tracey told me that I bet not let the associates be my final degree. Once I finished my bachelor's degree, my children were my motivating factor to go further. After completing the first three masters, my Aunt Adelaide, Uncle Marion, and Uncle Lee motivated me to continue my education. Uncle Lee went on to obtain several college degrees to motivate me. Once my wife, Dawn Tyler decided to go back to school, I was motivated to pursue my doctorate. She has been my rock and I hope to motive her to pursue her doctorate. My mother, Dorothy Griffin has been my number one cheerleader and has supported me with everything that I have ever done in life. She may not have been a fan of me joining the military, but she signed the papers to make me happy. My Uncles Preston, Darrell, Robert, Barry, and Aunt Pam, has offered words of encouragement. I would like to give a special dedication to my cousins Kenneth and Baron. I also would like to dedicate my study to my line brothers of the Omega Psi Phi Fraternity, Inc. William, Travis, Nii, Aaron, Brian, Terris, Donoven, and Juno. I dedicate my study to my three best friends, Troy, Andre, Ramona.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Cyber is derived from cybernetics and cybersecurity is a state of being protected against the criminal or unauthorized use of electronic data. Data breaches in healthcare are growing every year (Roy, 2016). Cybercrime in healthcare can potentially upset the trust of the facility in perspective to the relationship with the patient. This section provided the background of the problem and the purpose of the study.

Background of the Problem

Senior (information technology) IT leaders use cloud computing to store and retrieve data over Internet services rather than a local server or personal computer (Madarkar, Anuradha, & Waghmar, 2014). Madarkar et al. stated that performance, accessibility, and security are principle research topics in cloud security, which security is a critical topic in the research. Additionally, Gazzarata, Gazzarata, and Giacomini (2015) supported the important of security by stating that IT must secure patient health information (PHI) in electronic health records (EHR). Furthermore, cloud providers also serve applications with restorative research which makes cloud security vital in various countries. Madarkar et al. stated the absence of cloud security permits cyberattacks to compromise end client through which attackers can gain personal data. Therefore, an exploration into cloud security and EHR was vital.

Securing information was an urgent issue because business applications depend on concentrated sharing of Internet data (Kaddoura, Haraty, Zekri, & Masud, 2015). A legitimate exchange of electronic information can pass along a malware attack, which can

infect the rest of the database (Kaddoura et al.) Additionally, conventional strategies require checking the whole log for the duration of the attack, which is a moderate methodology (Kaddoura et al.). Therefore, new strategies were needed to ensure cloud security with EHR systems.

Problem Statement

Cyberattacks represent a risk to the security of patients' EHR (Mehraeen, Ghazisaeedi, Farzi, & Mirshekari, 2016). Majhi, Patra, and Dhal (2016) uncovered that 60 to 80% of security vulnerabilities in cyberattacks are because of system misconfigurations and absence of adequate security controls. The general IT problem is that cyberattacks disrupt patient safety and security. The specific IT problem is that some senior IT leaders in the healthcare industry lack strategies to implement cloud security to minimize EHR cyberattacks.

Purpose Statement

The purpose of this qualitative case study was to explore strategies senior IT leaders in the healthcare industry use to implement cloud security to minimize EHR cyberattacks. The population was senior IT leaders within a medical facility in Baltimore, Maryland who had strategies to implement cloud security to minimize EHR cyberattacks. The implication for positive social change was that the findings from this study reduced unauthorized exposure of health records to the public.

Nature of the Study

Qualitative, quantitative, and mixed method designs were considered for this study. Qualitative methods are intended to authenticate thoughts and reflections (Miner-

Romanoff, 2012). The qualitative method was appropriate for this study because the qualitative method explored authentic thoughts and reflections about how practitioners protect their systems from cyberattacks. Quantitative research is a practical technique for looking at connections between variables (Nimon, 2011). Quantitative research methodology was not chosen for this study because I was not looking at connections between variables. The mixed method approach includes the combination of qualitative and quantitative data (Cameron & Molina-Azorin, 2011). A mixed methods design was not selected as the research question does not require quantitative research. The qualitative method provided the flexibility to investigate how to implement cloud security to minimize EHR cyberattacks.

The design options for this study were case study, ethnography, and phenomenology. A case study is a variation that incorporates two or more perceptions of the same phenomenon (Santos & Eisenhardt, 2004). A case study design was used for this study to help produce precise descriptions of how to minimize cyberattacks. An ethnography study design helps investigates the functioning of cultures through the study of the social interactions and interpretations between individuals and groups (Keutel, Michalik, & Richter, 2014). Ethnography was not selected for my study because the purpose of this study was not to describe the functioning of social groups. The role of phenomenological research design is to understand how people live through a phenomenon (Miner-Romanoff, 2012). The phenomenological research design was considered, but the focus was not on a common phenomenon outside of the research

problem. In alignment with the research question, the most appropriate methodology for this study was the qualitative case study.

Research Question

What strategies do senior IT leaders in the healthcare industry use to implement cloud security to minimize EHR cyberattacks?

Demographic Questions

1. What is your role within your organization and do you have a team whose focus is primarily cloud security?
2. Describe the architecture of your EHR. Include if you have your cloud or use the third-party vendor. Describe the responsibility of a third-party vendor if applicable. What is your role in keeping EHR secure?

Interview Questions

1. What strategies have you used to implement cloud security to minimize EHR cyberattacks?
2. What are the challenges that you face that affect the security of patient EHR in the cloud?
3. What do you see as being the greatest motivation for those who wish to infringe on the facilities EHR?
4. How do you maintain the security of the EHR in the cloud?
5. What tools do you use to provide security of EHRs in the cloud? How do you use the tools? What do you do when vulnerability is identified?

6. What metrics do you use to assess the level in which the EHR is secure, at what frequency do you review these metrics, and who are these metrics reviewed with?
7. What is your role if a breach of the entire system is identified?
8. What is your role in the forensics of an identified breach of EHR as a suitable target for a cyberattack?

Conceptual Framework

The theory supporting this study was routine activities theory (RAT) which I selected over lifestyle exposure theory (LET), lifestyle routine activity theory (LRAT), and the theory of technology enabled crime. While authors attempt to legitimize their decision of rival theories, rival theories should not scrutinize the study determination unless the scholar can give a rationale behind why it is unusual during data collection (Baškarada, 2014). Imperfect rivals typically are preferred (Ralph, 2014), but in 1979, Cohen and Felson developed RAT to help assemble some diverse and previous unconnected criminological analyses into a single substantive framework.

RAT includes a core mapping of the criminogenic circumstance, which are motivated offenders, suitable targets, and absence of capable guardians (Drawve, Thomas, & Walker, 2013; Leukfeldt & Yar, 2016). Additionally, researchers use RAT to highlight the character of offender motivation, target suitability, and effective guardianship in explaining victimization patterns (Drawve et al., 2013). While a large group of research has drawn on RAT to advance comprehension of the geographic and worldly designing of crime, the focal components of the position, target reasonableness, guilty party motivation, and guardianship, are likely relevant to a broad range of

criminological results (Drawve et al., 2013). Notwithstanding an objective's reasonableness, the approach of an inspired criminal is required before a crime can happen of which Drawve et al., (2013) stated that the inspiration pushing a criminal can fluctuate by the description of the offense being submitted or the guilty party. Furthermore, guilty parties encouraged by weakness will probably use medications and liquor among their crime (Drawve et al., 2013). The frameworks aligned with cloud security and helped explore what would motivate offenders to hack into the EHR of medical facilities, who the suitable targets are, and how to protect those targets.

Definition of Terms

Cloud security. Cloud security is a model for empowering, network access to a shared pool of configurable processing resources that can be quickly provisioned and discharged with less administration exertion or service provider communication (Daylami, 2015).

Cyberattacks. The perpetrator intentionally misuses the computer systems or network (Rid & Buchanan, 2014).

Electronic health records (EHR). EHR is an electronic version of patient data kept over a period which can be accessed within the same network (Krist et al., 2014).

Malware. Malware, also known as malicious software, are intrusive or annoying programming that presents an issue in cloud security (Singh & Khurmi, 2015).

Private cloud. A cloud which is in an internal datacenter and not available to the public is known as a private cloud (Goyal, 2014).

Public cloud. A cloud which is pay-as-you-go to the public is known as a public cloud (Goyal, 2014).

Routine activities theory. RAT helps to explain that crime transpires, and criminals do not go out of their way to engage in crime. They take the time for offending while engaging in their regular actions (Corcoran, Zahnow, & Higgs, 2016).

Senior IT leader. Senior leaders are those who obtain positions within an organization, and the acquisition of their strategic skills become more important for efficient performance than their cognitive skills (Day, Fleenor, Atwater, Sturm, & McKee, 2014).

The theory of technology enabled crime. The theory of technology enabled crime suggests that crime is universal and depends on the availability (McQuade, 1998).

Victimology. Victimology correlates to crime legal, and scientific spheres such as international human rights law and humanitarian law, and to the criminal sciences including criminal law, criminal procedures, international criminal law, and of course, criminology (Asli, 2013).

Assumptions, Limitations, and Delimitations

There are several events influencing research and the outcomes. Acknowledging and documenting these events is part of obtaining integrity. The situations that occur in research are assumptions, limitations, and delimitations. I outlined the assumptions, limitations, and delimitations of this qualitative case study.

Assumptions

Corbin and Strauss (2014) indicated that assumptions are aspects that are accepted to be true without proof and includes beliefs about the subject. I assumed that the participant's results covered the overall organization. Additionally, I assumed that the participants answered each question accurately as possible. Finally, I expected that all participants provided me insight as to how to minimize EHR cyberattacks.

Limitations

Limitations are restrictions, shortcomings, or defects that limit the extent of realism in research (Busse, Kach, & Wagner, 2016). One potential limitation that was a factor in this study was the lack of participation from the senior IT leaders. Another limitation is private cloud versus public cloud. Some information was limited to what the IT leaders shared based on the privacy and security necessary for hospital information systems.

Delimitations

Delimitations are boundaries that a researcher sets for the study (Svensson & Doumas, 2013). The initial delimitation for this study was using a healthcare facility in Baltimore, Maryland, which is a public organization. Additionally, participants were from multiple departments within the organization, which requires participants to have at least five years of experience in cybersecurity and at least two years in their current role in their current position within the organization.

Significance of the Study

I have not found any other studies resembling the implementation of cloud security to minimize EHR cyberattacks, which is an opportunity to enhance the knowledge and practice in the area. Additionally, the improvement of the practice coincides with preventing the unauthorized disclosure of information. Therefore, this study may have significance on the professional practice as well as social change.

Contribution to Information Technology Practice

The focal point of the IT practice contribution was exploring strategies to minimize EHR cyberattacks. García-Valls, Cucinotta, and Lu (2014) stated that numerous organizations convert to cloud security despite the risk of security infringement. Additionally, Younis, Kifayat, and Merabti (2014) viewed cloud security as a standout amongst most ideal models in the IT. Furthermore, Salah, Calero, Zeadally, Al Mulla, and Alzaabi (2013) added that cloud security provides proficient malware identification for up to date activity status of the threats, which includes scanning in the cloud to prevent threats from reaching the client. Therefore, the strategic implementation of cloud security may cause an efficient early detection to avoid system unavailability.

Implications for Social Change

The implication for positive social change was that cloud security might reduce or eliminate the loss of patient's information as well as breaches of patient's privacy. Cyberattacks may result in data corruption (Teixeira, Shames, Sandberg, & Johansson, 2015) which prevents medical staff from accurately treating a patient. For example, the staff at a healthcare organization affected by a malware event may not be able to access

data essential for proper patient care, creating a risk for patient errors such as improper medication delivery. Additionally, the release of personally identifiable information can result in identity theft that undermines the patient's security and privacy. Therefore, reducing the occurrence of cyberattacks ensured that critical medical support systems remain in place and the assurance of patient's privacy.

A Review of the Professional and Academic Literature

The focus of this literature review was to provide a background to cloud security, cloud platform, the effects of malware, cyberattacks, and security risk in healthcare associated with the cloud. A breach of cloud security can affect many areas of technology. The literature review includes information on nine main themes. The themes include (a) history of cloud security; (b) system security; (c) risk, security, and privacy; (d) private cloud; (e) cloud platforms; (f) malware; (g) cloud in IT medical field; (h) conceptual framework; (i) cyberattacks and cloud security in healthcare. The cloud security themes were chosen to highlight the impact of malware and the primary theme risk, security, and privacy in healthcare.

This literature review contains articles from the Education Resource Information Center (ERIC), Thoreau Multi Database Search, Academic Search Complete, ProQuest Central, Google Scholar, SpringerLink, and ScienceDirect. Ulrich was used to verify that the references included in this study were peer reviewed. The literature review includes 99 articles, which 89 (90%) are peer reviewed and 87 (88%) articles are within the five years of expected CAO approval. In the literature, I reviewed the conceptual frameworks

(RAT and the rival theories LET, and technology enabled crime theory) and how they are applied to case studies.

History of cloud computing

Cloud computing was researched in the 1960s. Rajaraman (2014) stated that McCarthy suggested that cloud computing should become like a utility such as a telephone. The discussion of cloud computing lapsed between 1970s and 1990s; Jeong, Yi, and Park (2016) stated the reason was that computers were neither compact nor affordable for many individuals and organizations. Additionally, Helo, Suorsa, Hao, and Anussornnitisarn (2014) indicated that the components or ideas of cloud computing have not changed since the 1970s regarding the rationale between the applications, but Jeong (2016) stated that bandwidth for the Internet became widely available that improved access in the 1990s. Therefore, the increase of bandwidth availability brought the earlier cloud concepts to fruition.

Cloud computing has gone through many changes. Modic et al. (2016) indicated that cloud computing matured as an enabler for outsourcing data storage and processing needs which Helo et al. (2014) stated that this maturation requires a modification of cloud security. Additionally, cloud computing provides the ability to store and retrieve information from the cloud anyplace by interfacing the cloud application through the Web (Rao & Selvamani, 2015). Furthermore, Hashizume, Rosado, Fernández Medina, and Fernandez (2013) and Kumar, Gupta, Charu, Jain, and Jangir (2014) found that resources exist dynamically in cloud computing, but with more points of entry and more interconnection complexity with virtualized technology. Therefore, cloud

computing is a form of Internet-based, shared computing that requires a careful review of cybersecurity.

Some employees preserve IT costs because the organization only pays for what they used. Kushida, Murray, and Zysman (2015) stated that cloud computing advanced as the primary resource became less expensive, which aligns with the goal of cloud computing providing a reduction of IT expenses such as IT staff. Additionally, Chou (2015) noted that organizations do not need to invest in hardware, software, networking, and hiring IT staff, which organizations can offload into separate cloud infrastructures. Furthermore, Krishna, Kiran, Murali, and Reddy (2016) suggested that cloud computing provides organizations with the ability to plan, maintain, and control how employees save and retrieve organization's work. For example, Chou indicated that cloud platform services permit clients to use provider applications that run on a cloud infrastructure, which allows the client to control the application software. However, the developer must know how to work with clients to run selective software in the organizations (Chou, 2015). Therefore, clients have increased efforts, document control and can work from anywhere just from moving to the cloud. The cloud offers flexibility to organizations.

There are many technologies involved with cloud security. Asija and Nallusamy (2016) noted that the acceptance of cloud security allows careful IT considerations to change over to a progression of smaller working costs. Additionally, cloud security draws from all technologies such as Web services, virtualization, service-oriented architecture, and grid computing, and business models used to address IT aptitudes (e.g., software, platforms, hardware) as a scalable, flexible service applications (Kumar et al., 2014).

Although cloud-based organizations reduce costs for development by remaining agile, the level of cost reductions depends on the project (Almudarra & Qureshi, 2015). Therefore, agility in a cloud model manifests cost and time outcomes, although there is no effect on the quality due to security and privacy issues.

System Security

There was a need for system security in all fields that involves computer networks. One of the main concerns in development and operation of mission critical systems is system security. Kalloniatis et al., (2014) stated that organizations must correctly specify and implement system security requirements. Case and King (2014) stated that system security is a constant concern with stakeholders, and it was one of the greatest IT skill demands in 2013. For most organizations, risky electronic behaviors are minimal and are not likely a major security concern however, Jouini, Rabai, and Aissa, (2014) contested that information systems threats may cause a financial loss. The effects may vary such as in confidentiality or integrity of data, and others affect the vulnerabilities of the system (Jouini, Rabai, & Aissa, 2014). Jouini et al. (2014) stated that vulnerabilities are exploited weaknesses in a system by attackers who have a significant impact on the system. With the existence of vulnerabilities in a system, a threat may be revealed through a threat agent using an analytical diffusion method to produce undesired consequences.

Security in the Cloud

Procedures and individuals contribute to the development of risks. Cioca and Ivascu (2014) stated that cloud security involves security risks that may lead to hackers

attacking stored data, which Ali, Khan, and Vasilakos (2015) reported that understanding cloud security requires familiarization of the ideas that contribute with cloud computing. Additionally, new conventional devices are used and are depended on upon to upgrade and survey the quality of cloud security (Shaikha & Sasikumarb, 2015), which Arpaci, Kilicer, and Bardakici (2015) stated the survey includes the risks with transmitting sensitive data with cloud policies. Furthermore, Ali et al. (2015) noted that the security configurations of the cloud design are significant to providing secure cloud administrations to the client because misconfigurations can profoundly trade off the security of customers, applications, and the entire systems. Therefore, configuration requires appropriate setup for cloud computing usage, which includes keeping the system reliable with security strategies.

There is a risk of information abuse when organizations offer assets. Thus, securing data repositories is necessary to minimize risk (Schniederjans & Hales, 2016). For instance, Safa and Solms (2016) suggested that by sharing information-security knowledge help increase the level of knowledge and save money for the organization. Saving money usually happens with an acceptable tradeoff, but in exchange, data could be sold to a third party. Additionally, there are security risks in the field of cloud security (Rao & Selvamani, 2015; Shaikh & Sasikumarb, 2015), which Kote, Raja, and Raju (2015) included data breaches that have significant consequences due to the malicious user obtaining cloud data in a high esteem attack. Therefore, the leaks can lead to ruined reputations for the organizations.

Data privacy. Data privacy delimits the information that an individual or organization share. Shaikh and Sasikumar (2015) stated that data privacy issues are a concern while moving information through the cloud environment. However, Arpaci et al. (2015) stated the understanding of cloud security depends on the organization or individual's attitude towards the topic. Therefore, the management of an organization's IT team needs to project a vigilant attitude about data protection to ensure privacy and data security.

An effective cloud security policy should be clear and concise. Soomro, Shah, and Ahmed (2016) stated an effective information security policy has a role in managing information security with the development and implementation of cloud security. Additionally, Öğütçü, Testik, and Chouseinoglou, (2016). stated that as information related privacy issues are subject to the interpretation of the organization's legal team as cyber threats grow with technology, which includes measuring individual security awareness. Soomro et al. (2016) stated that some risks include changes in official outlines and information management systems. The organization structure for information security should facilitate reporting, efficient communication, clear authority, and fast workflow (Soomro et al., 2016). Users may not fulfill security requirements despite the awareness of security risks which increases security risks as IT transitions into online business (Soomro et al.). Security threats are not only a threat but a business as well.

Information security policies have a role in an organization's data management strategies, of which information security management should have visibility and have a positive impact on employee adherence to information security policy. Soomro et al.

(2016) stated that information security policy is ineffective without training and enforcement. Senior IT leaders should include measures to enhance information security policy awareness and training. Information security policy allows employees with information assets protection from malicious attacks and other vulnerabilities (Zang, 2014). Zang suggested that employees are the main reasons for data breaches and information security risks, as opposed to hackers and system failures. An assessment of information security risk is part of risk management which includes assessing risk, using qualitative and quantitative approaches, and incorporating means to counter these vulnerabilities (Zang). The private cloud contributes greater security facing these risks.

Private Cloud

An organization operates the entire infrastructure of a private cloud. The organization may manage the private cloud with a third party and may exist on premise or off premise (Goyal, 2014; Rani et al., 2015). A private cloud is available solely for a single organization. Private cloud purposely restricts access to its support to aid consumers from the same organization that controls the cloud (Jain & Kumar, 2014). A private cloud presents greater security than public clouds to an organization which has control over the infrastructure. A private cloud allows the organization to maintain the same workflow and security procedures which ensures the correct level of code is being executed. The private cloud is not hindered by network bandwidth and availability issues associated with public clouds (Jain & Kumar, 2014). Goyal (2014) and Rani et al., (2015) concurred that the advantage of a private cloud versus the public cloud is that of data security and privacy and the private clouds can offer the provider and user greater

control, security, and resilience (Jain & Kumar, 2014). The primary goal of the private cloud is to sustain a harmonious level of authority over governance, privacy, and security (Jain & Kumar, 2014). Rani et al., stated that due to limited resources, some disadvantages are the limited scalability and inflexible pricing. The significant detriment of private cloud is its more substantial cost than a public cloud.

Several private cloud providers supply object storage services (Bacis et al., 2017) such as Hewlett Packard Enterprise (HPE), VMware, Dell, Oracle, IBM, Microsoft, and Amazon Web Services (AWS). Cloud providers could infer sensitive information about the user accessing the cloud and the possibly delicate content of the outsourced dataset (Bacis et al., 2017). Transferring data to the cloud entails the secure management, storage, and protection of accesses to data.

HPE is a principal leader in the private cloud market. HPE's private cloud contributions include hardware, software, and services (Hsu, Ray, & Li-Hsieh, 2014). VMware is known for its virtualization software that runs many private cloud environments. Dell's private cloud incorporates virtual private cloud services, cloud management, and cloud security software, and other consulting services (Hsu et al.). Oracle includes its cloud platform, applications, infrastructure, lifecycle management tools and integration services (Hsu et al.). IBM includes hardware such as hosted private cloud services, IBM systems and IBM storage, cloud security tools and software like cloud manager and cloud orchestrator, and IBM cloud managed services (Hsu et al.). Numerous private clouds are running on Microsoft's Windows Server operating system which is integrated into Windows Server.

Cloud Platform Services

Cloud security platform services should consistently strive to contribute new services clients. There are three leading cloud platforms for cloud security: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS; Cioca & Ivascub, 2014). Cloud vendors deliver products to users within the various forms of SaaS, PaaS, and IaaS (Kshetri, 2013). Brender and Markov (2013) indicated that SaaS depends on IaaS and PaaS because SaaS incorporates elements of both IaaS and PaaS. SaaS provides a spectrum of applications in the form of word processing and spreadsheets. Kumar et al. (2013) suggested that cloud security offers an innovative method of computing with different service models that support various services to the users. PaaS hosts the hardware and software in its infrastructure (Kumar et al., 2014; Krishna et al., 2016). SaaS is where cloud providers establish and administer software in the cloud. To determine which platform to use for business, one should access the cloud need.

Cloud-based applications are deployed in the cloud and executed while in the cloud. The hybrid software deploys in the cloud, but runs on premise, or deployed on premise and runs in the cloud (Krishna et al., 2016). With on premises software such as Office 2010 deployment, there are many benefits that the cloud provider cannot provide, such as infinite scalability. The model of on premises software also is the same as the legacy (Krishna et al.). As stated by Krishna et al., on premises software usually requires a license for the end user or server whereas, legacy software such as Office requires a license per device. Cloud base software offers concurrent licenses.

Infrastructure as a service. An IaaS refers to devices that can be accessed over the Internet. IaaS will transform the role of the IT department, and this is an essential analysis to make (Sultan, 2014). The customer can outline computing means such as processing, storage, and networking services (Kumar et al., 2013). The issues related to IaaS in cloud security are asset, data, foundation system management, virtualization and multi-tenure, application programming interfaces (APIs), interoperability, and security (Madni, Latiff, Coulibaly, & Abdulhamid, 2016). The outcomes of these issues can convey in the class of full or partial infrastructure disruption.

The IaaS provider supplies the physical handling and stockpiling organizations with the system. Significant computation assets guarantee the facilitating environment and the cloud foundation for the IaaS consumers (Zota & Petre, 2014). The users of the cloud use IaaS to support operations (Cioca & Ivascu, 2014). The most difficult issue for IaaS in cloud security is taking care of and giving practical usage of property (Madni et al., 2016). IaaS helps to free up staff, and the infrastructure is flexible and scalable, which indicates that it expands and advance immediately.

Users do not control the infrastructure, but they do have control over the operating system. Hashizume et al. (2013) expressed that IaaS provides assets (i.e., servers, networks, and other processing resources) as virtualized systems through the Internet. Hashizume et al. stated that, with IaaS, cloud clients have better control over the security contrasted with alternative models as long there is no security chasm in the virtual machine (VM) screen. Clients control the product running on their VMs, and they are trustworthy to design security methods accurately.

Cloud suppliers manage the hidden registry, system, and capacity system. IaaS providers must attempt to secure their systems to minimize the risks that come from production, correspondence, observation, adjustment, and versatility (Hashizume et al., 2013). A primary reason for heightening security is because an outside vendor is managing the security of the products. A third-party vendor of IaaS is AWS. AWS offer to supply clients a grouping of records to help them in acquiring their agreement which incorporates the validation of Payment Card Industry consistency for AWS and irregular documentation (Rasheed, 2014). AWS provide general control concerning the balance between the security duties (Rasheed). AWS provides on-demand cloud computing platforms to organizations.

Platform as a service. PaaS give the freedom of managing application without the complexity of maintaining the infrastructure. PaaS provides a platform for executing applications and allowing individuals to develop and run software that can be used to deliver significant levels of service (Krishna et al., 2016). Third party vendors such as Google App Engine deliver computational resources through PaaS (Spoorthy, Mamatha, & Kumar, 2014). They can manage the runtime, middleware, operating systems, virtualization, servers, storage, and networking, which leave the user to manage applications and data.

Sometimes, there is no cost associated with PaaS. PaaS sends cloud-based applications over the Internet without the cost of purchasing and managing the essential equipment and programming layers (Hashizume et al., 2013). PaaS customers receive an available platform, through which they can deploy applications developed in a request in

the language (Kumar et al., 2013). The supplier manages the cloud base for the stage and procurements performance devices and assets for the consumers to create, test, actualize, and manage applications (Zota & Petre, 2014). PaaS does not replace infrastructure.

PaaS focuses on middleware which provides development tools and hosting options for cloud providers to manage. The selection of PaaS permits the use of remote VMs as a part of a point of community equipment and programming, evading tedious and costly demonstrations and additionally challenging support assignments. PaaS expands efficiency, gives organizations a chance to discharge items more quickly, and lessens programming expense (Coccoli, Maresca, Stanganelli, & Guercio, 2015). PaaS enables self service capabilities so that the end users can become more proficient developers, and it improves the developer productivity with a simple to use interfaces. As organizations modernize, platforms need to be upgraded. Consumers must stay up to date with the application packages. Bayramusta and Nasir (2016) indicated that consumers regulate the application packages, but they do not regulate the servers and operating system. The consumer has control over the application design (Bayramusta & Nasir, 2016). The consumer does not have control over the cloud infrastructure.

PaaS application security involves two programming layers: security of the PaaS stage and security of client applications conveyed on a PaaS stage. PaaS suppliers oversee securing the stage programming stack that incorporates the runtime motor that runs the client applications (Hashizume et al., 2013). Hashizume et al. (2013) claimed that PaaS provides common programming languages and it offers outside Web

management segments. Also, PaaS consumers need to rely on the security of Web facilitated improvement devices and third-party organizations.

Software as a service. SaaS is more of a model for delivering licenses. SaaS allows the cloud supplier to achieve, provide, and redesign the working method of the product applications on a cloud system so that the provisioned organizations meet the comparable level for the advantage of the customer (Zota & Petre, 2014). SaaS is probably the most known services of the cloud which provides on demand software services (e.g., Google Apps, Adobe Creative Cloud, and AutoDesk; Krishna et al., 2016). Cotroneo (2016) indicated that the ubiquity accumulated by the SaaS worldview to convey essential business applications had made the cloud a delicate security target. The underlying drivers circulated by patterns are viewed by different studies with regards to valuable associations and provide details regarding real security risks in the Cloud (Cotroneo, 2016). Security risks are concerns in SaaS due to the vulnerability of data not being secured.

SaaS is vulnerable because attackers can access data through other software on the same VM. Among the current studies on SaaS appropriation, Yang, Sun, Zhang, and Wang (2015) qualitatively surveyed the effect of IT infrastructure development and vulnerabilities. SaaS customers can administer applications in the cloud and can access it through numerous clients covering browsers and transportable devices (Kumar et al., 2013). A SaaS vendor such as Force.com manages the runtime, middleware, operating systems, virtualization, servers, storage, and networking, which leave the user to manage

applications and data (Spoorthy et al., 2014). Then you have the IaaS providers who do not manage runtime.

The customers are responsible for cloud services, whereas the provider stops the security capabilities. The customer is responsible for the security of software in IaaS architecture (Brender & Markov, 2013). The SaaS provider ensures the security of the applications (Brender & Markov, 2013). With control over security, transparency, and compliance, private cloud providers can receive substantial operational expenditures. The public uses the public clouds (Brender & Markov, 2013). The use of a private cloud provides preferences in healthcare through expanded soundness, security, and patient protection, as the healthcare organization maintains control and responsibility for the patient information (Lin et al., 2014). Community clouds implement cloud support for various organizations with the same security concerns and requirements. The hybrid clouds (public, private, or community) share standards that enable data and application portability (Brender & Markov, 2013). Hybrid cloud users should consider whether appropriate network connectivity and visualization are available.

A developmental model may build up a superior comprehension of natural elements regardless of whether to consider these issues while detailing an expectation to embrace SaaS. The effects of technological, organizational and environmental components on SaaS selection are a requirement for a developmental model that catches their overall effect (Yang et al., 2015). Kshetri (2013) explained that SaaS is a software performance model that provider hosts applications accessible to consumers over a network. Because of concerns associated with security, privacy and confidentiality critics

have argued that costs may outweigh the benefits (Kshetri, 2013). A substantial gap in SaaS remains within the cloud's security, privacy, and transparency.

Cyberattacks and Cloud Security in Healthcare

Cyberattacks come in many forms that are harmful towards private information such as protected health information (PHI) stored in EHR. Hashizume et al., (2013) stated to protect a patient's privacy; a requirement is to remove the PHI from the medical records before becoming publicly available for non-hospital researchers. Cyberattacks are socially or politically impelled attacks delivered primarily through the Internet. Attacks focus on the overall population of national and corporate organizations and are helped through the spread of vindictive projects, unapproved websites, fake sites, and a different method for taking individual or institutional data from focuses of attacks, bringing about the comprehensive impairment (Vale, 2014). Rid and Buchanan (2014) declared that the harm brought about cyberattacks is one of the essential recognizing elements of a network breach. The harm of a cyberattack, as opposed to offenses, is quite often exceedingly hard to bind and to measure.

The use of cloud security can no longer become the primary protection for the security of the EHR system. EHRs are exposed to cyberattacks as pointed out by Chen, Abdelwahed, and Erradi (2014) because it acquires the vulnerabilities of computers, hardware, software, and the network. Modern cyberattacks that sidestep the primary line of defense in organizations can be recognized and characterized by malware protections such as Malwarebytes (Rid & Buchanan, 2014). According to Jang-Jaccard and Nepal (2014), more than one million people are victims of cyberattacks daily which equates to

fourteen people per second. Levesque, Fernandez, and Somayaji (2014) suggested that understanding what type of patients and user are more helpful for cyberattacks is critical. The reason is that the analysis helps if IT needs set up an adequate system to alleviate and manages the impact of computer crime (Levesque et al. 2014). In healthcare, cyberattacks are becoming an issue.

Cyberattacks in healthcare and the EHR system is a reason for increasing the cloud security. Cloud security can enhance the conveyance of healthcare services benefits and can likewise profit healthcare research (Ermakova, 2015). With the current practice of healthcare, cloud security can help engage experts to convey better performances in viable organizations (Kaur & Chana, 2014). Cloud security offers many open doors and risks, but the risk depends on very delicate health information to be overseen remotely by cloud suppliers (Kaur & Chana, 2014). Cloud security in healthcare is a necessity (Kaur & Chana, 2014). With the exchange of information in the cloud, it is difficult for healthcare organizations to disclose whether the cloud is legal under the national security.

Numerous healthcare organizations keep EHRs behind a protected firewall. At present, health insurance portability and accountability act (HIPAA) and the American Recovery and Reinvestment Act (ARRA) within healthcare are advancing the relocation of EHRs to the cloud (Lin et al., 2014). Lin et al. (2014) stated that cloud customers should work with cloud suppliers who are HIPAA compliant to meet administrative regulations. Kshetri (2013) stated HIPAA requires technical, physical, and administrative security by healthcare providers to protect the privacy, integrity, and availability of patients' data. If found not in compliance with HIPAA standards, organizations may face

a fine up to $250,000 and ten years in prison. Healthcare organizations should check that potential cloud providers have strict protection and security conventions before signing a service contract (Lin et al., 2014). The contract will include more than just taking looking at the site of a cloud provider (Lin et al., 2014). The client should access the cloud supplier as a potential business associate (BA), which is required by HIPAA.

Cloud in IT Medical Field

There are numerous reasons why leaders of healthcare organizations resisted and now moving into the cloud. Healthcare organizations opposed the use of the cloud because of the result of discomfort avoidance, indolence, unique value, switching costs, and perceived threat. Attitude, subjective norm, and perceived function control are shown to have a direct effective on healthcare professionals' intention to use the cloud (Hsieh, 2015). Healthcare professionals within the healthcare organization see merit in cloud computing and use it and defend its usefulness for their operations (Sultan, 2014). Concerns such as security, privacy, and availability are among the highest solicitudes in healthcare's cloud adoption determinations preferably than the increasing cost of control (Kshetri, 2013). Healthcare organizations also are moving to the cloud because the organizations see it as being cost effective (Gupta, Seetharaman, & Raj, 2013). Moving to the cloud saves healthcare on power and people cost as well as zero capital cost.

Use of cloud in IT medical field has immensely expanded. Santos, Macedo, Costa, and Nicolau (2014) communicated that the developed support within healthcare organizations is an objective for cyber criminals because of the profusion of personal information they accumulate that can be adapted. Technology enabled crime produces

substantial criminal action in the cloud (Santos et al., 2014). Cyber criminals, in any case, are occupied with the information housed in HIS that can be misused for individual or business interests (Luna et al., 2016). Controls at present exist to keep these technologies enabled crime operations under control in many areas of data innovation (Luna et al., 2016). A few zones, advancement must fill a security void.

Health information systems cover an extensive variety of digital innovation and are progressively assuming a part in all procedures, for example, patient registration, data checking, lab tests and radiology. Around 95% of qualified medical facilities have received health information technology and exhibited significant use of this innovation (Luna et al., 2016). The extension of medical devices offers many points of entry to data systems, which add to information breaches (Luna et al., 2016). Technology enabled crime and data security are classified into two comprehensive fields: (1) interior threats that emerge from unseemly access of risk information by inside parties abusing powerlessness of data systems, and (2) exposed risks arising from outside professionals in the data flow chain misusing the revealed information past it's expected use.

Health information systems surround a comprehensive collection of technologies required for managing and sharing patient data electronically. The market has now come to depend intensely on these advances, which introduce risks that can prompt to foreswearing of administration and data breaches. Data breaches are the greatest threat to healthcare organizations and, more particularly, data fraud is the fundamental element encouraging impending security risks (Luna et al., 2016). Understanding criminal

motivation in healthcare, you can prognosticate inherent crimes to prevent possible crimes. In this way, RAT was in harmony with the development of cybercrime.

Conceptual Framework

Founded by Lawrence E. Cohen and Marcus Felson in 1979, routine activity theory (RAT) was to help assemble criminological reviews into a substantive system. RAT proposes that victimization measures diverge transversely for demographic because individuals engage in different activities (Cohen & Felson, 1979). Routine activities interfere the similarities connecting demographic characteristics and victimization (Bunch, Clay-Warner, & Lei, 2015). Cohen and Felson (1979) introduced RAT to help expand the theory of human ecology by Hawley in 1950. Hawley believed that there are three components of human life: rhythm, tempo, and timing (Cohen & Felson, 1979). Rhythm, tempo, and timing influence the rates at which people carry out crime.

Researchers have utilized RAT as the information systems security research when assessing the distinctions between events or vulnerabilities in an environment and implemented protections and safeguards established within an environment (Khey & Sainato, 2013). Researchers theorized that RAT might be alluring to a prospective offender of crimes because of their belonging or something inherently attractive about that person (Holt & Bossler, 2013b). The aim should likewise be in close physical and temporal proximity to a guilty party to be known and perceived.

Routine Activities Theory

Studies that analyzed RAT frequently focus on the overall culpable crime mirroring the conjunction of these components of crime (i.e., motivated offenders,

suitable targets, and absence of guardians). Cohen and Felson (1979) suggested that the probability of crime is extended when the three precepts of RAT are united in space and time (Williams, 2015). The three components are a motivated offender, a suitable target and the absence of a capable guardian (Choi, Cronin, & Correia, 2016; Elmaghraby & Losavio, 2014). At an individual level, motivated offenders, capable guardianship, and target attractiveness would likely increase the risk of cyberbullying victimization. The linkage of these elements improves the probability of crime; the nonappearance of a component diminishes it (Elmaghraby & Losavio, 2014). RAT can guide to data security and recommend potential vulnerabilities and suggestions for upgraded IT security.

Knowing how to reduce risk of victimization is important. By applying principles connected to RAT, IT professionals may be in a unique position to contribute to reducing the risk of victimization events (Choi et al., 2016). RAT is a useful beginning stage for exhibiting variables that increase adolescents' risk of accepting sexts. Wolfe, Marcum, Higgins, and Ricketts (2016) used multivariate regression models to test the congruity of RAT to document presentation. The multivariate regression models provided insight into the causal devices that may carry susceptibility to sexting amongst adolescents between the ages of 12 to 17 (Wolfe et al., 2016). Braga and Clarke (2014) proposed that social disorganization and RAT are similar and should be united. Peguero, Popp, and Koo (2015) asserted that RAT conceptualizes the elements related to criminal victimization. Peguero et al. (2015) employ RAT to investigate how race and ethnicity interface with circumstance and victimization. Peguero et al. (2015) findings revealed the relationship of RAT and operation differs crosswise over racial and ethnic minority groups.

The motivated offender class is distinguished by inspirations that range from benefit to extreme condition. Inspirations might be independent or in products grasp allurement, incitement, convenient time and fatigue (Elmaghraby & Losavio, 2014). The nearness of capable guardians alludes to regularly present people who have the capability to deflect offenses or direct recuperation by repair (Elmaghraby & Losavio, 2014). When capable guardians supervise suitable targets, motivated offenders are monitored by handlers, and managers oversee docile places, crime prevention is possible (Choi et al., 2016). RAT is used as a lens through which to view the observations of increasing guardianship and reducing target suitability of young people most at risk for victimization of cyberbullying (Choi et al., 2016). Victimization fits within the RAT components of reducing target eligibility by making potential aggressors aware that higher risk groups are connected to IT professionals who act as mentors within healthcare environment.

RAT is a theory of criminal events that can be applied to technology. RAT has grown to be commonly tested and supported theories in the discipline of victimology (Reyns, Henson, & Fisher, 2015). Its primary tenets include the possibilities for victimization when motivated offenders confront suitable targets in conditions needing capable guardians (Reyns, Henson, & Fisher, 2015). Without these three essential criteria, the theory contests that victimizations are significantly less likely to happen. Researchers suggest that RAT was established as a theory for multiple criminal activities (Leukfeldt & Yar, 2016). One such explanation of the various factors of crime is a combination of motivation, opportunity, and the absence of a capable guardian (Leukfeldt

& Yar, 2016). Montolio and Planells (2016) both agree that RAT concentrates more on the features of crime rather than on the offender.

RAT is also useful in developing explanations for cybercrime. Although RAT embodies various components, studies show only awareness to the routine online activities. Cohen and Felson (1979) confirmed that certain elements must be present for a crime to transpire: a motivated criminal with nefarious aims and the capacity to move on inclinations. By considering a small number of cybercrimes, results cannot be theorized (Leukfeldt & Yar, 2016). If victims are incompatible from non-victims, then any seeming correlation linking victimization and lifestyles would be deceptive. Bunch, Clay-Warner, and McMahon-Howard (2014) studied the effects of victimization on routine activities and asserted that they consider either victimized people adjust their routine activities following victimization or if there is a connection between victimization and high-risk activities. Victimization lifestyles are the result of underlying factors that lead to both the victimization and the lifestyles (Bunch et al., 2014). Vecchio (2013) stated that while the connection among offending and victimization is established, less is known about what contributes to the various effects of victimization on anticipated behavior. Victims historically garnered less scholastic inspection than offenders, emphasis on the victim population and their experiences is now commonplace.

It has been theorized that victims and offenders are often demographically, culturally, and behaviorally similar. As the individual risk of victimization increases with the amount of time potential victims spent around motivated offenders, some of the most at risk individuals are those involved in illicit drug use and street crimes (Vecchio, 2013).

Additional amplifying victimization risk amongst street offenders is a common disinclination or incapacity to report crimes (Vecchio, 2013). As per RAT, people's social conduct affects the potential for victimization. In a broad sense, the chances of becoming a victim of an attack are much more prominent on a night out than they would be if one spent the night home alone (Näsi, Oksanen, Keipi, & Räsänen, 2015). Victims of an attack can occur at any time.

RAT may be useful to create the impression that numerous parts of online victimization reinforce a comparable theoretical approach. From the RAT point of view, we could contend that both suitability for turning into an objective and the part of guardianship assume a prominent role both in the on the network and separated situations (Näsi et al., 2015). As noted above, broad urban areas provide openings and reasonable focuses to criminals. Living in a larger city may likewise relate to life decisions that improve the probability of victimization (Näsi et al., 2015). The absence of guardianship, specifically, is typical for those living in the major urban areas. The same may apply to some degree to the individuals who are less incorporated socially (Näsi et al., 2015). Victim assumption presumes that victims can completely interpret the criminal act and RAT is one of the best known, best studied, and most referred for victimization (Doerner & Lab, 2015). Victimization is referred to as being a victim.

According to RAT, opportunity structures affect the prevalence of deviant behavior. Offenders remained particularly interested in goals to which they assign a value for whatever reason and the succession of the appearance of a motivated offender and a suitable target, and the inadequacy of a capable guardian controls these structures

(Leukfeldt, 2014). Crime prevention will have to come from a different angle than target hardening alone (Leukfeldt, 2014). According to RAT, capable guardians also play a significant role.

Rival Theory/Lifestyle Exposure Theory

Lifestyles are patterned, repetitive or routine activities. Hindelang, Gottfredson, & Garofalo (1978) developed the lifestyle exposure theory (LET) in 1978. According to LET, research investigating the correlation connecting lifestyles and crime should avoid pooling or be grossing crime standards, because measuring the consequences of lifestyles on composite dimensions of crime leads to contradictory conclusions (Hindelang et al., 1978). LET is one of the first methodical theories of criminal victimization developed by Hindelang et al. (1978). LET was originally intended to account for discrepancies in the risks of violent victimization across social groups, but it has been lengthened to accommodate property crime, and it forms the basis for more elaborate theories of target selection processes. Since the 1950s, victimization theories generated practical, as well as anecdotal support, which most notably in the form of lifestyle-exposure (Hindelang et al., 1978). The basic premise underlying the LET is that demographic differences in the plausibility of victimization.

LET adjusts to the previous section concerning the relationship between statistic attributes and victimization risk. Hindelang et al. (1978) proposed the LET, which essentially concentrates on the victims' day by day social collaborations, instead of focusing on the attributes of individual guilty parties or different causal factors. Hindelang et al. (1978) found that people's professional and leisure exercises are

individually connected with crime victimization. LET qualities of lifestyles expose individuals to victimization risk (Reyns & Henson, 2015). LET is a representation of victimology that announces that the probability an individual will experience a victimization depends profoundly upon the concept of lifestyles such as high-risk places and high-risk times (Hindelang et al., 1978). Lifestyle concludes the reasonableness of personal victimization through the intermediary variables of presentation and relationships.

LET involves varieties in statistical attributes (e.g., age, sexual orientation). LET is a victimization theory that proposes people are likely to become victims of crime than others because of their way of life (Hindelang et al., 1978). Crowl and Battin (2016) use LET as a design to examine the multifaceted connection of lifestyle as it relates to crimes against an individual. Crowl and Battin's conclusions indicated that lifestyle choices could influence suspicion of a crime. Crowl and Battin's results also show that various individual elements and living arrangements arbitrarily are associated with personal fear of the offense.

LET and RAT surfaced as a significant predictor of victimization. LET and RATs emerged in the late 1970s as complete examples outlined to demonstrate inequalities in the risk of victimization (Vakhitova, Reynald, & Townsley, 2015). Researchers use LET and RAT to view victimization as the convergence of a motivated offender, a target, and the absence of guardianship (Pratt & Turanovic, 2015). A capable guardian can take on many forms and people play a significant role in a crime. LET provides a conceptualization of risk in probabilistic expressions; RAT only represents the

victimization event itself (Pratt & Turanovic, 2015). These theories differ towards how the functions of people are at “risk” for victimization.

RAT and LET recognized to be influenced by victimization. RAT and LET suggest that victimization rates contrast across a demographic audience since people in societies participate in various activities (Bunch et al., 2015). Routine activities intercede the connections between demographic qualities and victimization. Because of the core supposition carries both thoughts, several researchers have attempted to test its legitimacy, and the tests that do endure should depend primarily on cross sectional, non-comparable information (Bunch et al., 2015). The improvement of routine activities and lifestyle viewpoints have mainly aided in the investigation of the victim and offender overlap (Vecchio, 2013). Victims differ in their demographic if they have not been perpetrator profiled.

Rival Theory/Lifestyle Routine Activity Theory

Lifestyle routine activity theory (LRAT) provides a recommendation that routine activities may open some people and their property to more serious risks. LRAT occurs if certain practices elevate one’s odds of being victimized and one of the three key elements (i.e., motivated offender, an attractive target/victim, and the absence of capable guardianship) is missing (Pratt & Turanovic, 2015). Miethe and Meier (1990) presented a fundamental theory of victimization known as LRAT. With the determination of an incident, victims inside a socio-spatial setting controlled by the standard utility, focus less over RAT versus LET (Miethe & Meier, 1990). Tseloni and Pease (2014) claimed that lifestyle and routine activities are associated with personal victimization whether these

effects are solely individual or area. LRAT for example, single people encounter higher personal crimes than do other groups because of greater exposure.

LRAT recognizes that similarity to convinced guilty parties, presentation to unsafe conditions, target appealing quality, and the avoidance of proficient guardians are the key variables that decide the probability of criminal victimization. Generations of victimologists have integrated RAT and LET into a LRAT of criminal victimization that underlines the significance of lifestyles and routine activities in producing opportunities for victimization (Reyns & Henson, 2015).With the awareness of the social nature of a crime, RAT sets that the simultaneousness of the three components (i.e., motivated offenders, suitable and attractive targets, capable guardians) improves the probability of violent victimization (Cohen & Felson, 1979). The risk of victimization happens when criminals are in the vicinity to each other.

Criminology focuses on LRAT of crime. Cohen and Felson (1979) contend that crime as a planned phenomenon in the public arena is subject to three segments: a motivated offender, a suitable target, and a lack of capable guardianship. Joining these components improves the probability of criminal or impulse action and intensifies the likelihood of victimization. LRAT is presently the most compelling and fundamental criminological theory (Ilievski, 2016). The approach depends on two basic thoughts: that the offense happens when stimulated guilty parties are nearer to unprotected targets; and, on the act depends on the probability of an event influencing regular exercises, which incorporate administrations, family, relaxation and other everyday activities.

From a methodological perspective, the measure of hate crimes utilized as a part of exploitation studies does not on a very basic level vary from those of different types of crime either. Van Kesteren (2016) reported that because hate crimes are distinctive, there is no motivation behind why their circulation among target populaces could not represent comparable elements as other individual violations, such as lifestyle related geological or social closeness to potential guilty parties. A positive relationship between instructive achievement and violent crime victimization is not an unusual finding in victimological studies (Van Kesteren, 2016). There are four categories for victimology: (1) cyber trespass; (2) cyber deception theft; (3) cyber porn and obscenity; and (4) cyber violence. Cybercrime typology is considered one of the most comprehensive frameworks to recognize the establishment of technology into diverse classes of offending (Holt & Bossler, 2013b). Understanding the reasons for vulnerability and the risk of people through both a general theory of crime and ways of LRAT has a focal place in victimology (Pratt, Turanovic, Fox, & Wright, 2014). Low self-control might be an essential risk to victimization (Ilievski, 2016). Identified with inconsistencies in the way of life decisions, it is just single reason individuals become victims.

While research has recently started to examine the use of LRAT to cybercrime, current literature concentrates on victimization. Marcum, Higgins, and Ricketts (2014) noticed that impulses of cyber stalkers could fit into two classes: mechanical and social components. The two classes imply more noticeable information and abilities of the Internet, and additionally an abnormal state of the obscurity of a deviant cyber behavior.

The existing literature applies the calculated ideas with a specific end goal to test the relationship between routine activity, lifestyle, and malware crime. My study discussed risky offline lifestyles, computerized guardianship, and the avoidance of malware crime in cloud security. More prominent levels of introduction to guilty parties, target engaging quality, and lower levels of guardianship improved the chance of avoiding malware crime. My study demonstrated a relationship between demographic attributes, offending, and lifestyle differences.

Rival Theory/Technology Enabled Crime Theory

Understanding and controlling relatively complicated crime is initially difficult, and there is endless debate among the criminals and law enforcement for technological success. Sam C. McQuade developed the theory of technology enabled crime in in 1998 to include crime, policing, and the security enabled with technologies that make it possible (McQuade, 1998). As criminals do innovate, law enforcement must catch up to avert, control, deter, and prevent new forms of crime (McQuade, 1998). Technology crime waves signify as a way of recognizing how technology enabled innovative criminal behavior emerges, impacts society, and then diffuse. General conditions regarding a formal theory of technology enabled crime, policing, and security implies that the theories of technological complexity and technology crime fluctuations (McQuade, 1998). These concepts intend to correlate, but not supersede, existing theories of crime causality and technical improvement and dissemination.

The theory of technology enabled crime includes crime, policing and security enabled with technologies that make them possible. As criminals gain a technological

edge to commit a sophisticated crime, policing and security results in relatively complex and therefore irrepressible threats to society (McQuade, 1998). Intrigue criminals perpetually take the influence of new technologies often as the result of discovering how to do so from other criminals (McQuade, 1998). Crime does not need habitual offenders or convicted felons, but rather an opportunity.

The new crimes incorporated the course of pernicious programming and hacking that can bring about significant financial harm and the loss of accurate information and protected technology in healthcare. Holt and Bossler (2013a) analyzed some work on types of cybercrime, and the practices used to address the issue. Holt and Bossler found technology allowed help of new crimes that were not likely. Holt and Bossler investigated writing on different types of technology enabled crime (i.e., cybertrespass, cyber deception, cyber viciousness). Cybertrespass happens when an individual is attempting to hack into a computer system or information source without the authorization of the system proprietor, consequently damaging the limit of possession (Holt & Bossler, 2013a). Cyber viciousness incorporated the ways people can bring about a loss to an active or virtual environment (i.e., stalking, online harassment; Holt & Bossler). Cyber deception included the use of the Internet to secure data or illicitly acquire objects of worth from an individual or company.

Organized operations that make use of conventional technology enabled crime methodologies improved the use of networked computers for criminal purposes. Organized crime is not a new phenomenon (Raymond-Choo & Grabosky, 2013). The pursuance of financial gain has been a driving force behind the traditional organized

crime. In unique cases, criminal organizations may engage the services of former law enforcement officers with a degree of technological expertise (Raymond-Choo & Grabosky, 2013). Another category of the organized crime group consists of likeminded individuals who ordinarily know each other only online, but who are involved in an organizational structure working collectively toward a common goal since the Internet makes it considerably straightforward to adhere and plan activities (Raymond-Choo & Grabosky, 2013). The Internet has changed open doors for crime and abnormality, much as it has evolved differently how people socialize.

RAT and rival theories LET, LRAT, and technology enabled crime theory are used to establish conformity by including the suitability of targets and motivation prompting cybercrime. RAT is an extension of LET and a review of computer crime and victimization (Elmaghraby & Losavio, 2014). One of the fundamental ideas in the LET is a way of life factors, which is alluded to in RAT as their target suitability component. This way of life factors adds to potential computer crime victimization (Cohen & Felson, 1979). RAT provides an honest and thorough understanding of the reasons for crimes. At its root is the possibility that without great controls, guilty parties will go after appealing targets (Odumesi, 2014). To have a crime, a motivated offender must go to an equal place from an alluring target. Because that alluring target is never in the same situation from a propelling guilty party, the objective will not be taken, harmed, or struck (Glasser & Taneja, 2017). RAT was connected however with the acknowledgment that LET gives an entire clarification of the reasonable target fundamental found in RAT.

Usage of RAT

RAT applies to this study as in it gives immense comprehension to why individuals take part in cybercrime. The conceptual framework concludes that RAT is suitable for investigating and describing cyberattacks. RAT is empirically applied to various cyberattacks and records some of the methodological issues it requires. Technology enabled crime theory applies since it provides us knowledge and understanding of the new methods and procedures used by cyber criminals. Technology enabled crime theory additionally helps with awareness of new types of aberrance; social mishandle or multiple crimes through the imaginative use of innovation.

By adjusting Felson and Cohen's RAT, RAT is conceivable to make a profile of how to minimize EHR cyberattacks. RAT will be utilized to supports multi-level clarifications of crime (Johnson & Groff, 2014). RAT concentrate on offenses at the occasion level and consider the essential natural conditions for a crime to happen at a particular place and time. RAT conditions highlight the network between components that produce crime opportunity and at last crime occurrences (Johnson & Groff, 2014). Because we can figure what routine activities offer ascent to transnational crime, it is then conceivable to create crime counteractive action activities that remain to decrease crime on a worldwide scale.

As the use of data and correspondence advances increments and advances, technology enabled crime is probably going to proceed. Technology enabled crime as of now ranges over a wide variety of activities (McQuade, 2006). These incorporate crimes that include breaches of an individual or corporate protection, violations perpetrated by

people that intentionally adjust information inside businesses or government offices revenue driven, personal or political goals, and violations that include efforts to upset the operation of the network. Composed operations which make utilization of conventional technology enabled crime procedures will likewise increment as the usage of organized computers for criminal purposes creates (McQuade, 2006). There is no single comprehensive response to reacting to technology enabled crime (McQuade, 2006). Countering these risks is a multidimensional test and requires significant coordination and synergistic efforts on an extensive variety of government and private division substances.

As criminals contend with security and policing authorities for innovative preferred standpoint ceaselessly complex crime, policing and security brings about moderately confounding and, in this manner, unmanageable risks to society. New, versatile and standard violations rise after some time to make technology crime waves, the size of which can hypothetically be measured, looked at and anticipated (McQuade, 2006). Conceivable bearings for activity incorporate building up public-private sector participation and data sharing activities, setting up teams devoted to the investigation and indictment of technology enabled crime cases, improving the training and instructive abilities of police, prosecutors and IT experts (McQuade, 2006). Additionally, while there are some quantitative assessments of many computers influenced by specific infections or different malignant projects that course through the network, it is difficult to express this as many violations carried out by an individual guilty party, rather than a separate crime with numerous casualties.

There is a significant gap in information requiring the need for further studies. Criminological analysis of a compromised VM contributes significant information about the gaps in security (McCarthy, Herger, & Khan, 2014). Comprehensive evaluations of the theory are implicitly missing from the literature. With a few omissions, most studies have not operationalized all the core thoughts of the theory (Reyns, 2015). The time-based relationship of the system provides comprehensive insight into the matter of compliance (McCarthy et al., 2014). Malignant clients can store snapshots containing malicious code in open vaults negotiating with different clients or even the cloud system (Hashizume et al., 2013). If another client uses this image, the VM that this client performs will contaminate the covering malware. Also, inadvertent information spillage can be presented by VM replication (Hashizume et al., 2013). Snapshots preserve the configurations' current state. When analyzing snapshots, it is not required to leave the VM agent undisturbed (McCarthy et al., 2014). By leaving the snapshot undisturbed, create volumes can be created for the use of VMs.

The theory of RAT, and the rival theories of LET, LRAT, and technology enabled crime theory, was useful in breaking down the data research proposed in the present study. While there is research supporting the use of RAT, LET, LRAT and technology enabled crime theory to cybercrime, other research considering LRAT and cybercrime offensive, is inadequate. The researcher intends to analyze these components and ideally further the understanding and research of cloud security and malware infringement. Risky online and offline behavior and additionally social learning components that facilitate crime are relied upon to improve the probability of malware occurring.

Malware in Healthcare

There was a 26 % increase from 2013 to 2014 of new malware variants growing to 317,256,956 events. With the use of code obfuscation techniques, new malware variants continue production (Hellal & Romdhane, 2016). Malware is a set of codes or removal of software implemented to harm a network or individual systems. Malware can be referred to as viruses, worms, Trojan horses, logic bombs, spyware, and adware (Hellal & Romdhane, 2016). A lack of information security leads to most malware infections (Holt & Bossler, 2013b). Frequent updates can protect you from must issues.

Many organizational activities now rely on Web-based technologies. Individual online activities may put them virtually closer to infected records or attack devices. The most widely recognized security implements are the computer-based use of antivirus, antispyware, and adware programs intended to scan system files (Holt & Bossler, 2013b). Because there is proof of a relationship between conventional online practices and malware exploitation, there is a connection between unsafe online practices, cyber deviance, and the risk of infection (Holt & Bossler). Malware infringements are risks associated with the implementation of cloud security. There is risk associated with the implementation of cloud security and the potential risk of malware infringements (Tan, Chua, & Thing, 2015). Değerli, Aytekin, and Değerli (2015); Subramanian, Abdulrahman, and Zhou (2014) stated that individuals in healthcare have various levels of willingness to adopt innovations and products.

There is an absence of research on malware. By understanding the purposes of attacks will expand the defender's practice of the most proficient method to moderate

attacks (Maheux, 2014). Malware advance as new strands are created daily, yet, a portion of the standards have continued as before. The reason for this is that malware have changed from instructive, dissents, and abilities to benefit to hidden actions and harm (Maheux, 2014). The expectation is a piece of understanding malware; initially, antivirus organizations were searching for malware that had a financial benefit (Maheux, 2014). Because malware is additionally being used by governments and military, tracking down potential malware exercises was widened to other systems (Maheux, 2014). Understanding the goals of malware empowers organizations with assessing the adequacy of their malware defenses.

The developing predominance of malware provokes important economic loss to individuals and organizations. Malware detection has been one of the most common computer security problems of high interest (Hellal & Romdhane, 2016). Gomez (2015) stated that healthcare entities are unprepared for cyberattacks given the magnitude of the threat. Healthcare organizations do not know the extent of cyberattacks and facilities do not require healthcare providers to report adverse issues associated with.

Malware is a way that allows hackers to gain access to personal data through the Web. As malware breaches systems, hackers form a relationship outside of the system that holds the stolen data (Manworren, Letwat, & Daily, 2016). Hackers use software designed to go through internal firewalls and security before reaching the Internet. One of the most important hacking techniques is social engineering that allows someone to gain access to credentials or technical systems (Manworren et al., 2016.) Scrutinization of malware contaminations has not shown a reasonable relationship between different types

of computer guardianship and decreased chances of malware infection (Holt & Bossler, 2013b). Contamination of medical records due to malware can be reduced by moving medical records into the cloud.

My study contributed to the literature by exploring how RAT may apply to cloud security to protect against malware in healthcare. Scholars use a variety of structures when conferring literature reviews that frequently include a well-organized interpretation and organization of existing literature correlated to an appropriate topic (Callahan, 2014). When conducting literature reviews, researchers become accustomed to a problem, explain various theories and approaches authorities used in prior research on the topic, identify possible gaps within the existing body of literature, and reveal general hurdles and issues concerning the subject (Pickering & Byrne, 2014). This study explored to fill this gap by investigating the issue to minimize EHR cyberattacks.

Transition and Summary

The purpose of my proposed study was to explore the implementation of cloud security to minimize EHR cyberattacks. This section contained an introduction to the problem of the implementation of cloud security. The review of literature was to increase understanding of the background of cloud security, cloud security in healthcare, malware, risk, security, privacy, cloud platforms, and conceptual framework. The leading cloud platforms discussed are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

As the conceptual framework, RAT provided a viewpoint from which to explore the motivated offenders, suitable targets, and absence of guardians. RAT offered the

framework and provided an insight into the causes of cloud security crime which show that criminals prey on the weak and each of these frameworks provided a perspective on cloud security in healthcare and why some senior IT leaders in the healthcare industry lack strategies to implement cloud security to protect against malware.

Section 2 provided details and explanations on the research methodology selected for this study. This section expanded on the role of the researcher, sets the participant criteria, compares the research methods, and explores the population sampling, ethical research, data collection, analysis, reliability, and validity. Section 3 contains the results of the study based on a discussion of the data collected.

Section 2: The Project

In Section 2, I discuss the project and the reason for a qualitative case study. This section went into detail about the role of the researcher and the procedures for gaining access to participants. Then I provided with a description and justification of the research method and design. Next, the criterion for selecting participants and explanation for the population is discussed. I also provided justification for using the method and design, descriptions of instrumentation or data collection tools, and the consenting process for the research. I also present data analysis of the research questions and information regarding the reliability and validity of the study.

Purpose Statement

The purpose of this qualitative case study was to explore strategies senior IT leaders in the healthcare industry use to implement cloud security to minimize EHR cyberattacks. The population was senior IT leaders within a medical facility in Baltimore, Maryland who had strategies to implement cloud security to minimize EHR cyberattacks. The implication for positive social change was that the findings from this study reduced unauthorized exposure of health records to the public.

Role of the Researcher

My role in this qualitative study was to conduct the research, collect data, analyze the findings, and impartially present the results. Eyre, George, and Marshall (2015) stated that the researcher should welcome a participative and process-oriented assessment that concentrates on the most proficient method generates research proof for the targeted audience. Additionally, Eyre et al. stated that the planning of a project, data formation,

analysis and understanding of data, diffusion of findings is negotiated collaboratively with stakeholders. Therefore, I outlined the study to permit individuals to characterize and hand off his or her understandings of methodologies to complete cloud security protection to minimize EHR cyberattacks. I also identified subjects and implications that arose from the discourse. Additionally, I had an initial discussion to establish the expectations for both researcher and participant, which Davies and Coldridge (2015) stated can help create the value of the researcher as an active interpreter. Therefore, I reached out to senior IT leaders within the medical facility who has strategies to minimize EHR cyberattacks.

I worked in the medical business for over 12 years, during which EHR attacks were not an issue because the facilities were not exchanging electronic data from location to location. I assisted two hospitals with IT issues, which included implementing paperless solutions. Additionally, paperless methods in healthcare have improved data security, legibility, retrieval, sharing, and efficient data entry (Dudek, Papp, & Gofton, 2015). Finally, the transition allowed each department to quickly retrieve medical records without going to patient records which were my first practical application for cybersecurity.

The Belmont Report involves the ethical use of human subjects and focuses on the basic principles of respect for persons, beneficence, and justice during the study (United States Department of Health and Human Services, 1979). Additionally, Cugini (2015) stated that researchers need to comprehend ethical standards to handle the human subject appropriately. Furthermore, the ethical standards explained in the Belmont Report

and the organizational structures for research based on those standards have served society well by building up a stable structure for research failure (Califf & Sugarman, 2015). Therefore, I adhered to the principles outlined in the Belmont Report.

Once I selected the organization, I conducted a preliminary phone discussion with the human resources (HR) manager of IT of the medical facility that provided me a list of eligible participants. Additionally, I took into consideration the three basic ethical principles of respect for persons, beneficence, and justice emphasized in the Belmont Report which the US Department of Health and Human Services (1979) dictated the responsibility of explaining the potential risk. Therefore, the ethical standards and rules of the Belmont Report on the protection of human subjects were essential in this manner.

Recording and transcription of interviews were steps used to mitigate bias for this study. Baur et al. (2015) expressed that without full disclosure, distinguishing what personal stakes or inclinations reflected in research is hard and that advancements have demonstrated being straightforward alone are insufficient to mitigate bias. Additionally, Smith & Noble (2014) stated that researchers must update information to mitigate bias and view data from a personal lens. To reduce bias, I conducted my study within the medical facility that is separate from the industry of my current employment, which helped establish new thoughts and ideas. Furthermore, I was the primary data collection instrument. Ethics, integrity, and functional competence are essential for ensuring quality research (Baur et al., 2015). To relieve my predisposition, I stayed open to new insights within the research.

I implemented an interview protocol for member checking and data saturation to mitigate bias and viewed data through a personal lens. Fusch, Fusch, and Ness (2017) pointed out that complete removal of bias is impossible, but one should use interview protocol, member checking, and data saturation to mitigate bias with the use of one personal lens throughout the data collection method of the study. Additionally, the interview protocol controls the researcher precision in data saturation and to provide an arrangement of questions as well as assist the researcher through the meeting procedure (Castillo-Montoya, 2016). Furthermore, qualitative researchers use an interview protocol to guarantee consistency and dependability of the research (Fusch, and Ness, 2015). Therefore, I used the interview protocol to guarantee consistency with the participants and to remain on task.

Participants

The participants in the study were senior IT leaders located at a Baltimore, Maryland medical facility. An initial phone discussion was used with the HR manager of IT of the Baltimore medical facility to review the participants, the logistics, and the criteria for participants' view of how to minimize EHR cyberattacks. The eligibility criteria included participants being at least 18 years old as well as understanding the cloud infrastructure within their facility. Additionally, the participant also needed to have worked at their perspective facility for a minimum of two years and have comprehensive experience working with cloud security, which included having strategies used to secure patient records in the cloud. Furthermore, the participants' required knowledge and practical experience with tools used to provide security of EHR in the cloud. Maxwell

(2013) stated that research participants must qualify in the field of study have the capacity to produce the necessary data to explain the research questions. Additionally, Chughtai and Buckley (2013) stated that trust is progressively viewed as a critical determinant of individual and hierarchical viability. Therefore, participants had to meet the qualification criteria to be interviewed for this study.

The participants from this study aligned with the overarching research question by denoting strategies that senior IT leader in the healthcare industry uses to implement cloud security to minimize EHR cyberattacks. Additionally, the credibility of participants was determined during the interview process, which Joolaee, Amiri, Farahani, and Varaei (2015) stated that was necessary for meaningful research. Furthermore, participant's knowledge of the topic was used in the study, which Leedy and Ormrod (2013) noted that participants' capacity to answer the research questions is an essential part of the applicant's selection process. Finally, each research question was presented with clarity to avoid misconceptions from the participants, Leedy and Ormrod stressed that participants need to understand the research question before engaging in data delivery. Hence, the gatekeeper vetted the participants' through the process of elimination based on the demographic research questions.

Participants and researcher should establish a rapport, which I did by introducing myself and asking questions to develop a professional relationship with the participant. Additionally, Ruetzler, Taylor, Reynolds, Baker, and Killen (2012) stated that a researcher's attire could affect the impressions and final decisions of an interview.

Therefore, a working relationship was established through interacting and dressing in a professional manner.

Building a relationship with participants is fundamental for how participant perceived the researcher (Rizvi, 2016). Additionally, Elo et al. (2014) stated that having clear understanding remains vital for the researcher to engage participants and the participants' primary attribute so that the transferability of the outcomes to various settings can be studied. An introduction letter (see Appendix C) stating the purpose of the research was sent via email and personal stories were used to establish rapport with my participants.

The initial phase of a working partnership with the participants was to communicate with them. Yilmaz (2013) stated that the researcher should set the tone for the rest of the meeting. Additionally, individuals can clarify how they understand their general surroundings and their encounters through meetings with open-ended inquiries (Yilmaz, 2013). That is the reason qualitative research requires a thorough investigation of the issues in their participant’s general knowledge. Open-ended questions are used to compile data into codes, topics, classes, or necessary measurements (Lewis, 2015). Open-ended questions let the researcher comprehend and introduce the world as it is observed and experienced by the participants without foreordaining those stances (Yilmaz, 2013). I used pen-ended questions to obtain comprehensive, significant, and reasonable answers.

Participants were contacted via email with the help of the gatekeeper through email which was the HR manager of IT of the medical facility. The gatekeeper ensures the researcher access to the participants (McFadyen & Rankin, 2016; Peticca-Harris,

DeGama, & Elias, 2016). While gatekeepers may help with granting permission to contact potential participants, they do not necessarily guarantee that participant will cooperate with the researcher (McFadyen & Rankin, 2016). Additionally, any problems arising from interactions with participants may undermine gatekeepers' organizational standing or reputation (Peticca-Harris et al., 2016; McFadyen & Rankin, 2016). Therefore, the gatekeepers were communicated and I explained the purpose of my study and discuss the interview protocol (see Appendix D).

Research Method and Design

A qualitative research and a case study were the most appropriate approach as the focus of the study was to be exploring the implementation of cloud security against malware. Qualitative research frequently involves building up a great depth of comprehension (Boddy, 2016). Accordingly, a case study including many participants can be of significance and can create high quality knowledge (Boddy, 2016). Therefore, a case study design was appropriate to build point by point descriptions of the organization's cloud environment to arrange the information and identify with the implementation of cloud security against malware and protective strategies.

Research Method

Qualitative method was used rather than a quantitative method, as it empowered further investigation of the essential components of my research. Kahlke (2014) established that the qualitative method is less theory-driven, which Soltani, Ahmed, Liao, and Anosike (2014) expanded with the idea that qualitative methods help recognize a participant's ability to be centralized. Additionally, the study's topic is less theory-driven,

which makes the qualitative method more applicable than quantitative. Through a qualitative approach, researchers can pass on implications that rise out of the qualitative technique (Alshamaila, Papagiannidis, & Li, 2013). This approach helped me assemble the information expected to answer the research questions. The qualitative methodology requires a researcher to communicate their situations and expectations, and to analyze and uncover their presumptions and predispositions (Fassinger & Morrow, 2013). Effective communication builds and maintains relationships. Haegeman, Marinelli, Scapolo, Ricci, and Sokolov (2013) stated that qualitative deals with understanding the view and behavior whereas quantitative covers the social phenomena. As the researcher, understanding the perspective and demonstrated behavior allowed me to have control over the situation and was proactive and efficient. Qualitative research contributed relevant data for the implementation of cloud security.

A quantitative method was considered, but not chosen. Quantitative method is used to analyze studies, quantify a problem, and collects information on foreordained instruments that yield information, which focuses on empirical rather than contextual information (Purohit & Singh, 2013). However, strategies to minimize EHR cyberattacks were the focus, not quantifying patterns of attacks. Additionally, quantitative researchers can expand the thoroughness of qualitative reviews; this practice is steady with various philosophical standards (Frels & Onwuegbuzie, 2013). Furthermore, the quantitative researchers manage the thoroughness of data collection through numbers, which Thamhain (2014) stated that quantitative methodologies are recommended to support increased assessment. Despite the benefits of the quantitative method, quantitative

method for this study was not selected because data collection through empirical data was not applicable.

Mixed method research was considered since it is a combination of qualitative and quantitative methodologies. The mixed method approach includes collecting information to comprehend the best way to explore an issue from closed ended and open-ended approach (Purohit & Singh, 2013), which Green et al. (2014) felt included surveying and quantitative based requests. However, my study consisted of only the open-ended approach, which did not include the use of surveys. Additionally, mixed methods research has a fixed variable across studies and can render useful advantages when exploring complex research questions (McCusker, & Gunaydin, 2014). In comparison to using a single method, mixed methods research provided an excellent grasp of the subject under research and had a better scope. However, mixed methods are time consuming, and quantitative analysis was not required for the subject area, which is why mixed method was not used for this study.

Research Design

To adequately address the research questions, I chose a case study design as opposed to phenomenology or ethnography. Vohra (2014) indicated that the case study design was best used to deliver depictions of the authority phenomenon employing details to determine the information and to identify the records. Being in an exploratory role, the case study design contributed insight into my research. Additionally, Cronin (2014) stated that case study practices present a complete and precise display of a case, while Raeburn, Schmied, Hungerford, and Cleary (2015) added that case studies accommodate

the viewpoints of participants who may come from various backgrounds. Furthermore, case study was used to explore multiple facets of a phenomenon and to adequately address the research questions, which the design affords details not easily obtained by other designs.

A phenomenology design was a viable option for the study. Phenomenology lacks the level of flexibility of a case study (Hyett, Kenny, & Dickson-Swift, 2014), but Gill (2014) stated that phenomenologically design focuses on the human subject and allows a verbalization of the commonalities of individuals' occurrences within appropriate circumstances. Phenomenological research assumes the likelihood of placing their aims in a comprehensible location so that the phenomenology can verify experiences (Whittemore, 2014). However, commonalities of individuals' occurrences were not the focus, but the commonalities of the group were. Additionally, a flexible qualitative data collection method of a group was required rather than an explanation of an individual experience. Therefore, phenomenology design was not used which would deviate from the research question.

Ethnography was also considered but not used. Hudson and Hudson (2013) described ethnography as a qualitative design that permits an investigation of cultural phenomena which mirror the learning and arrangement of implications managing the life of a social gathering. Additionally, Cruz and Higginbottom (2013) described the examination of appropriate documents, participant investigation, and formal and informal interviews as data collection tools for ethnography, which Morse (2016) added that the ethnography aligns with the usage of a theoretical framework rather than conceptual.

However, my research plan did not require a theoretical framework, nor was I investigating the cultural phenomena relevant to the study. Additionally, there was no need to investigate the participants, but rather gain insight into the strategies used to counter cyberattacks on EHR. Therefore, ethnography was not chosen because an unknown issue was not being sought.

Population and Sampling

The population for my study was senior IT leaders from a medical facility in Baltimore, Maryland. Population attributes in a qualitative study relate to no indication of a deviation of a significant difference (Stern, Jordan & McArthur, 2014; Taylor, McNeill, Girling, Farley, Lindson-Hawley, & Aveyard, 2014). As described above, a gatekeeper was used to help coordinate efforts for me to interview the participants. Additionally, the purpose of selecting a population is to identify as much of information as possible with the least number of participants (Malterud, Siersma, & Guassora, 2016). Therefore, the populations for this qualitative case study based on the defined eligibility criteria were five senior IT leaders that include the senior vice president of IT services, deputy chief information systems officer (DCISO), chief research information officer (CRIO), chief systems architect (CSA), and the chief information security officer (CISO). Finally, each IT leader for the study had knowledge and experience implementing strategies to minimize EHR cyberattacks.

Census sampling design is used for accountability purposes (Tobin, Nugroho, & Lietz, 2016), which Simou and Koutsogeorgou (2014) added that the inclusion criteria should capture all participants of interest. Therefore, the inclusion criteria included the

individuals being in their current role at least two years and the willingness to participate, and the experience necessary to minimize EHR cyberattacks. Additionally, the exclusion criteria of the study included withdrawing from the study. Census sampling strategy was incorporated into the predetermined method of selecting participants and has 100% participation. Using census sampling establishes a sampling frame for conducting studies of many establishments (Charman, Petersen, Piper, Liedeman, & Legg, 2017). Census sampling is a method used to select the samples and all the eligible employees for a study (Hosseinabadi, Karampourian, Beiranvand, & Pournia, 2013; Omondi, Ombui, & Mungatu, 2013). Census sampling was used from within the population of the participants who are eligible to participate.

The interview took place with eligible participants, which included phone interviews with 45-minute timeslots and in-person interviews in a private conference for those who prefer in-person interviews. Additionally, the interview protocol (see Appendix D) was followed, which includes the same demographic and interview questions for all participants. Finally, all participants signed the consent form before the interview, which outlines that their personally identifiable information was not disclosed.

Member checking and triangulation was used to verify the accuracy and reliability which ensured the credibility of my study. Turner and Thompson (2014) stated that member checking involves returning and reviewing the results of the study with the participants. Additionally, member checking and data triangulation are used to ensure that the authenticity of data (James, 2017). Furthermore, Data saturation happens once the researcher cannot produce or when new information produces little or no changes

(Fusch & Ness, 2015; Malterud, Siersma, & Guassora, 2016; Tran, Porcher, Falissard, & Ravaud, 2016). Therefore, member checking was performed within a few days of the interviews and analyze the information to ensure data saturation was reached.

Ethical Research

The ethical considerations were observed by protecting participant's privacy and distributing the consent form. The consent is an ethical requirement describes the researcher's obligation to advise the participants of the risks of the study, benefit of the study, and their rights as a participant (Check, Wolf, Dame, & Beskow, 2014). Additionally, Dekking, Van der Graaf, and Van Delden (2014) and Kumar (2013) stated that the consent should be collected by an objective individual who also indicates the voluntary characteristics of participation. Finally, Dekking et al. (2014) also included that informed consent help enforces the protection of participant's rights. Therefore, the informed consent contained language to ensure confidentiality and protection, which was emailed to all potential participants before any data collection. Once the consent was signed, the participant agreed to the volunteer to the nature of the study and may opt-out at any time.

After receiving the signed informed consent, participants were given a copy, and a copy will be saved for five years with all other documents involving the research. Additionally, participants that indicated in-person delivered the informed consent by email or in-person, while all phone interview participants delivered by email. Hadidi, Lindquist, Treat-Jacobson, and Swanson (2013) stated that the right to withdraw is an essential ethical protection, which the researchers should inform the participants of this

right. A voluntary study was ensured by informing the participant of their right to withdraw in the informed consent as well as the beginning of the interview. Finally, participants were reminded that they could withdrawal with written or verbal notice without repercussion.

All recorded and hard copy data from this case study was stored on an encrypted hard drive, which was placed in a safe for five years to safeguard the rights of the participants. Additionally, the requirements for security in research depend on the situation and the setting (Deuter & Jaworski, 2016). Therefore, the name of the organization and participants are kept confidential with code words that only the researcher know which included keywords such as Participant #1 and Participant #2 that masked the identity of participants. Furthermore, IRB approval was obtained from Walden University's Center for Research Quality (approval number 10-26-17-0534748) before contacting or recruiting individual study participants, which was stressed in the NIH training course that was completed for using human subjects (see Appendix A). Finally, Brière, Proulx, Flores, and Laporte (2015) stated monetary incentives could lead to unethical behavior such as coercion, which good language knowledge facilitates communication in that context. Therefore, participants were informed that no monetary incentives would be provided for participation in this study.

Data Collection

In this section, how data was collected and applied during the study is discussed. Semistructured interviews with open-ended questions were the primary data collection methods (see Appendix E) which were used in the interview protocol (see Appendix D)

to collect data from the participants. Additionally, the interview protocol helped capture essential information such as the participant's background, demographics, an introduction to the study, the person’s position as it relates to the medical facility. Semistructured interview techniques were used to create an overall picture of how senior IT leaders in healthcare minimize EHR cyberattacks, which was triangulated with organizational documents obtained from the gatekeeper.

Data Collection Instruments

As the primary data collection instrument, semistructured interviews were conducted by using open-ended questions throughout my study. Bourke (2014) stated that the researcher is the primary data collection instrument due to the nature of qualitative research. Additionally, Rimando et al. (2015) stated that the data collection process could be influenced by the magnitude of the data collection instrument or by how long a participant will be interested in the development of providing data. Furthermore, strategies that encourage open-ended questions incorporate prolonged engagement and reflexivity (Cope, 2013), which Shannon and Hambacher (2014) added that reflexive journals increase the authenticity of data collection. Participation and reflexivity was increased by spending time with the participants in their environment as well as using a reflexive journal to record how decisions were implemented.

My goal was to ensure the participants of the active researcher. Grossoehme (2014) stated that qualitative research works with composed writings, various interpretations of individual meetings or center gathering discussions and tries to comprehend the significance of involvement in a study sample. Therefore, probing

questions was asked that allowed the participants to know if their response to their answers to the research question was understood. Additionally, Cope (2013) stated that prolonged engagement contributes to building trust and affinity with sources to cultivate productive, detailed reactions which provide scope because constant perception gives depth to the review. Frequent communication with the participants was maintained until the conclusion of the study to keep them engaged.

The principal instruments that were used were the semistructured interview and organizational documents which the gatekeeper provided the documents. A semistructured interview will enhance and reintegrate at the time of data collection between researcher and participant, (Mojtahed, Nunes, Martins, & Peng, 2014). To align with the interview protocol, all participants were asked the same questions during the semistructured interview. By following the interview protocol, the reliability of my semistructured interviews was increased.

Data Collection Technique

Once approved by Walden University's IRB (approval number 10-26-17-0534748), semistructured approach was used for an in person and phone interview. McIntosh and Morse (2015) stated an advantage of semistructured interview was that it provides a presence of the interviewer and gives structure to the interview situation. Additionally, telephone communication includes the benefit of enhanced accessibility, private auditory communication, and efficient use of time and labor, which the availability of participants through telephone conversation makes it beneficial over potential unavailable face-to-face interviewees. Therefore, I always made myself

available to the participants. However, McIntosh and Morse (2015) expressed disadvantages such as long-distance charges, participant's lack of access to a phone, or lack of telephone coverage. Therefore, collect calls was allowed during the data collection period.

To collect data from my participants, communication with the gatekeeper was sustained to get their availability, phone numbers, and email addresses. McRae et al. (2013) stated that gatekeepers help with the difficulties of securing informed consent, which the gatekeeper ensures that they adhere to the interests of the organization. While gatekeepers do not have the authority consent for participants, they may execute the decisions about participation, which means that gatekeepers must avoid any conflicts of interest (McRae et al., 2013). After obtaining the availability, phone numbers, and email addresses, each participant was contacted to schedule a time to either meet in person or over the telephone.

The interview protocol was used to remain on task. After obtaining the list of participant's email addresses, the participants were communicated with via email to review the informed consent. O'Malley, Gourevitch, Draper, Bond, and Tirodkar (2015) stated that the basis for the interview protocol is to explain the procedures and methods for conducting the research, which conducted the interview. After receiving signed consent forms, interviews were scheduled, which the participants were reminded that all interviews were audio recorded. Furthermore, a smartphone was used in airplane mode to record and restrict network activity to ensure the privacy of the participant then transferred the recording to an encrypted hard drive. Additionally, all recordings on the

smartphone were destroyed by deleting the information and then resetting the phone to the factory setting to ensure the privacy of the participants. Finally, all recordings were transcribed into a text document, which was stored on the encrypted hard drive.

After the interviews, member checking was performed to ensure the accuracy of the data collected, data saturation, and the correct interpretation of the data. Member checking is identified as a validation technique (Kornbluh, 2015; Morse & McEvoy, 2014), which Birt, Scott, Cavers, Campbell, and Walter (2016) added that member checking helps investigate whether results have resonance with the participants' knowledge. Additionally, member checking offers an opportunity to identify individual inclinations of the researchers by requesting elective perspectives on the translation of the information (Kornbluh, 2015). Therefore, member checking was used to guarantee the accuracy of the interviews by going over the information that was gathered with the participants after the interview. A second interview (phone) was scheduled with each participant lasting 20 minutes. The data collected from the recording was transcribed and read back to each participant. The transcription of data collected was a timely process because all sections were played back multiple times to ensure that no data was missing that was stated by the participants. After each paragraph, all participants stated that I could proceed to the next paragraph because all information was transcribed accurately.

Advantages of employing multiple data collection techniques are to use more data sources that contribute opportunities for validity and reliability of a study (Bowden & Williams, 2013). Additionally, Ryan (2013) stated that examining company documents can enhance the quality of interviews. Therefore, the gatekeeper was reached out to

obtain additional information that was helpful with identifying the organizational document that is beneficial to my study. Documents of interest included ledgers, policy manuals, training minutes, and any other documents related to my study about cyberattacks.

Data Organization Techniques

Data organization for my study included storing audio recordings, notes, and transcribed data on an encrypted hard drive, which was adequately labeled for efficient analysis. Additionally, each participant and data had a unique identifier (i.e., participant #1, P1; P1+; participant #2, P2; P2+, etc.), which the plus (+) sign to the participant identifier indicated that the participant provided additional information. Furthermore, Flannery and Gormley (2014) used data organization for organizing, indexing, sorting and retrieving qualitative data. As the researcher, all transcriptions were performed to ensure the privacy of the participants. While NVivo software is an easy to understand the program, the software cannot do most of the work for us (Castleberry, 2014). Therefore, data analysis and themes were recorded in NVivo.

While some automatic coding functions exist inside this program, the procedure had to monitor and analyze. NVivo provides an easy to use format to enable sorting, composition, and characterization of information until the researcher discovers the answer to the research question (Castleberry, 2014). Additionally, NVivo allows the researcher to collect, file, and break down various types of data, which includes Excel spreadsheets, Access database, Microsoft Word documents (.doc and .docx), portable document format (.pdf), rich text (.rtf), and plain text (.txt), most forms of audio, photos,

and video files (Castleberry, 2014). The versatility of NVivo allows me to organize the necessary documents for analysis.

Recorded information was stored on an encrypted hard drive in the safe for five years, which data destruction occurred by shredding hard copies and reformatting the hard drive followed by grinding it into scrap. Additionally, handwritten documents and company documents are stored in a safe and will be destroyed by shredding after five years. Protecting data is necessary to maintain the confidentiality and respect of the participants' privacy (Fabian, Ermakova, & Junghanns, 2015). Therefore, the identity of all participants and the facility was not disclosed to any party besides me.

Data Analysis Technique

Methodological triangulation was used to examine the data and find the answers to the research questions. Methodological triangulation provides avowal of various data collection technique that incorporates advantages and disadvantages (Houghton et al., 2013). Additionally, methodological triangulation is a type of triangulation which use at minimum two collection methods to analyze a comparable phenomenon (Heale & Forbes, 2013; Hussein, 2015; Houghton et al., 2013), and enhances credibility by accessing data from multiple sources and data validation. Therefore, semantical document clustering was used to identifying significant themes which include using interviews and document analysis to consolidate relevant data in support of approaching the conceptual framework and research question. Finally, my conceptual framework offered a basis for implicating different emphases of my coding scheme.

Another process for methodological triangulation was to ensure data saturation. Yin (2014) stated that methodological triangulation assists to achieve data saturation and validity of the study. After using methodological triangulation, data saturation was achieved that enriched my study by obtaining as much information as possible to ensure rigor. Considering whether there is sufficient saturation of data, data is not likely to change the finding (Lewin et al., 2015). Data saturation was achieved because new information continued to emanate because all eligible participants were interviewed. Furthermore, the researcher uses multiple strategies for information accumulation trying to pick a well declaimed, complete perspective on the phenomenon, which includes incorporating interviews, perceptions, and journaling from the research procedures (Cope, 2015). Therefore, methodological triangulation was used to analyze all the data from interviews, journals, and company documents.

My triangulation method included analyzing organizational and company documents, phone discussions with the gatekeeper, interviews that allowed me to be more personal with the participants and document analysis of research reports. Examining company documents can enhance the quality of interviews (Ryan, 2013). After the transcription of data collected, from the audio recording of the phone interviews or notes taking during the face to face interview, data was stored in a word document and all questions were in the "Heading 1" format. Zamawe (2015) indicated that NVivo offers the option to import audio recordings and partition them into audio excerpts. The thematic analyses were used and then discuss the implications of these finding.

Coding was based on the data analysis, research questions, and conceptual framework. The adoption of thematic analysis allows a better comprehension of the most impactful coding (Halverson, Graham, Spring, Drysdale, & Henrie, 2014). Thematic analysis is a classified under the qualitative descriptive design, which is a set of techniques that are transparent and systematic and used to analyze textual data and interpret a theme (Vaismoradi, Jones, Turunen, & Snelgrove, 2016). All data collected from a participant was shared amongst that participant and me, which the participants verified through member checking the accuracy of data gathered. After defining the codes, codes were based on words and phrase, which help establish the themes for the study. By using thematic analysis after coding, the issues which are essential themes were determined to become significant themes in data collection.

The computer-assisted analysis tool NVivo was used to provide evidence-based implications for qualitative research. NVivo is qualitative software analysis tools that draw outcomes based on similarities collected from the performance of the same dataset. NVivo enables the researcher to code the data and to create themes or categories (Sotiriadou, Brouwers, & Le, 2014). NVivo has an auto coding function that makes it exceedingly manageable while coding data. NVivo was used to auto code and verify the results with manually coding. Braun and Clarke (2014) used the thematic analysis techniques for coding qualitative data and then used that code to identify patterns across the data set about the research question. Thematic analysis techniques were used to identify patterns to code themes and subthemes.

Document clustering was used to gather the unsupervised records for compelling applications in content mining and data recovery. The performance of proficient document clustering is because of the term level, sentence level, and idea level procedures in the high dimensional document range (Nagaraj & Kalarani, 2016). The semantical document clustering algorithm uses the semantic weight of words to sort the themes in the reports. Then the similarity between the sentences is estimated by using a program which considers the weight and the similarity for efficient clustering (Nagaraj & Kalarani, 2016). NVivo was used as the document clustering tool.

Clustering is one of the common beneficial tasks in text mining. A constant challenge in the document clustering is to decide the number of document clusters (Timande, Chandak, & Kamble, 2014). If the number of clusters is parturient or an inadequate, it conclusively deprives clustering accuracy (Timande, Chandak, & Kamble, 2014). Once the clusters were added in NVivo, omission of pertinent data was verified.

Reliability and Validity

Researchers use reliability and validity to disclose the tone of a study. Tiira and Lohi (2014) stated that the reliability of the questions in a study could be assessed by continuously interviewing participants; there would be a possibility of hesitation. Leung (2015) pointed out that the nature of reliability extends in the consistency. Phrased differently, each participant was asked the same questions multiple times. Both criteria of reliability and validity are intended to make qualitative research trustworthy (Morse, 2015b). All participants were assured that they could trust me after interviews were over because no information from the previous participants was disclosed. Elo et al. (2014);

Houghton, Casey, Shaw, and Murphy (2013) indicated that there are four approaches to rigors in research of reliability (i.e., dependability, credibility, transferability, confirmability). Dependability, credibility, transferability, and confirmability all were addressed in my study. System reliability, availability, and integrity are the most important security points (Wang & Lu, 2013). Availability, integrity, and confidentiality are three abnormal state cybersecurity goals (Wang & Lu, 2013). All participants' confidentiality was respected and the integrity of my study was ensured.

Validity is defined as the length to what scores reached on an assessment instrument. The validity of obtained scores is essential for an evaluation of the study (Ali, Carr, & Ruit, 2016). The themes obtained from NVivo were used to come up with a scoring system. There are two types of validity (i.e., statistical conclusion validity and internal validity). Statistical conclusion validity alludes to a precision of deduction about the closeness and quality of the relationship between two factors (Richardson, Hudspeth Dalton, Shafer, & Patterson, 2016). Statistical conclusion validity inaccurately connects statistics, inconsistent treatment performance, and different variance of diversity into the experimental setting. Internal validity alludes to regardless of whether causation can induce the factual conclusions (Richardson et al., 2016). The credibility of my study related to validity. In any case, the key is not the selection of the concept, but how the ideas are presented about trustworthiness.

Dependability. The dependability related to RAT as there has to be a routine for the crime to take place. Dependability helps provide proof that conclusions of research could be repeated (Amankwaa, 2016). Member checking was used for the dependability

of the qualitative research. Member checking is a procedure that includes welcoming participants to audit the discoveries for precision and projected importance (Welch, Grossaint, Reid, & Walker, 2014). Member checking was used to affirm and revise data and to make sure that there is consistency with the experience of the participants. Member checking is to get confirmation of the data transcribed accurate (Harvey, 2015). Dependability refers to the establishment, to which data progress over time (Bengtsson, 2016). A reflexive journal is a method of achieving dependability (Houghton et al., 2013). A reflexive journal was used to track of coding decisions.

Credibility. Credibility of the study came as a result of the participant response. The credibility concentrated on the results of the participants. Credibility demonstrates the truth of the finding (Amankwaa, 2016). When triangulations are combined, it causes a more factual finding than the use of only one approach (Bjurulf, Vedung, & Larsson, 2013). The approach was member checking followed up with methodological triangulation at the conclusion of the interviews with the participants. Methodological triangulation is when you use multiple methods dealing with the same phenomenon to collect data (Carter et al., 2014). Member checking was used as a means of ascertaining credibility and used data triangulation during the interviews and collection of documents obtained from the organization. Throughout this study, company documents were collected to accompany the face-to-face interviews and phone interviews encompassing the phenomenon at the medical facility.

Transferability. Details of the study were documented to determine transferability. Transferability demonstrates that a finding is applicable in other contexts

(Amankwaa, 2016). Transferability was demonstrated through data collection. Transferability is critical to recognize because one of its primary roles is to bequeath attitudes that are used outside of the learning setting (Eller, Lev, and Feurer, 2014). Researchers can transfer the results from this study to their study. Researchers support the review's transferability with a rich, detailed description of the unprecedented situation, area, and individuals contemplated, and by being straightforward about analysis and dependability (Connelly, 2016). To delimit the transferability, details of the data that was provided by the participants was recorded and data collect was accurately document.

Confirmability. The use of sound note taking after the interviews from multiple participants ensured the confirmability of the findings. Auditability commonly referred to as confirmability is the orderly record keeping of every single methodological choice, for example, a record of the sources of information, sampling, decisions, and expository systems and their execution (Amankwaa, 2016; Cope, 2014; Tong & Dew, 2016). Reflexive journals were kept and stored with the all of the data collected. Confirmability ensures trustworthiness in qualitative research, and it explains that the results of a study shaped by the response of the participants and not the bias of the researcher (Amankwaa, 2016). Both research and data credibility is assessed, alongside the constancy and confirmability of the information and general findings (El Hussein, Jakubec, & Osuji, 2015). To establish confirmability, it was important to check and recheck the participants' responses to the interview questions that were being administered during the interviews to ensure that the interpretation of the meanings were correct.

Data saturation. Without reaching data saturation, the quality of the research content validity would have been in question. Data saturation happens once there is enough repetitive information, and nothing else can come out of the research (Fusch & Ness, 2015; Gentles, Charles, Ploeg, & McKibbon, 2015). For this is the reason, it was important to interview multiple participants. Data saturation was composed solidly with conviction and competence. The resulting theory is finished with complete portrayals for every idea, and with appropriate cases (Morse, 2015a). You should have high data and valuable information that is insufficient. Data saturation is initially encouraged by sampling (Morse). Since qualitative samples are limited, they should be sufficient and suitable (Morse). Data saturation is a state of enlightening repetition where excessive information accumulation contributes close to nothing or just the same old thing new to the research. Saturation has additionally been used as a guide that adequate information collection has been accomplished (Gentles et al., 2015). Data was collected until all information became repetitive indicating that data saturation was achieved. Data saturation was achieved by using census sampling to accumulate data from everyone in the study.

Transition and Summary

In section two, prospective of the study was further discussed. The purpose of the study was reemphasized, and the role of the researcher and participant was addressed. The primary research collection instrument and how the ethical guidelines to conduct the study were discussed. Census sampling was used to select participants to achieve data saturation. Additionally, the methods, research design, population, and sampling were

pointed out. Then, the ethical responsibility that is required by the IRB was discussed. Next, the data collection and data analysis technique was talked about. Collection of data from phone interviews and face to face interviews along with organizational documents were pointed out. My data was organized and analyzed in NVivo. Methodological triangulation was used to ensure saturation. Finally, in this section, methods to ensure the reliability and validity were included. Validity and reliability was addressed in the study through member checking. Section three will cover the overview of the study and then go into the findings.

Section 3: Application to Professional Practice and Implications for Change

This section contains information from the qualitative study, including a presentation of the findings and how they can be applied to professional practice. Next, I discuss information from my study that might provide social change and make recommendations for immediate action. Finally, I provide recommendations for further study as well as personal reflections related to the study.

Overview of Study

The purpose of this qualitative case study was to explore strategies senior IT leaders in the healthcare industry use to implement cloud security to minimize EHR cyberattacks. The data for this research study came from conducting semistructured, phone interviews, and analyzing organizational documents. In this section, I begin with a brief overview of why and how this study addressed effective information technology practice, review of the questions or issues, and provided a summary of the findings.

Presentation of the Findings

The overarching research question for my study was: What strategies do senior IT leaders in the healthcare industry use to implement cloud security to minimize EHR cyberattacks? In this section, I present the findings and five major themes that I identified after conducting the study. The population for this study was senior IT leaders from a medical facility located in Baltimore, Maryland. I conducted two semistructured, face-to-face interviews and three phone interviews, which were member checked to ensure accurate transcription and to enhance the methodical triangulation process. Methodological triangulation was used to analyze the two sources of data which were

semistructured interviews and organizational document analysis. Five major themes emerged from the study: (a) requirement of coordination with the EHR vendor and the private cloud vendor, (b) protection of the organization, (c) requirements based on government and organizational regulations, (d) access management, (e) continuous improvement. These five major themes provided potential strategies that could be used for implementing cloud security to minimize EHR cyberattacks.

In line with these themes, I found that a primary strategy used by the organization is to have a private cloud to support the EHR, which services multiple healthcare organizations owned by the main organization while analyzing and developing processes and policies to enter the commercial cloud arena for archive storage. Understanding this strategy includes learning more about the policies, agreements with vendors, and tools used as they migrate the EHR storage to the cloud, and then use this information to develop a business case to move the EHR to a commercial cloud. Additionally, the organization is developing a precision medicine archive of the EHR data to assist analysis research and outcomes understanding. The analytical environment in a commercial cloud environment uses this ported data.

Theme 1: Requirement of Coordination with the EHR Vendor and the Private Cloud Vendor

One emergent theme from the data collected was the protection of the infrastructure through coordination with the EHR vendor and the private cloud vendor and their own cybersecurity team. The organization uses a vendor solution for its EHR. Participant #3 stated that one would refer them as an EMR customer who is public

knowledge. The EHR is an application that runs on top the infrastructure of the cloud provider for network access, hardware, operating system a cloud services. The EMR is a suite of Windows and UNIX servers in the organization's data center. Participant #1 stated that the organization implements their EHR using their hardware in a private cloud. Participant #4 shared that the architecture of the EHR is dependent upon that the EHR vendor's design. The EHR is a patient-centric model that runs in a private cloud.

All cases related to security and system functionality are negotiated with a very rigorous contract with the vendor, and both have worked with the organization in important ways to provide them with some protections for their EHR. Participant #4 also stated that the organization works with the vendor closely to ensure that they are uses best practices in all areas. The organizational document Vendor Terms and Conditions, states that the vendor shall defend, guarantee and hold harmless the organization, employees, and agents, against all losses, liabilities, judgments, awards, and costs arising out of or related to any claim that the organization use or possession of the products. Also in the organizational document Vendor Terms and Conditions, it is stated that no settlement that prevents the organization from continuing to use the products will be made without the organization prior written consent. At its own expense, the organization shall have the right to participate in defense of any suit or proceeding through counsel of its choosing. If recall or modification of any of the products is required or voluntarily recommended, the vendor shall immediately notify the organization in writing of such recall at no additional charge to the organization and replace such products. The

statement found in the organization document gives the organization the option the back out of the vendor agreement.

Participant #2 stated that his organization has a security team focused on just the EHR and they ensure that the staff is trained with a thoughtful orientation with the understanding that they are responsible for the protection of the data. Participant #4 stated that within the security team are 46 employees with cybersecurity as a part of their responsibility, but not all of them are full-time cybersecurity experts. Many are embedded in other teams with some cybersecurity expertise that is focused on a specialty of which they are conducting their work.

Participant #1 stated that most senior IT leaders perceive that the level of cloud security provided by critical cloud providers are a gauge, to the point that most organizations are not able to make security decisions that are superior to what the business cloud organizations have given. Participant #1 established and implemented the information security strategies and directives consistent with the vision of the organization. Participant #4 stated that the organization spent about a year investigating cloud security and privacy regulations before implementing the private cloud and the organization has a team that is focused on security including cloud security.

As noted in the literature and stated by Kirubakaramoorthi, Arivazhagan, and Helen (2015), a private cloud is run entirely by a third-party vendor. Private clouds are secure, very safe, and aim to clear many of the questions regarding cloud security (Kirubakaramoorthi et al.. In the organizational document Rollout, Why EMR, The Pathology Blog, and Faculty Senate, the organization's EMR presents an enormous

opportunity to streamline and systematize care, which includes replacing clinical and financial computer systems through the state While the rollout of EMR has taken several years, the system will permit for organizational growth by allowing providers access from any location and device. Additionally, the EMR will consolidate inpatient, outpatient, emergency department, and other patient data within a single system. The organization created a comprehensive record for every patient, viewable by as many members of that patient's care team as possible.

In the organizational document A Comprehensive Report, vendors are contacted to provide information on technologies and assessments. The security technology usually focused on concerns such as redundant and unnecessary purchases and the effect of technology in generating fear for lack of training on the use and assessment of the technology. Because the private cloud-based systems can be manipulated electronically through system software and antivirus, other defense measures should be in place or provided by the vendor to avoid victimization.

The private cloud encompasses the migration of private hardware infrastructure usually located in a data center. Some common reasons for developing private cloud includes being cost-efficient, flexible, data safe, integration into the organization's environment, and backup control to name a few (Davidovic, Ilijevic, Luk, & Pogarcic, 2015). If an organization prefers a private cloud, it is necessary to invest substantial assets in the construction of needed infrastructure. With the private cloud, this can be the case as long as the organization has available computer resources provided to users on request (Davidovic et al., 2015). The service provider can optimize the resources

accessible from organization to organization, considering the interest that occurs at that instant (Lian, 2017). Prior studies indicated that the distinction of trust among organizations and service providers are most significant for thriving partnership (Rohrmann & Cunha, 2015). Trust has been integrated into the cloud computing success and the validity in the context of the private cloud computing in healthcare. By combining private cloud computing in healthcare, trust can improve the perception of the success of cloud computing (Rohrmann & Cunha, 2015).

LET and LRAT aligned with the theme coordination with the EHR vendor and the private cloud vendor because both correlate to victimization. LRAT occurs if responsible practices promote one's odds of being victimized and one of the three principal elements (Pratt & Turanovic, 2015). LRAT recognizes the key variables that decide the likelihood of criminal victimization (Reyns & Henson, 2015). While research explores the use of LRAT to cybercrime, current literature concentrates on victimization. The existing literature applies the ideas with a specific end goal to test the relationship between routine activity, lifestyle, and malware crime. LET and RAT both view victimization through the lens of the motivating an offender, targets that are attractive and the absence of capable guardianship (Pratt & Turanovic, 2015). These theories differ, nonetheless, in how they see the behaviors that put individuals at risk for victimization. Where LET understands the danger in probabilistic terms, RAT describes merely the victimization event itself (Pratt & Turanovic, 2015). The difference is significant and that its dissolution over time is considered for the study of vendor victimization.

Table 1

First Major Theme

Source of data collection	*D*
Participants	4
Organizational Documents	2

Note. Theme 1, coordination with the EHR vendor and the private cloud vendor; *d*= data collected from.

Theme 2: Protection of the Organization

The second theme emergent was the need to utilize security tools, employing regular patch management, and implementing encryption. Participant #4 also stated that while the organization maintains the security of the EHR with 60 to 70 categories of tools. I found similar recognition of some of the tools in the organizational documents. Some tools are mentioned in the organizational document Right Tool were considered excellent. However, because of security concerns, the organization discourages the use of them. The organization uses several recommended internal tools with private cloud-based file sharing in a secure environment with real-time collaboration.

According to Participant #4, the protection of the infrastructure includes auditing, logging and patch management. Participant #4 stated that each server requires patches at the OS level. The EHR must be patched for both security and functionality. Third party software is patched. Patches are conducted with an approved timeframe after they are identified. The common secure barrier of isolation disconnection from the network where

it is not necessary or needed attack detection compromised the security team deploys detection, and that is to protect the hardware on which the EHR is mounted. Participant #4 identified the need to protect the infrastructure from phishing and malware. The organizational document Know Cybersecurity reviewed the effects and processes to address malware instances.

The organizational document Medical Record System indicated that the private cloud option requires crypto. Crypto promotes the encryption and decryption of data storage (Kiruthika & Laxmi Sree, 2014). The participants and organizational document Self Protection states that the cloud-based EHRs are encrypted typically at the transport level. Since patient data is governed by the privacy regulations regardless of storage method, the participants noted that cloud-based EHR encryption is less expensive than on-premise, while organizational document Self Protection states that decryption is more expensive but includes the benefits of secure implementation and remote accessibility. All five participants share that the organization’s EHR is on premise and their hot backup is via a third party commercial organization although the organization owns and manages the hardware. Therefore, when a patient's EHR needs to be obtained from the private cloud by a healthcare professional, Participant #2 stated that the decryption process must be approved by the hospital, and then the files can be decrypted and accessed.

Participant #4 stated in the organizational document Medical Record System, breaches attracts expensive lawsuits which cause the information security department to be on alert. They developed a set of networking and system support tools that have a centralized IT service. The traffic on the VPN in the private cloud is fully encrypted. All

access to the cloud has been integrated with the active directory system. In the literature, vulnerabilities in a system may be revealed through an agent using analytics and by understanding patterns and trends within the data (Jouini et al., 2014). Standard encryption methods today provide insufficient circumstances or none at all to operate on encrypted data without decrypting it first. But encryption restricts the likelihood of outsourcing on the externally stored information (Bos, Lauter, & Naehrig, 2014).

According to Participant #3, the amount of time that the data is in the clear is relatively short. It is only when the organization is doing analytic views in the cloud of that environment where data is dynamically decrypted. Encryption presents a tool for ensuring the privacy of medical data. It restricts the functionality for performing on such data. Encryption that is used today provides insufficient chance to function on encrypted data without decrypting it first (Bos et al., 2014). The data is partitioned so that even if a partition is compromised, it is isolated or insulated. They can only penetrate so far into a data environment before they hit a firewall on another layer of decryption strategy.

Online performance is a way of recognizing malicious activity, indicating through the RAT propositions of the ubiquity of a target and absence of protection (Pyrooz, Decker, & Moule, 2015). With all of the participant responses, it was evident that each senior IT leader understood that the organization remained a target of a potential cyberattack. Through testing, each senior IT leader declared that there was no absence of protection within the organization. Jackson (2015) stated that vulnerability is not an issue of exploitation, but a motivated offender. This position takes the burden off the victim

and places it on the shoulders of the offender. However, few definitions place constraints on an offender situation presumably to encompass as many offender types as imaginable.

RAT aligns with patch management and testing because if you eliminate patch management, you become a suitable target. The RAT attempts to define the minimum qualifications essential for a crime to occur and to focus attention on elements of crime self-governing of the offender. Whereas the RAT produces characteristics of the situations, targets, or victims of crime, it only regards that the offender must be motivated to seize the opportunity.

RAT and LRAT aligned with the theme protection of the infrastructure because both correlates to victimization. While the RAT accounts for criminality when possible offenders and victims are contemporaneously within the same environment without the presence of a capable guardian, it does not satisfactorily address victimization and offending that take place in non-physical areas (Choi & Lee, 2017). This is because the theory assesses the physical confluence of space and time between the victim and offender. Another aspect of LRAT is that it is mostly used to assess real crimes that can be implemented online for which individuals can end up in places where they become suitable targets for victimization (Choi & Lee, 2017). As related to RAT, the senior IT leaders of the organization are depicted as targets while implementing cybersecurity strategies with the understanding that they remained targets while protecting their EHR system from data breaches.

Protection of the environment aligned with the tenets of the RAT. Participant #4 stated that the organization investigated 20 to 30 security-related incidents daily, while

the firewall blocks the millions of security-related incidents. RAT includes visibility, accessibility, and guardianship. RAT approach to crime is dependent on the ability to surround offenders and targets, in the absence of a capable guardian (Leukfeldt & Yar, 2016). Participant #2 stated that the organization uses a private cloud and the organization has a security team who focus on the elimination of potential threats such as cyberattacks and hacking of sensitive information. Further, they are looking for a viable solution that eliminates these potential threats. RAT accounts for criminality when possible offenders and victims come together within the same environment without the presence of a capable guardian, and it does not sufficiently address victimization that takes place in other locales. This is because the theory values the physical convergence of space and time between the victim and offender (Choi & Lee, 2017).

According to the RAT approach to crime, the absence of guardianship from the implementation of EHR cybersecurity can result in increased cyberattacks. RAT can map to information security and recommend vulnerabilities and resolutions for IT security (Elmaghraby & Losavio, 2014). Senior IT leader should consider private cloud to implement cloud security to minimize EHR cyberattacks because it compensates for the shortcomings of the RAT. Senior IT leader might head off cybersecurity attacks by focusing on criminal motivation. Cohen and Felson (1979) stated that RAT is primarily a theory of victimization focusing individually on those who are suitable targets for motivated offenders. However, the RAT in the protection of the infrastructure attempts to specify the insignificant conditions necessary for a crime to occur and to focus attention on factors of crime autonomous of the offender. Whereas RAT provides components of

the situations, targets, or victims of crime, and notes that the offender must be motivated to seize the opportunity.

Suitable targets are viewable as those who require the protection to prevent an attack. LET was the secondary rival theory used for this study which aligned with the theme patch management and testing. Based on the LET, research shows that the position of a victim should be conveyed into attention when victimization is studied, as the victim's behavior may improve the possibilities of becoming victimized (Kokkinos & Saripanidis, 2017).

The literature contributed insight to cyberattacks in healthcare and aligned with the data from my interviews and organizational documents. Healthcare is a prime target for the cyberattacker as it impacts the unprecedented. IT has an enormous impact on the social well-being and national security (Kruse, Frederick, Jacobson, & Monticone, 2017). Cybersecurity has become an integral part of any organization, and the mass usage of networked systems has given rise to critical threats vulnerabilities which have a significant social impact (Kruse et al., 2017).

Table 2

Second Major Theme

Source of data collection	*D*
Participants	3
Organizational Documents	4

Note. Theme 2, protection of the organization; *d*= data collected from.

Theme 3: Requirements Based on Government and Organizational Regulations

The third theme to emerge from data was attention paid to requirements centered on government and organizational regulations based on the HIPAA, and the Health Information Technology for Economic and Clinical Health (HITECH) and the organizational policies that govern research and data proposed by the Institutional Review Board (IRB) of the organization. HIPAA governs the privacy of health records following the Privacy Rule (Hedden, Jessop, & Field, 2014). HIPAA governs how Covered Entities (CEs) protect and secure PHI (ONC, 2016). The organization's document noted that for that describes the circumstances in which CEs are permitted, but not required, to use and disclose PHI for specific exercises without first securing an individual's authorization. The literature talks about removing PHI and, for example, Liu, Musen, and Chou (2015) said that if there are 500 or more individuals involved in a data breach, a report must include the state of the entity breached, the name, the type of record, number of records affected, and if any external vendors are involved using PHI. To ensure the wellbeing of patients, strategies to mitigate the risk and effect of potential data breaches are essential for healthcare systems and clinicians.

Compliance and breach management are two major requirements of HIPAA. Compliance centers on maintaining privacy and confidentiality. Breach management provides policies and procedures, sample forms, workflow diagrams and a breach risk assessment to assist with the ascertainment and necessary steps to stay in compliance with federal law (Downing, 2014). Participant #1 identified that the CISO and the legal HIPPA office with the assistance of outside experts must perform computer forensics and

other postmortem tasks to understand the cause of the breach and confirm the eradication of the breach.

Studies have shown that lack of access to shared data is one of the leading causes of breaches in the healthcare (Castiglione et al., 2015). In the initial phase of a breach, Participant #1 assesses the extent and severity of the violation, and if it is a severe data security breach, proactive notification is the right strategy. Next, they would identify who and what has been affected and addressed the immediate threat. If it is as simple as needing to reset passwords, then immediately force a password reset. After containing the breach and business operations restored, the challenging work and communications get initiated.

Healthcare organizations must comply with HIPAA privacy rules that are introduced through federal regulations (Kaushal & Khan, 2014). HIPAA addresses both the privacy and security guidelines of PHI, as they complement each other to perform the designated obligations (Pussewalage & Oleshchuk, 2016). Health records data needs to be centrally accessible while supporting privacy guidelines. To protect sensitive data, it is imperative to know where it is located. The organizational document Privacy and Security, the HIPAA Rules present federal protections for patient health information, and HIPAA addresses the patients' rights concerning their health information.

Organization document: Cloud Exceeded HIPAA, states that cloud providers that operate in the healthcare world is required by federal HIPAA legislation to manage healthcare data securely and confidentially. Sharing of health information proposes privacy and security issues that conflict with HIPAA standards (Thilakanathan et al.,

2014). At the organization in my study, there were teams of data retrieval experts all of whom have completed HIPAA training. All participants agreed that adequate cybersecurity training is necessary for minimizing cyberattacks in a cloud-based EHR-HIPAA. Participants #2, #3, and #5 stated that formal HIPAA continuing training units (CTU) are an annual requirement while participant #1 and 4 mentioned that their training was informal. Continuous education is a process which takes place during the everyday professional work in the field of health services (Yfanti, & Sipitanou, 2016). Fundamental prerequisites to fulfill educational needs to improve the existed knowledge and improve the quality of service in healthcare, reduce work stress, improve critical thinking, self-confidence, and initiative, eliminate work mistakes, accomplish better working condition and certify that there are skilled and satisfied (Yfanti, & Sipitanou, 2016). Continuous training education should take place whenever there are new advances. CTU is a prerequisite to improve and ensure the quality of healthcare services (Yfanti, & Sipitanou, 2016).

The participants believe that HIPAA CTU training enhanced the continuity and information security management within organizations. The organization's training programs are rigorous. They make sure every person gets trained annually on privacy and security, and their access is taken away if they do not complete the training. By implementing training programs, organizational leaders can solve technological challenges found within some organizations (Sindhuja, 2014). Leaders of an organization understand the importance of implementing adequate information security controls within

critical systems, but some leaders neglected to ascertain security training and awareness programs within their organizations (Ismail, Sitnikova, & Slay, 2014).

There are those who have cloud security training, but the training limits their ability to store the EHR in the cloud. While the organization partners cloud computing service provider (CCSP) for hardware and software handling, the participants stated that the CCSP should provide cloud awareness programs about threats and security controls. With cloud computing, the participating organization can save patient data on a cloud-based server instead of a local tape or a hard disk. The organization uses a local cloud for the EMR. One of the most significant benefits of the organization's current cloud is that it enables the organization to access other organizational data.

Information found in an organizational document Newsletter states that the organization use an online training source for their cloud-based file sharing and file storage service which enables staff to collaborate and share information and can be accessed through any device (i.e., desktop, laptop, phone, or tablet). The program makes it easy to upload content, organize files, share links to data, and manage file and folder permissions. With the program, the staff can collaborate with colleagues both inside and outside the organization anytime, anywhere, from any device. The cost of the program and the online training is free. Each user is trained on how to login to the file sharing through a web GUI.

Furthermore, since the HITECH Act ordered new requirements on healthcare organizations regarding meaningful use criteria, which encourage reimbursements from the US government for patient care (Kruse, Bolton, & Freriks, 2015). As part of the

HITECH Act included additions to HIPAA reviewing the protection of human participants in research is the role of the IRB (DeMeo, Nagler, & Heflin, 2016). In the organizational document IRB Human Subjects, an individual retrospective case report is a project expected to develop data to be shared for educational and medical goals. The organization's policy states that a single case report is a retrospective analysis of one, two, or three clinical proceedings but is not research that must be approved by the IRB. “(If more than three cases are involved in the analytical activity, the activity will constitute research)". Although IRB approval is not obliged, specific HIPAA Privacy Rule obligations apply to the use and acknowledgment of PHI for a single case report. Researchers who dismiss HIPAA identifiers from the case report data before disclosure of the data are not required to obtain a signed privacy authorization from the case report. No illustrations or photos in the case report should lead to the identification of the patient. Researchers are not required to submit an authorization form to the IRB for review.

In the organizational document, Participant #2 identified that operational responsibilities are to ensure that research access to clinical data adheres to federal and state requirements that we follow the institutional review board (IRB) policies and expectations and approvals. For example, if an IRB asserts that an investigator can only identify data, then the data team responsible for delivering only the identified data to that investigator. There is a large team in the organization that facilitates this process. There are teams of security staffers helping and assisting; there are teams of people generating safe analytic environments, secure analytic framework environments (SAFE) to allow

investigators to examine their data in an environment where they're not likely to be compromised with very strong security perimeters of encryption of data at rest.

The organization document: IRB Compliance Training, the HITECH Act requires that any breach of HIPAA confidentiality is to be reported. It is essential that researchers understand and comply with HIPAA regulations as they pertain to research. Under the HIPAA Privacy Rule, you must meet specific requirements before using or disclosing individually identifiable health information for research.

The IRB has a relationship with the data trust for identifying and improving the data that a researcher may obtain from the job. There are requirements set for that researcher as to where and how he may house that data and constraints on subsequent sharing. That is all primarily done by policy and education of the users. However, the training course assumes you have a basic understanding of the HIPAA requirements. If you are required to complete the course, you must first complete the required, relevant basic privacy course on the organization's Intranet site. Taking the HIPAA training courses online requires you to have at minimum Adobe Flash 8+ installed on your machine with the POP-UP blockers turned off, including both your browser and any toolbar you may have running.

RAT is a theory which imposes a situation to analyze the experiences and information (Cohen & Felson, 1979). When measuring the different responses obtained from all participants, a notable distinction of similarity amongst the respondents became self-evident. Similar responses emerged about behavior and attitudes that indicated the daily activities and interactions about HIPAA training. Furthermore, when asked about

daily activities and if training was mandatory, participants wittingly stated that they came into a significant amount of contact with individuals that can be identified as delinquent with the training. The emerging trends in responses contributed a genuine belief of the meaning of lifestyle options that placed these individuals in positions for opportunities for exposure in activities that increased their probabilities of both victimization and offending.

The research findings of breach incidents about the theft of patient information are also are contradictory to the issues reported in the study of Cascardo (2015) who remarked that a notable number of HIPAA data breach violations correlate to employee theft. RAT aligns with HIPAA breach management without key personnel and senior managers; you will have a lack of a guardian. Where the breach has occurred as a result of a missing element, the senior IT leader, and possibly the authority should also be involved. HIPAA data breach violations relate to employee theft or unintentional loss. Knowledge regarding data breaches uncovered during this study may add to the broader field of breach management and information security research.

RAT is worthwhile in explaining the participation of the IRB and other aberrant behaviors when considering obtaining approval to research healthcare. Though RAT discounts ethical and social determinants, RAT provides a level picture of deviance that is useful in deconstructing the timeliness assumption connected with a crime. The theory concentrates on the offender’s behavior, the decisions that lead one to commit a crime at a time, and specific crime events. RAT operates on the suspicion that anyone that has the opportunity can delimit a crime.

Table 3

Third Major Theme

Source of data collection	*d*
Participants	5
Organizational Documents	4

Note. Theme 3, requirements based on government regulations *d*= data collected from.

Theme 4: Access Management

A fourth theme that emerged is access management. Access management includes the tools to captivate and record user information such as the user's identity and manage the removal of access privileges (Lloyd, 2015). Participant #4 identified that there is a team to ensure that access is granted based on a role that a person has. A person is only able to see the parts of the EHR that are important for their specific areas of responsibility. Participant #3 stated that an issue with a cloud presence is the challenge of configuring hundreds of user roles, which defines the read, write, and execute access on the data for each member of the organization. Additionally, the EHR has an intense application level security. The organization’s EHR uses multi-factor authentication, which requires a password as well as a physical device such as mobile device. Participant #2 uses Google authenticator, which allows secure access to EHR by acting as a token that is dynamically changing and guarded with a security policy. The ability to get this on a cell phone is restrictive with a secret password that no one maintains.

Participant #4 stated the organization is exploring other biometrics, such as fingerprint, iris identification, and facial recognition for security verification. While facial recognition has reliability and security issues such as spoofing, biometrics is susceptible to the same attack, but a combination with other measures decreases the security risk. Participant #3 stated that there are a vast number of user roles that define what data and who they can see, and what actions that they can take. Each access to the system, every change of data, every review of data, and every entry of data is logged with the date, time and users.

Participant #3 stated that the organization's security team performed exhaustive security audits of the cloud environments and found it to be state of the art at a level which assures management and leadership of this organization that the likelihood of compromise is negligible. Participant #3 team run checks against the vendor's software to integrate with the organization's Active Directory scheme. The checks are part of the participant's projects but are performed externally to the participant's responsibilities.

In the organizational document Best Practice, access management provides initiatives such as template management techniques to use as an electronic referral management system and use of benchmarks and metrics. For measuring the impact of the access management at the organization, the staff utilized a downstream revenue analysis. It identifies revenue captured for patient visits after an initial visit to the site of study. All participants claimed that attackers are motivated to access sensitive data to include patient records. Organizational document Best Practice, suggested that offenders in healthcare attack the target's valuable information, such as patient data and financial

records. IT security professional should consider access management in their cloud security strategies because it counterbalances the deficiencies of the criminal motivation.

Security and privacy metrics assist both measuring and evaluating the security effectiveness. Participant #4 stated that the challenges with the security of patient records could potentially face internal and external threats. The logs and metrics of usage of the EHR are looked at in the same fashion as the data center in general. Participant # 1 and 4 reviews all metrics and metrics makes setting targets more manageable and dissuades people from disputing the goal behind the target.

Participant #4 stated that managing the data as it leaves the EHR is just as important as reviewing the EHR. The access to the warehouse is primarily controlled through an organization called the data trust which is an enterprise executive organization that defines requirements for who can use and who has access to the data warehouse which has the data and in the case of research precisely what that usage may consist of. Participant #3 stated that if a researcher were not obeying the storage rules for the data that the researcher legitimately was approved to receive, but not correctly handling it, or updating his server security profile, the organization would try to bring it under the institutional management to eliminate the vulnerability of that server. Preventing those situations from occurring, the organization started a process to go out and proactively assess the security profile of servers before their research datasets are delivered. The organization has role-based security for all the administrators and potential users of the cloud copy of the data.

According to my analysis of organizational document Best Practice, senior IT leaders should support the healthcare standards because they adhere to the RAT's tenets of approved methods. Leukfeldt and Yar (2014) stated that there are infinite targets suitable for restrictive predation data, personal information, as well as computer systems that may be compromised and intruded by unlawful interference and invasions. Besides, capable guardians may take a multifariousness of forms, such as network administrators, users, as well as a range of automated protections such as firewalls, VPN, antivirus software, ID authentication, and access management systems.

In the organizational document Access Management, mobile technologies add new complexities to how the organization approaches someone's identity and access management. Reports aim to help access control specialists improve their evaluation of the security access control systems by examining the administration, performance and support properties of devices that embeds each system. Information security professionals with ID and access management experiences are in high demand because of the growth in the cloud and mobile technologies which are creating potential vulnerabilities.

In the organizational document Safe From Cyberattacks, Participant #4 stated that hackers seek medical facilities because of they see unpatched vulnerabilities, and they are seen as an easy target. Little indicates patient data have been singled out. The recent attacks on medical centers across the nation seem to be motivated by money. Participant #4 stated that the organization uses technical instruments to battle attacks such as random numeric code after entering their password which is called multifactor authentication.

The multifactor authentication makes attacks such as phishing for passwords less useful. The organization attacks dropped significantly after the password protection.

RAT aligns with access management because crime cannot be committed without the opportunities to violate the law. Chances for an offense transpire when people's daily routines make them suitable targets for motivated offenders either because of inadequate protection or because they cannot protect themselves. Motivated offenders have didactic beliefs that support fraud and the conclusion that the rewards from theft overbalance the risks. Thus, motivated offenders commit crimes when they encounter the lack of access management.

Mobile victimization aligns with the tenants of RAT. The probability of a crime happening depends on the presence of a motivated offender, the victim, and the absence of a capable guardian, whereas traditional methods to understanding crime focus mainly on the initial element of this equation, the offender (Lusinga & Kyobe, 2017). The conceptual framework provided insight into the participants' perceived application of access management. I found that the participants believe that a cyberattacker look to steal the personal information of patients to commit fraud such as applying for credit or get medical services. Their concern is not to determine what damage that they can do to your credit or how much it will cost you to restore your name. This aligns with Cohen and Felson (1979) who defined RAT as needing a suitable target, the absence of a capable guardian, and a motivated offender.

Table 4

Fourth Major Theme

Source of data collection	*d*
Participants	4
Organizational Documents	3

Note. Theme 4, access management; *d*= data collected from.

Theme 5: Continuous Improvement

Another theme to emerge was reviewing new technologies continuously to assess the security posture and to improve the security posture. One such technology included the implementation of data loss prevention (DLP) tools. DLP is a strategy for making sure that users of the organization do not send sensitive or critical information outside the network. Participant #5 shared that DLP tools are used to identify the location of sensitive data within databases, servers, and file shares. Sensitive data is currently identified as alphanumeric text that follows the format of a medical record number, insurance number, social security number and credit card numbers are matched. Upon identification an administrator reviews if the location of the sensitive data is appropriate. The cloud presents numerous benefits and seems to exhibit unique risks to healthcare organizations concerning privacy and security (Kaushal & Khan, 2014). It is necessary for cloud providers to recognize the risk and concerns in public clouds adequately.

The organizational document Newsletter states that patient data saved in the private cloud can be obtained from tablets, personal computers (PC)s or Macs, but

provisory on a specific location or server. For patients who visit different specialists as a part of their healthcare, the accessibility of their information from one location of the organization to another location of the organization is beneficial. Participant #5 stated that the flexibility of the private cloud allows the doctors, patients, users, and appointment locations to be added quickly and efficiently without being expensive or have downtime. While transitioning from a traditional client-server system to a cloud-based system may seem intimidating at first, the organization benefit financially and save time.

Protected medical information (PMI) includes patient health data, insurance and payment data, and similar data that can be traced back to individuals. Laptops, personal digital assistant (PDA), and even universal serial bus (USB) sticks are not allowed to hold confidential data based on the organization policies. Participant #3 stated that the PMI could reveal a patient's consent externally in the progression of medical treatment. The organization is obligated to take logical steps only to release the necessary information. Failure to make these measures will lead to fines and financial settlements.

According to Participant # 2, devices to weaken the insider threat include monitoring, detection, mitigation, and deterrence. DLP tools may be used to detect, mitigate insider threats, and monitor data usage. Participant #3 stated that the countermeasures that discourage the abuse of internal systems concentrate on four factors, awareness of security policies, monitoring, preventive software, and training. Monitoring alone is not satisfactory for maintaining the insider threat. Monitoring

apprehends the intention but not the motivation, and it is difficult to recognize patterns of misapplication.

Participant #1 has a firewall and a security team in charge of ensuring the privacy of organizational and patient data. The organizational document Considerations for Unified Communications, data recorded and stored needs protection. The protection is done by archiving the data on servers and using DLP products to control access to the data. The organization has segmentation firewalls as part of their infrastructure which ensures that their most important applications are still protected. The segmentation firewalls help to neutralize threats. The segmentation firewall provides an additional layer of security where it is most needed. The segmentation firewalls primary purpose is to secure the internal network traffic. The organization uses the segmentation firewall to provide an additional level of protection for sensitive, high-risk areas of the network.

Participant #2 stated that the organization tries every step of the query, provisioning of data, and analysis of data to ensure that the data is in a secure and auditable environment. The organization no longer permits investigators to download data to their desktop and be able to potentially compromise that data even if it's an inadvertent compromise. There is no option to mess up the chain of custody for data management which stays in a secure environment through every step of the process.

Participant #2 stated that there is data leaving the organization, data-in-transit, and data entering the cloud environment. Then, of course, there are frontal attacks on the client itself. Each of those steps and stages poses a potential security threat. The simplistic way to deal with data leaving the organization which is state of the art is to

encrypt before going into the cloud environment. The organization has an end to end encryption of data, and the data is not decrypted until it is safely residing in a cloud environment. Then the data is only decrypted on demand so that when the organization needs to analyze that data or use that data, it will be dynamically decrypted and then reverts to encryption at rest state.

The benefit of continuous improvement in data loss prevention was an essential theme in the scholarly literature. Health information systems surround a significant accumulation of technologies required for maintaining and sharing patient data electronically. As stated by Luna et al. (2016), data breaches are the preeminent threat to healthcare organizations. Hackers form a relationship outside of systems that hold the stolen data through malware (Manworren et al., 2016). The conceptual framework infers that RAT is suitable for investigating and describing data loss preventions.

RAT aligns with DLP because RAT provides us with a framework to impose loss prevention conditions and solve problems in a structured way. A motivate offender's action can be handled by adjusting environmental signals. With this information in position, loss prevention can be accomplished if the costs are constructed higher than the benefits of committing a crime. RAT represented senior IT leaders as surmising that they remained targets and as implementing cloud security to minimize EHR cyberattacks to protect their systems from data breaches. Impediments cannot provide insight into the actual act of insider threat. RAT presents more attention to the larger society.

Table 5

Fifth Major Theme

Source of data collection	*d*
Participants	4
Organizational Documents	2

Note. Theme 5, continuous improvement; *d*= data collected from.

Applications to Professional Practice

The findings of this study contribute means for senior IT leaders in the healthcare industry to implement cloud security strategies to minimize EHR cyberattacks. The IT effect of this issue is that organizations may profit from EHR cloud security. Discussions to accomplish interoperability within the healthcare industry continue to emphasize the need for healthcare facilities to adopt and implement EHR systems actively. The disinclination of healthcare organizations to implement EHR to achieve interoperability could efficiently share and interpret patient data within heterogeneous systems (Blackman, 2017). Researchers could potentially benefit from the findings of this study by expanding on the strategies which could contribute to a reduction in data breaches, unauthorized access, or misused patient data. The controls put into place by the strategies enable the IT department to control the flow of sensitive PHI. Ideally, the only people who should see the information are doctors, patients, and insurance companies (i.e.,

authorized agents). If the flow of information deviates from that, the IT department has to research, repair, and recover, which stops them from performing other functions. So controls to help with this can enable the IT department to work efficiently.

Implications for Social Change

The information from this research may impact social change by reducing fraudulent use of personal identifiable information and personal health information. The patient information exposed by a data breach can have long term effect on healthcare organizations and the patients. Cloud security strategies may affect how physicians practice by permitting efficient private access to updated records from other authorized medical personnel. The cloud-based EHR allows access to both medical personnel and patients, which the strategies may allow for secured communication between different sites for the treatment of patients. Controlling access to data from multiple systems requires granularity levels of privilege ranging from single patients to an entire population (Demurjian et al., 2014). Without applying the strategies, healthcare providers and patients may face legal repercussions due to either legal requirements or the unlawful disclosure of the information to public channels.

The other social implication is awareness of the necessity in securing EHR in the cloud. A significant measure in countering data breaches in healthcare is to identify threats that lead to data loss (Tu, Spoa-Harty, & Xiao, 2015). Senior IT leaders might use the results of this study to assess and compare their vulnerability, which increases as new threats appear with new technological innovations. By applying the findings of this study,

senior IT leaders may stress importance of cloud security, which protects the organization and the patients from public exposure of sensitive, personal, or confidential information.

Recommendations for Action

The recommended action for healthcare organizations should implement cloud security for their EHR systems which includes processes and policies to prevent the loss or corruption of data. Kavitha, Kannan, and Kotteswaran (2016) suggested that health records are either misplaced or remain under the guidance of health care providers and get destroyed. Implementing cloud-based EHR presents an opportunity for remote prescribing, vaccination management, disease diagnosis, remote diagnosis, and remote real time monitoring and PHR. Senior IT leaders in the healthcare industry have been cautious with implementing cloud security. Participants stated that it will take years to achieve appropriate security for their site's requirements despite currently testing public cloud. Organizational leaders should designate policies and characterize data and controls to guarantee users appropriately manage their data categories (Weber & Carblanc, 2014).

Senior IT leaders should mandate formal cybersecurity training programs for all staff and employees to increase security awareness and minimize threats to data assets. Continuous training helps employees develop the skills and knowledge to handle patient information securely (Alhogail & Mirza, 2014). Cloud security training should include topics preventing, offsetting, and combating threats. Senior IT leaders should consider the motivations behind cyberattacks because these attacks are necessitating issues for sensitive patient data. Senior IT leaders should also consider the use of cloud security for EHR to counterbalance the deficiencies of the RAT.

A review of the findings will be disseminated to interested participants, senior IT leaders, and other interested individuals in healthcare organizations throughout the country. Holtfreter and Harrington (2015) stated that data breaches and exposure of sensitive information could result in fraud or identity theft. To improve the information security in the cloud and prevention programs within the organizations, healthcare practitioners, and senior IT leaders may utilize the results of the study to examine technology strategies, information security risks, and threats that could contribute to EHR data privacy breaches in the cloud. Once the study is approved, I will create an abridge version to submit to journal that receives a lot of exposure to help other researcher in the field of RAT and cybersecurity.

Recommendations for Further Study

The limitations of the study involved a lack of knowledge regarding storing EHR in the cloud and the lack of participation from senior IT leaders. The gatekeeper provided participants based on job title and daily work activities, but only five agreed to participate. However, data saturation was reached for this study. Also, the absence of cloud-based EHR or awareness of the impact of the cloud limited the study within a single organization. Therefore, further research is necessary to expand the knowledge of cybersecurity and EHR.

The next step in researching this topic includes using the multiple case study design with different organizations and states to produce consistent themes. The consistent themes will translate into variables for a quantitative correlational study. This method increases external validity by generalizing within a population. After the results

of the case study, another multiple case study will be designed to explore the global community, which will show comparison and contrast of cyberattacks and cloud-based EHR between the United States and other countries.

Reflections

The past two years have been challenging, but I reaped the rewards in the form of advancements in both, my research and academic writing skills. Despite delays due to the initial topic not being an IT problem, a topic that involved my experience in the medical and IT field provoked my interest. After 12 years in the medical field and 17 years in the IT field, the continuous evolution of technology and privacy concerns in the health field made the topic relevant to me for current and future research.

The next challenging factor was finding an appropriate conceptual framework, including discovering how to use it for a study. However, finding a theory was challenging because the IT theories did not focus on cybercrime, which was the nature of my research question and problem. Therefore, RAT was selected because the focus involves criminology.

The most challenging portion of the proposal was the literature review, which was held to rigorous standards necessary to transition from a practitioner to a scholar-practitioner. After making revisions necessary to meet the standards, the proposal was successfully presented to my committee in an oral conference. After I gained approval from Walden and the organization's IRB, the one-year process of designing the study was concluded and I was ready to collect the data.

Due to scheduling, four weeks was required to collect and conduct member checking of the data from the participants. Based on initial data, an assumption was made that all medical facilities used cloud-based EHR, but some of the interviewees contradicted this assumption. There is more to learn about the topic.

Summary and Study Conclusions

Despite HIPAA security standards for protecting patient data, organizations tend to disregard the imminent threats of hackers exploiting vulnerabilities within the healthcare infrastructure. Senior IT leaders need to increase awareness of cybersecurity, as well as include it in risk management portfolios. While organizations are starting to consider cybersecurity, the next opportunity is to integrate cloud security into the paradigm to protect patients from being exploited by malicious individuals. While cloud-based software may be fiscally desirable, senior IT leaders should not implement the infrastructure at the risk of exposing the patients.

References

Alhogail, A., & Mirza, A. (2014). A framework of information security culture change. *Journal of Theoretical & Applied Information Technology*, *64*(2), 540–549. Retrieved from http://www.jatit.org/

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences, 305,* 357-383. doi:10.1016/j.ins.2015.01.025

Ali, S. H., Carr, P. A., & Ruit, K. G. (2016). Validity and reliability of scores obtained on multiple-choice questions: Why functioning distractors matter. *Journal of the Scholarship of Teaching and Learning, 16*(1), 1-14. doi:10.14434/josotl.v16i1.19106

Almudarra, F. & Qureshi, B. (2015). Issues in adopting agile development principles for mobile cloud computing applications. *Procedia Computer Science, 52,* 1133-1140. doi:10.1016/j.procs.2015.05.131

Alshamaila, Y., Papagiannidis, S., & Li, F. (2013). Cloud computing adoption by SMEs in the north east of England. *Journal of Enterprise Information Management, 26*(3), 250-275. doi:10.1108/17410391311325225

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity*, *23*(3), 121-127. Retrieved from http://tuckerpub.com/jcd.htm

Arpaci, I., Kilicer, K., & Bardakici, S. (2015). Effects of security and privacy concerns on educational use of cloud services. *Computers in Human Behavior, 45*, 93-98. doi:10.1016/j.chb.2014.11.075

Asija, R. & Nallusamy, R. (2016). Healthcare SaaS based on a data model with built in security and privacy. *International Journal of Cloud Applications and Computing, 6*(3), 1-14. doi:10.4018/ijcac.2016070101

Asli, M. A. (2013). Introducing general theory of victimology in criminal sciences. *The International Journal of Humanities, 20*(3), 53-79. Retrieved from http://eijh.modares.ac.ir/article_11016_79e78dedd0067130f58cad4220494e97.pdf

Bacis, E., Vimercati, S. D., Foresti, S., Paraboschi, S., Rosa, M., & Samarati, P. (2017). Distributed shuffle index in the cloud: Implementation and evaluation. *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, 1-6. doi:10.1109/cscloud.2017.25

Baškarada, S. (2014). Qualitative case study guidelines. *Qualitative Report, 19*(24), 1-18. Retrieved from http://www.nova.edu/ssss/QR/QR19/baskarada24.pdf

Baur, X., Budnik, L. T., Ruff, K., Egilman, D. S., Lemen, R. A., & Soskolne, C. L. (2015). Ethics, morality, and conflicting interests: how questionable professional integrity in some scientists supports global corporate influence in public health. *International Journal of Occupational and Environmental Health, 21*(2), 172-175. doi:10.1179/2049396714y.0000000103

Bayramusta, M. & Nasir, V. A. (2016). A fad or future of IT?: A comprehensive literature review on the cloud computing research. *International Journal of Information Management*, *36*(4), 635-644. doi:10.1016/j.ijinfomgt.2016.04.006

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open*, *2*, 8-14. doi:10.1016/j.npls.2016.01.001

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research*, *26*(13), 1802-1811. doi:10.1177/1049732316654870

Bjurulf, S., Vedung, E., & Larsson, C. G. (2013). A triangulation approach to impact evaluation. *Evaluation*, *19*(1), 56-73. doi:10.1177/1356389012472248

Blackman, S. (2017). Towards a conceptual framework for persistent use: A technical plan to achieve semantic interoperability within electronic health record systems. *Proceedings of the 50th Hawaii International Conference on System Sciences (2017)*, 4653-4662. doi:10.24251/hicss.2017.566

Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research: An International Journal*, *19*(4), 426-432. doi:10.1108/qmr 06 2016 0053

Bos, J. W., Lauter, K., & Naehrig, M. (2014). Private predictive analysis on encrypted medical data. *Journal of Biomedical Informatics*, *50*, 234-243. doi:10.1016/j.jbi.2014.04.003

Bourke, B. (2014). Positionality: Reflecting on the research process. *Qualitative Report*, *19*(33), 1-9. Retrieved from http://www.nova.edu/ssss/QR/QR19/bourke18.pdf

Bowden, F. & Williams, P. (2013). A framework for determining the validation of analytical campaigns in defence experimentation. *20th International Congress on Modelling and Simulation*, 1131-1137. Retrieved from http://www.mssanz.org.au/modsim2013

Braga, A. A. & Clarke, R. V. (2014). Explaining high-risk concentrations of crime in the city: Social disorganization, crime opportunities, and important next steps. *Journal of Research in Crime and Delinquency*, *51*(4), 480-498. doi:10.1177/0022427814521217

Braun, V. & Clarke, V. (2014). What can "thematic analysis" offer health and wellbeing researchers? *International Journal of Qualitative Studies on Health and Well-being*, *9*(1), 1-2. doi:10.3402/qhw.v9.26152

Brender, N. & Markov, I. (2013). Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. *International Journal of Information Management*, *33*(5), 726-733. doi:10.1016/j.ijinfomgt.2013.05.004

Brière, S., Proulx, D., Flores, O. N., & Laporte, M. (2015). Competencies of project managers in international NGOs: Perceptions of practitioners. *International Journal of Project Management*, *33*(1), 116-125. doi:10.1016/j.ijproman.2014.04.010

Bunch, J., Clay-Warner, J., & Lei, M. (2015). Demographic characteristics and victimization risk: Testing the mediating effects of routine activities. *Crime & Delinquency*, *61*(9), 1181-1205. doi:10.1177/0011128712466932

Bunch, J., Clay-Warner, J., & Mcmahon Howard, J. (2014). The effects of victimization on routine activities. *Criminal Justice and Behavior*, *41*(5), 574-592. doi:10.1177/0093854813508286

Busse, C., Kach, A., & Wagner, S. (2016). Boundary conditions: What they are, how to explore them, why we need them, and when to consider them. *Organizational Research Methods*, 1-36. doi: 10.1177/1094428116641191

Califf, R. M. & Sugarman, J. (2015). Exploring the ethical and regulatory issues in pragmatic clinical trials. *Clinical Trials, 12*(5), 436-441. doi:10.1177/1740774515598334

Callahan, J. L. (2014). Writing literature reviews a reprise and update. *Human Resource Development Review, 13*, 271-275. doi:10.1177/1534484314536705

Cameron, R. & Molina-Azorin, J. F. (2011). The acceptance of mixed methods in business and management. *International Journal of Organizational Analysis, 22*(1), 14-29. doi:10.1108/ijoa 08 2010 0446

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum, 41*(5), 545-547. doi:10.1188/14.ONF.545-547

Cascardo, D. (2015). Physician challenges in 2015. *Journal of Medical Practice Management*, 30(6), 395–398. Retrieved from http://www.mpmnetwork.com/section_47_MPM-Journal.cfm

Case, C. J. & King, D. L. (2014). System security: A trend analysis of student electronic resources uses policy perceptions and risky behavior. *American Society of*

Business and Behavioral Sciences, 10(1), 31-42. Retrieved from http://commons.nmu.edu/cgi/viewcontent.cgi?article=1110&context=facwork_journalarticles#page=32

Castiglione, A., Pizzolante, R., De Santis, A., Carpentieri, B., Castiglione, A., & Palmieri, F. (2015). Cloud-based adaptive compression and secure management services for 3D healthcare data. *Future Generation Computer Systems, 43-44*, 120-134. doi:10.1016/j.future.2014.07.001

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *Qualitative Report, 21*, 811-831. Retrieved from http://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2337&context=tqr

Castleberry, A. (2014). NVivo 10 [software program]. Version 10. QSR International; 2012. *American Journal of Pharmaceutical Education, 78*(1), 25. doi:10.5688/ajpe78125

Check, D. K., Wolf, L. E., Dame, L. A., & Beskow, L. M. (2014). Certificates of confidentiality and informed consent: Perspectives of IRB chairs and institutional legal counsel. *IRB: Ethics and Human Research, 36*(1), 1-8. doi:10.1038/gim.2014.102

Chen, Q., Abdelwahed, S., & Erradi, A. (2014). A model-based validated autonomic approach to self-protect computing systems. *IEEE Internet of Things Journal, 1*(5), 446-460. doi:10.1109/jiot.2014.2349899

Choi, K., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior, 73,* 394-402. doi:10.1016/j.chb.2017.03.061

Choi, K., Cronin, S., & Correia, H. (2016). The assessment of capable guardianship measures against bullying victimization in the school environment. *Police Practice and Research, 17*(2), 149-159. doi:10.1080/15614263.2015.1128161

Chou, D. C. (2015). Cloud security: A value creation model. *Computer Standards & Interfaces, 38,* 72-77. doi:10.1016/j.csi.2014.10.001

Chughtai, A. A. & Buckley, F. (2013). Exploring the impact of trust on research scientists' work engagement. *Personnel Review, 42,* 396-421. doi:10.1108/PR 06 2011-0097

Cioca, L. & Ivascu, L. (2014). IT technology implications analysis on the occupational risk: Cloud security architecture. *Procedia Technology, 16,* 1548-1559. doi:10.1016/j.protcy.2014.10.177

Coccoli, M., Maresca, P., Stanganelli, L., & Guercio, A. (2015). An experience of collaboration using a PaaS for the smarter university model. *Journal of Visual Languages & Computing, 31,* 275-282. doi:10.1016/j.jvlc.2015.10.014

Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608. doi:10.2307/2094589

Connelly, L. M. (2016). Understanding research. Trustworthiness in qualitative research. *MedSurg Nursing Journal, 25*(6), 435-436. Retrieved from https://www.amsn.org/

Cope, D. G. (2014). Methods and meanings: Credibility and trustworthiness of qualitative research. *Oncology Nursing Forum, 41*(1), 89-91. doi:10.1188/14.onf.89-91

Corbin, J. & Strauss, A. (2014). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (4th ed.). Los Angeles, CA: Sage Publications, Inc.

Corcoran, J., Zahnow, R., & Higgs, G. (2016). Using routine activity theory to inform a conceptual understanding of the geography of fire events. *Geoforum, 75*, 180-185. doi:10.1016/j.geoforum.2016.07.015

Cotroneo, D. (2016). Automated root cause identification of security alerts: Evaluation in a SaaS cloud. *Future Generation Computer Systems, 56*, 375-387. doi:10.1016/j.future.2015.09.009

Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *Nurse Researcher, 21*(5), 19-27. doi:10.7748/nr.21.5.19.e1240

Crowl, J. N. & Battin, J. R. (2016). Fear of crime and the police: Exploring lifestyle and individual determinants among university students. *The Police Journal*, 1-20. doi:10.1177/0032258x16676289

Cruz, E. V. & Higginbottom, G. (2013). The use of focused ethnography in nursing research. *Nurse Researcher, 20*(4), 36-43. doi:10.7748/nr2013.03.20.4.36.e305

Cugini, M. (2015). Successfully navigating the human subject's approval process. *Journal of Dental Hygiene, 89*(1), 54-56. Retrieved from http://jdh.adha.org/content/89/suppl_1/54.full.pdf

Davidovic, V., Ilijevic, D., Luk, V., & Pogarcic, I. (2015). Private cloud computing and delegation of control. *Procedia Engineering, 100,* 196-205. doi:10.1016/j.proeng.2015.01.358

Davies, S. & Coldridge, L. (2015). 'No man′s land': An exploration of the traumatic experiences of student midwives in practice. *Midwifery, 31*(9), 858-864. doi:10.1016/j.midw.2015.05.001

Day, D. V., Fleenor, J. W., Atwater, L. E., Sturm, R. E., & McKee, R. A. (2014). Advances in leader and leadership development: A review of 25years of research and theory. *The Leadership Quarterly, 25*(1), 63-82. doi:10.1016/j.leaqua.2013.11.004

Daylami, N. (2015). The origin and construct of cloud security. *International Journal of the Academic Business World, 9*(2), 39-45. Retrieved from http://jwpress.com/IJABW/IJABW.htm

Değerli, A., Aytekin, Ç., & Değerli, B. (2015). Analyzing information technology status and networked readiness index in context of diffusion of innovations theory. *Procedia Social and Behavioral Sciences, 195*, 1553-1562. doi:10.1016/j.sbspro.2015.06.190

Dekking, S. A., Van der Graaf, R., & Van Delden, J. J. (2014). Strengths and weaknesses of guideline approaches to safeguard voluntary informed consent of

patients within a dependent relationship. *BMC Medicine, 12*(1). doi:10.1186/1741-7015-12-52

DeMeo, S. D., Nagler, A., & Heflin, M. T. (2016). Development of a health professions education research-specific institutional review board template. *Academic Medicine, 91*(2), 229-232. doi:10.1097/acm.0000000000000987

Demurjian, S. A., Algarín, A. D., Bi, J., Berhe, S., Agresta, T., Wang, X., & Blechner, M. (2014). A viewpoint of security for digital health care in the United States. *International Journal of Privacy and Health Information Management, 2*(1), 1-21. doi:10.4018/ijphim.2014010101

Deuter, K. & Jaworski, K. (2016). Assuming vulnerability: Ethical considerations in a multiple-case study with older suicide attempters. *Research Ethics*, 1-12. doi:10.1177/1747016116649994

Doerner, W. G. & Lab, S. P. (2015). *Victimology* (7th ed.). Philadelphia, PA: Taylor & Francis.

Drawve, G., Thomas, S. A., & Walker, J. T. (2013). The likelihood of arrest: A routine activity theory approach. *American Journal of Criminal Justice, 39*(3), 450-470. doi:10.1007/s12103 013 9226 2

Dudek, N. L., Papp, S., & Gofton, W. T. (2015). Going paperless? Issues in converting a surgical assessment tool to an electronic version. *Teaching and Learning in Medicine, 27*(3), 274-279. doi:10.1080/10401334.2015.1044661

El Hussein, M., Jakubec, S. L., & Osuji, J. (2015). Assessing the facts: A mnemonic for teaching and learning the rapid assessment of rigor in qualitative research

studies. *Qualitative Report, 20*(8), 1182-1184. Retrieved from http://nsuworks.nova.edu/tqr/vol20/iss8/3

Eller, L. S., Lev, E. L., & Feurer, A. (2014). Key components of an effective mentoring relationship: A qualitative study. Nurse Education Today, 34(5), 815-820. doi:10.1016/j.nedt.2013.07.020

Elmaghraby, A. S. & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research, 5*(4), 491-497. doi:10.1016/j.jare.2014.02.006

Elo, S., Kaariainen, M., Kanste, O., Polkki, T., Utriainen, K., & Kyngas, H. (2014). Qualitative content analysis: A focus on trustworthiness. *SAGE Open*, *4*(1), 1-10. doi:10.1177/2158244014522633

Ermakova, T. (2015). Understanding physicians' adoption of health cloud. *Computer Science and Information Technology, 5*(1), 17-24. doi:10.5121/csit.2015.50102

Eyre, L., George, B., & Marshall, M. (2015). Protocol for a process-oriented qualitative evaluation of the Waltham Forest and East London Collaborative (WELC) integrated care pioneer programme using the Researcher-in-Residence model. *BMJ Open*, *5*(11), 1-10. doi:10.1136/bmjopen-2015-009567

Fabian, B., Ermakova, T., & Junghanns, P. (2015). Collaborative and secure sharing of healthcare data in multi-clouds. *Information Systems, 48*, 132-150. doi:10.1016/j.is.2014.05.004

Fassinger, R. & Morrow, S. L. (2013). Toward best practices in quantitative, qualitative, and mixed- method research: A social justice perspective. *Journal for Social*

Action in Counseling & Psychology, *5*(2), 69-83. Retrieved from http://jsacp.tumblr.com/

Flannery, T., & Gormley, G. (2014). Evaluation of the contribution of theatre attendance to medical undergraduate neuroscience teaching – A pilot study. *British Journal of Neurosurgery*, *28*(5), 680-684. doi:10.3109/02688697.2014.896873

Frels, R. K. & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling and Development*, *91*(2), 184-194. doi:10.1002/j.1556-6676.2013.00085.x

Fusch, P. I. & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *Qualitative Report*, *20*(9), 1408-1416. Retrieved from http://www.nova.edu/ssss/QR/QR20/9/fusch1.pdf

Fusch, P. I., Fusch, G. E., & Ness, L. R. (2017). How to conduct a mini-ethnographic case study: A guide for novice researchers. *Qualitative Report*, *22*(3), 923-941. Retrieved from http://nsuworks.nova.edu/tqr/vol22/iss3/16

García-Valls, M., Cucinotta, T., & Lu, C. (2014). Challenges in real time virtualization and predictable cloud security. *Journal of Systems Architecture*, *60*(9), 726-740. doi:10.1016/j.sysarc.2014.07.004

Gazzarata, G., Gazzarata, R., & Giacomini, M. (2015). A standardized SOA based solution to guarantee the secure access to EHR. *Procedia Computer Science*, *64*, 1124-1129. doi:10.1016/j.procs.2015.08.582

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. A. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *Qualitative*

Report, *20*(11), 1772-1789. Retrieved from http://nsuworks.nova.edu/tqr/vol20/iss11/5/

Gill, M. J. (2014). The possibilities of phenomenology for organizational research. *Organizational Research Methods*, *17*(2), 118-137. doi:10.1177/1094428113518348

Glasser, D. & Taneja, A. (2017). A routine activity theory based framework for combating cybercrime. In *Identity theft: Breakthroughs in research and practice*, 69-78. doi:10.4018/978 1-5225 0808 3.ch004

Gomez, J. (2015). Cyber security in healthcare: Understanding the new world threats. *Divurgent*, 1-13. Retrieved from http://www.divurgent.com/cyber security in healthcare/

Goyal, S. (2014). Public vs private vs hybrid vs community - cloud computing: A critical review. *International Journal of Computer Network and Information Security*, *6*(3), 20-29. doi:10.5815/ijcnis.2014.03.03

Green, C., Duan, N., Gibbons, R., Hoagwood, K., Palinkas, L., & Wisdom, J. (2014). Approaches to mixed methods dissemination and implementation research: Methods, strengths, caveats, and opportunities. *Administration and Policy in Mental Health and Mental Health Services Research*, 1-16. doi:10.1007/s10488-014-0552-6

Grossoehme, D. H. (2014). Overview of qualitative research. *Journal of Health Care Chaplaincy*, *20*(3), 109-122. doi:10.1080/08854726.2014.925660

Gupta, P., Seetharaman, A., & Raj, J. R. (2013). The usage and adoption of cloud security by small and medium businesses. *International Journal of Information Management, 33*(5), 861-874. doi:10.1016/j.ijinfomgt.2013.07.001

Hadidi, N., Lindquist, R., Treat-Jacobson, D., & Swanson, P. (2013). Participant withdrawal: Challenges and practical solutions for recruitment and retention in clinical trials. *Creative Nursing, 19*(1), 37-41. doi:10.1891/1078-4535.19.1.37

Haegeman, K., Marinelli, E., Scapolo, F., Ricci, A., & Sokolov, A. (2013). Quantitative and qualitative approaches in future-oriented technology analysis (FTA): From combination to integration? *Technological Forecasting and Social Change, 80*(3), 386-397. doi:10.1016/j.techfore.2012.10.002

Halverson, L. R., Graham, C. R., Spring, K. J., Drysdale, J. S., & Henrie, C. R. (2014). A thematic analysis of the most highly cited scholarship in the first decade of blended learning research. *The Internet and Higher Education, 20*, 20-34. doi:10.1016/j.iheduc.2013.09.004

Harvey, L. (2015). Beyond member-checking: a dialogic approach to the research interview. *International Journal of Research & Method in Education, 38*(1), 23-38. doi:10.1080/1743727x.2014.914487

Hashizume, K., Rosado, D. G., Fernández Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud security. *Journal of Internet Services and Applications, 4*(5), 1-13. doi:10.1186/1869 0238 4 5

Hawley, A. H. (1950). Human ecology: A theory of community structure. *American Sociological Review, 15*(5). doi:10.2307/2086931

Heale, R. & Forbes, D. (2013). Understanding triangulation in research. *Evidence Based Nursing*, *16*(4), 98. doi:10.1136/eb-2013-101494

Hellal, A. & Romdhane, L. B. (2016). Minimal contrast frequent pattern mining for malware detection. *Computers & Security*, *62*, 19-32. doi:10.1016/j.cose.2016.06.004

Helo, P., Suorsa, M., Hao, Y., & Anussornnitisarn, P. (2014). Toward a cloud based manufacturing execution system for distributed manufacturing. *Computers in Industry*, *65*(4), 646-656. doi:10.1016/j.compind.2014.01.015

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: an empirical foundation for a theory of personal victimization: An empirical foundation for a theory of personal victimization*. Cambridge, MA: Ballinger.

Holt, T. J. & Bossler, A. M. (2013a). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20-40. doi:10.1080/01639625.2013.822209

Holt, T. J. & Bossler, A. M. (2013b). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, *29*(4), 420-436. doi:10.1177/1043986213507401

Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. *Journal of Financial Crime*, *22*(2), 242-260. doi:10.1108/jfc-09-2013-0055

Hosseinabadi, R., Karampourian, A., Beiranvand, S., & Pournia, Y. (2013). The effect of quality circles on job satisfaction and quality of work-life of staff in emergency

medical services. *International Emergency Nursing*, *21*(4), 264-270. doi:10.1016/j.ienj.2012.10.002

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher*, *20*(4), 12-17. doi:10.7748/nr2013.03.20.4.12.e326

Hsieh, P. (2015). Healthcare professionals' use of health clouds: Integrating technology acceptance and status quo bias perspectives. *International Journal of Medical Informatics*, *84*(7), 512-523. doi:10.1016/j.ijmedinf.2015.03.004

Hsu, P., Ray, S., & Li-Hsieh, Y. (2014). Examining cloud computing adoption intention, pricing mechanism, and deployment model. *International Journal of Information Management, 34*(4), 474-488. doi:10.1016/j.ijinfomgt.2014.04.006

Hudson, S. & Hudson, R. (2013). Engaging with consumers using social media: a case study of music festivals. *International Journal of Event and Festival Management, 4*(3), 206-223. doi:10.1108/ijefm 06 2013 0012

Hussein, A. (2015). The use of triangulation in social sciences research: Can qualitative and quantitative methods be combined? *Journal of Comparative Social Work, 4*(1), 1-12. Retrieved from https://doaj.org/article/a76dfb64227a46d3b7878af4c5b2d52e?

Hyett, N., Kenny, A., & Dickson-Swift, V. (2014). Methodology or method? A critical review of qualitative case study reports. *International Journal of Qualitative Studies on Health and Well Being, 9*(0). doi:10.3402/qhw.v9.23606

Ilievski, A. (2016). An explanation of the cybercrime victimisation: Self-control and lifestyle/routine activity theory. *Innovative Issues and Approaches in Social Sciences*, *9*(1), 30-47. doi:10.12959/issn.1855 0541.iiass 2016 no1-art02

Ismail, S., Sitnikova, E., & Slay, J. (2014). Using integrated system theory approach to assess security for SCADA systems cyber security for critical infrastructures: A pilot study. *11th International Conference on Fuzzy Systems and Knowledge Discovery*, 1000–1006. doi:10.1109/fskd.2014.6980976

Jackson, S. L. (2015). The vexing problem of defining financial exploitation. *Journal of Financial Crime*, *22*(1), 63-78. doi:10.1108/jfc-05-2014-0026

Jain, A., & Kumar, R. (2014). A taxonomy of cloud computing. *International Journal of Scientific and Research Publications*, *4*(7), 1-5. Retrieved from http://www.ijsrp.org

James, N. (2017). Using narrative inquiry to explore the experience of one ethnically diverse ESL nursing student. *Teaching and Learning in Nursing*, 1-6. doi:10.1016/j.teln.2017.08.002

Jang-Jaccard, J. & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973-993. doi:10.1016/j.jcss.2014.02.005

Jeong, H., Yi, G., & Park, J. H. (2016). A service composition model based on user experience in Ubi cloud comp. *Telecommunication Systems*, *61*(4), 897-907. doi:10.1007/s11235 015 0045 2

Johnson, S. D. & Groff, E. R. (2014). Strengthening theoretical testing in criminology using agent-based modeling. *Journal of Research in Crime and Delinquency*, *51*(4), 509-525. doi:10.1177/0022427814531490

Joolaee, S., Amiri, S. R. J., Farahani, M. A., & Varaei, S. (2015). Iranian nursing students' preparedness for clinical training: A qualitative study. *Nurse Education Today*, *35*(10), e13 e17. doi:10.1016/j.nedt.2015.07.026

Jouini, M., Rabai, L. B., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489-496. doi:10.1016/j.procs.2014.05.452

Kaddoura, S., Haraty, R. A., Zekri, A., & Masud, M. (2015). Tracking and repairing damaged healthcare databases using the matrix. *International Journal of Distributed Sensor Networks*, *2015*, 1-8. doi:10.1155/2015/914305

Kahlke, R. M. (2014). Generic qualitative approaches: Pitfalls and benefits of methodological mixology. *International Journal of Qualitative Methods*, *13*(1), 37-52. doi:10.1177/160940691401300119

Kalloniatis, C., Mouratidis, H., Vassilis, M., Islam, S., Gritzalis, S., & Kavakli, E. (2014). Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. *Computer Standards & Interfaces*, *36*(4), 759-775. doi:10.1016/j.csi.2013.12.010

Kaur, P. D. & Chana, I. (2014). Cloud based intelligent system for delivering healthcare as a service. *Computer Methods and Programs in Biomedicine*, *113*(1), 346-359. doi:10.1016/j.cmpb.2013.09.013

Kaushal, D. S., & Khan, Y. (2014). Cloud computing services in medical healthcare solutions. *International Journal of Research, 1*(4), 312-324. Retrieved from https://internationaljournalofresearch.com/

Kavitha, R., Kannan, E., & Kotteswaran, S. (2016). Implementation of cloud based electronic health record (EHR) for Indian healthcare needs. *Indian Journal of Science and Technology, 9*(3), 1-5. doi:10.17485/ijst/2016/v9i3/86391

Keutel, M., Michalik, B., & Richter, J. (2014). Towards mindful case study research in IS: A critical analysis of the past ten years. *European Journal of Information Systems, 23*(3), 256-272. doi:10.1057/ejis.2013.26

Khey, D. N. & Sainato, V. A. (2013). Examining the correlates and spatial distribution of organizational data breaches in the United States. *Security Journal, 26,* 367-382. doi:10.1057/sj.2013.24

Kirubakaramoorthi, R., Arivazhagan, D., & Helen, D. (2015). Analysis of cloud computing technology. *Indian Journal of Science and Technology*, *8*(21), 1-3. doi:10.17485/ijst/2015/v8i21/79144

Kiruthika, V., & Laxmi Sree B. R. (2014). A smart crypto scheme for multi owner data authentication over cloud service. *International Journal of Computer Science and Information Technologies, 5*(6), 7567-7571. Retrieved from http://www.ijcsit.com

Kokkinos, C. M., & Saripanidis, I. (2017). A lifestyle exposure perspective of victimization through Facebook among university students. Do individual differences matter? *Computers in Human Behavior, 74,* 235-245. doi:10.1016/j.chb.2017.04.036

Kornbluh, M. (2015). Combatting challenges to establishing trustworthiness in qualitative research. *Qualitative Research in Psychology*, *12*(4), 397-414. doi:10.1080/14780887.2015.1021941

Kote, A., Raja, P. V. K., & Raju, M. V. (2015). Cloud data security challenges and its solutions. *International Journal of Computer & Communication Engineering Research*, *3*(5), 89-92. Retrieved from http://ijccer.org/index.php/ojs/article/view/204/87

Krishna, B. H., Kiran, S., Murali, G., & Reddy, R. P. (2016). Security issues in service model of cloud security environment. *Procedia Computer Science*, *87*, 246-251. doi:10.1016/j.procs.2016.05.156

Krist, A. H., Beasley, J. W., Crosson, J. C., Kibbe, D. C., Klinkman, M. S., Lehmann, C. U., … Waldren, S. E. (2014). Electronic health record functionality needed to better support primary care. *Journal of the American Medical Informatics Association*, *21*(5), 764-771. doi:10.1136/amiajnl-2013-002229

Kruse, C. S., Bolton, K., & Freriks, G. (2015). The effect of patient portals on quality outcomes and its implications to meaningful use: A systematic review. *Journal of Medical Internet Research*, *17*(2), e44. doi:10.2196/jmir.3171

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1-10. doi:10.3233/thc-161263

Kshetri, N. (2013). Privacy and security issues in cloud security: The role of institutions and institutional evolution. *Telecommunications Policy*, *37*(4-5), 372-386. doi:10.1016/j.telpol.2012.04.011

Kumar, N. (2013). Informed consent: Past and present. *Perspectives in Clinical Research, 4*(1), 21. doi:10.4103/2229-3485.106372

Kumar, P., Kumar, L., Kumar, K., Kumar, S., & Lal, S. (2013). Security threats to cloud security. *International Journal of IT, Engineering and Applied Sciences Research*, *2*(1), 25-29. Retrieved from http://www.irjcjournals.org/ijieasr/Jan2013/5.pdf

Kumar, R., Gupta, N., Charu, S., Jain, K., & Jangir, S. K. (2014). Open source solution for cloud security platform using OpenStack. *International Journal of Computer Science and Mobile Computing, 3*(5), 89-98. doi:10.13140/2.1.1695.9043

Kushida, K. E., Murray, J., & Zysman, J. (2015). Cloud security: From scarcity to abundance. *Journal of Industry, Competition and Trade*, *15*(1), 5-19. doi:10.1007/s10842 014 0188 y

Leedy, P. D. & Ormrod, J. E. (2013). *Practical research: Planning and design* (10th ed.). Upper Saddle River, NJ: Pearson Education.

Leukfeldt, E. R. & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280. doi:10.1080/01639625.2015.1012409

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551-555. doi:10.1089/cyber.2014.0008

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, *4*(3), 324–327. doi:10.4103/2249-4863.161306

Levesque, F. L., Fernandez, J. M., & Somayaji, A. (2014). Risk prediction of malware victimization based on user behavior. *2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE)*. doi:10.1109/malware.2014.6999412

Lewin, S., Glenton, C., Munthe-Kaas, H., Carlsen, B., Colvin, C. J., Gülmezoglu, M., … Rashidian, A. (2015). Using qualitative evidence in decision making for health and social interventions: An approach to assess confidence in findings from qualitative evidence syntheses (GRADE-CERQual). *PLOS Medicine*, *12*(10), 1-18. doi:10.1371/journal.pmed.1001895

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice*, *16*(4), 473-475. doi:10.1177/1524839915580941

Lian, J. (2017). Establishing a cloud computing success model for hospitals in Taiwan. *INQUIRY: The Journal of Health Care Organization, Provision, and Financing*, *54*, 1-6. doi:10.1177/0046958016685836

Lin, C., Abdul, S. S., Clinciu, D. L., Scholl, J., Jin, X., Lu, H., … Li, Y. (2014). Empowering village doctors and enhancing rural healthcare using cloud security in a rural area of mainland China. *Computer Methods and Programs in Biomedicine*, *113*(2), 585-592. doi:10.1016/j.cmpb.2013.10.005

Liu, V., Musen, M. A., & Chou, T. (2015). Data breaches of protected health information in the United States. *JAMA*, *313*(14), 1471-1473. doi:10.1001/jama.2015.2252

Lloyd, T. (2015). Access management: the overlooked but critical enabler. *Learned Publishing*, *28*(4), 292-298. doi:10.1087/20150408

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Healthcare*, *24*(1), 1-9. doi:10.3233/thc151102

Lusinga, S., & Kyobe, M. (2017). Testing a typology of mobile phone victimisation using cluster analysis. *The Electronic Journal of Information Systems in Developing Countries*, *78*(1), 1-36. doi:10.1002/j.1681-4835.2017.tb00574.x

Madarkar, J., Anuradha, D., & Waghmare, S. (2014). Security issues of patient health records in e Hospital management in cloud. *International Journal of Emerging Research in Management & Technology*, *3*(6), 46-51. Retrieved from http://www.ermt.net/docs/papers/Volume_3/6_June2014/V3N5 199.pdf

Madni, S. H., Latiff, M. S., Coulibaly, Y., & Abdulhamid, S. M. (2016). Resource scheduling for infrastructure as a service (IaaS) in cloud security: Challenges and

opportunities. *Journal of Network and Computer Applications, 68,* 173-200. doi:10.1016/j.jnca.2016.04.016

Maheux, B. (2014). Assessing the intentions and timing of malware. *Technology Innovation Management Review, 4*(11), 34-40. Retrieved from http://www.timreview.ca

Majhi, S. K., Patra, G., & Dhal, S. K. (2016). Cyber physical systems & public utility in India: State of art. *Procedia Computer Science, 78,* 777-781. doi:10.1016/j.procs.2016.02.052

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies. *Qualitative Health Research, 26*(13), 1753-1760. doi:10.1177/1049732315617444

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons, 59*(3), 257-266. doi:10.1016/j.bushor.2016.01.002

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2014). Juveniles and cyber stalking in the United States: An analysis of theoretical predictors of patterns of online perpetration. *International Journal of Cyber Criminology, 8*(1), 47-56. Retrieved from http://www.cybercrimejournal.com/marcumetalijcc2014vol8issue1.pdf

Maxwell, A. J. (2013). *Qualitative research design: An interactive approach* (3th ed.). Thousand Oaks, CA: Sage.

McCarthy, M. A., Herger, L. M., & Khan, S. M. (2014). A compliance aware software defined infrastructure. *International Journal of Services Computing, 2*(2), 58-71. doi:10.1109/scc.2014.79

McCusker, K., & Gunaydin, S. (2014). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion, 30*(7), 537-542. doi:10.1177/0267659114559116

McFadyen, J., & Rankin, J. (2016). The role of gatekeepers in research: Learning from reflexivity and reflection. *GSTF Journal of Nursing and Health Care (JNHC), 4*(1), 82-88. doi:10.5176/2345-718X_4.1.135

McIntosh, M. J., & Morse, J. M. (2015). Situating and constructing diversity in semi-structured interviews. *Global Qualitative Nursing Research, 2*, 233339361559767. doi:10.1177/2333393615597674

McQuade, S. C. (1998). Towards a theory of technology enabled crime. *Unpublished manuscript*. George Mason University, Fairfax, Virginia.

McQuade, S. C. (2006). Technology enabled crime, policing and security. *The Journal of Technology Studies, 32*(1), 32-42. doi:10.21061/jots.v32i1.a.5

McRae, A. D., Bennett, C., Brown, J. B., Weijer, C., Boruch, R., Brehaut, J., … Taljaard, M. (2013). Researchers' perceptions of ethical challenges in cluster randomized trials: a qualitative analysis. *Trials, 14*(1), 1. doi:10.1186/1745-6215-14-1

Mehraeen, E., Ghazisaeedi, M., Farzi, J., & Mirshekari, S. (2016). Security challenges in healthcare cloud security: A systematic review. *Global Journal of Health Science*, *9*(3), 157-166. doi:10.5539/gjhs.v9n3p157

Miethe, T. D. & Meier, R. F. (1990). Opportunity, choice and criminal victimization rates: A theory of a theoretical model. *Journal of Research in Crime & Delinquency*, *27*, 243-266.

Miner-Romanoff, K. (2012). Interpretive and critical phenomenological crime studies: A model design. *Qualitative Report, 17*(27), 1-32. Retrieved from http://files.eric.ed.gov/fulltext/EJ981463.pdf

Modic, J., Trapero, R., Taha, A., Luna, J., Stopar, M., & Suri, N. (2016). Novel efficient techniques for real time cloud security assessment. *Computers & Security*, *62*, 1-18. doi:10.1016/j.cose.2016.06.003

Mojtahed, R., Nunes, M. B., Martins, J. T., & Peng, A. (2014). Equipping the constructivist researcher: The combined use of semi-structured interviews and decision-making maps. *Electronic Journal of Business Research Methods*, *12*(2), 87-95. Retrieved from http://www.ejbrm.com/volume12/issue2

Montolio, D. & Planells, S. (2016). Does tourism boost criminal activity? Evidence from a top touristic country. *SSRN Electronic Journal*, *50*(2), 216-238. doi:10.2139/ssrn.2341639

Morse, A. & McEvoy, C. (2014). Qualitative research in sport management: Case study as a methodological approach. *Qualitative Report, 19*(17), 1-13. Retrieved from http://nsuworks.nova.edu/tqr/vol19/iss31/3/

Morse, J. M. (2015a). "Data were saturated . . . ". *Qualitative Health Research, 25*(5), 587-588. doi:10.1177/1049732315576699

Morse, J. M. (2015b). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research, 25*(9), 1212-1222. doi:10.1177/1049732315588501

Morse, J. M. (2016). Underlying ethnography. *Qualitative Health Research, 26*(7), 875-876. doi:10.1177/1049732316645320

Nagaraj, R., & Kalarani, X. A. (2016). Semantically document clustering using contextual similarities. *International Journal of Applied Engineering Research, 11*(1), 71-76. Retrieved from https://www.ripublication.com/ijaer16/ijaerv11n1_13.pdf

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: a multi nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *16*(2), 203-210. doi:10.1080/14043858.2015.1046640

Nimon, K. (2011). Improving the quality of quantitative research reports: A call for action. *Human Resource Development Quarterly*, *22*(4), 387-394. doi:10.1002/hrdq.20091

O'Malley, A. S., Gourevitch, R., Draper, K., Bond, A., & Tirodkar, M. A. (2015). Overcoming challenges to teamwork in patient-centered medical homes: A qualitative study. *Journal of General Internal Medicine*, *30*(2), 183-192. doi:10.1007/s11606-014-3065-9

Odumesi, J. O. (2014). A socio technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology, 6*(3), 116-125. doi:10.5897/ijsa2013.0510

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56,* 83-93. doi:10.1016/j.cose.2015.10.002

Omondi, M. P., Ombui, K., & Mungatu, J. (2013). Factors affecting effective strategy implementation for attainment of Millennium Development Goal 5 by international reproductive health non-governmental organizations in Kenya. *The TQM Journal, 25*(5), 507-519. doi:10.1108/09596110110403712

Peguero, A. A., Popp, A. M., & Koo, D. J. (2015). Race, ethnicity, and school-based adolescent victimization. *Crime & Delinquency, 61*(3), 323-349. doi:10.1177/0011128711398021

Peticca-Harris, A., DeGama, N., & Elias, S. R. (2016). A dynamic process model for finding informants and gaining access in qualitative research. *Organizational Research Methods*, *19*(3), 376-401. doi:10.1177/1094428116629218

Pickering, C. & Byrne, J. (2014). The benefits of publishing systematic quantitative literature reviews for PhD candidates and other early career researchers. *Higher Education Research & Development, 33,* 534-548. doi:10.1080/07294360.2013.841651

Pratt, T., Turanovic, J. J., Fox, K. A. & Wright, K. A. (2014). Self-control and victimization: A meta-analysis. *Criminology, 52*(1), 87-116, DOI: http://dx.doi.org/10.1111/1745 9125.12030

Pratt, T. C. & Turanovic, J. J. (2015). Lifestyle and routine activity theories revisited: The importance of "risk" to the study of victimization. *Victims & Offenders, 11*(3), 335-354. doi:10.1080/15564886.2015.1057351

Purohit, B. & Singh, P. P. (2013). Data leakage analysis on cloud security. *International Journal of Engineering Research and Applications, 3*(3), 1311-1316. doi:10.1.1.418.9020&rep=rep1&type=pd

Pussewalage, H. S. G. & Oleshchuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management, 36*(6), 1161-1173. doi:10.1016/j.ijinfomgt.2016.07.006

Pyrooz, D. C., Decker, S. H., & Moule, R. K. (2015). Criminal and routine activities in online settings: Gangs, offenders, and the Internet. *Justice Quarterly, 32*(3), 471-499. doi:10.1080/07418825.2013.778326

Raeburn, T., Schmied, V., Hungerford, C., & Cleary, M. (2015). The contribution of case study design to supporting research on Clubhouse psychosocial rehabilitation. *BioMed Central Research Notes, 8*(1), 1-7. doi:10.1186/s13104-015-1521-1

Rajaraman, V. (2014). Cloud computing. *Resonance, 19*(3), 242-258. doi:10.1007/s12045-014-0030-1

Ralph, P. (2014). Evaluating process theories in software engineering. *Proceedings of the 3rd SEMAT Workshop on General Theories of Software Engineering - GTSE 2014*, 5-8. doi:10.1145/2593752.2593754

Rani, B. K., Rani, B. P., & Babu, A. V. (2015). Cloud computing and inter-clouds – types, topologies and research issues. *Procedia Computer Science*, *50*, 24-29. doi:10.1016/j.procs.2015.04.006

Rao, R. V. & Selvamani, K. (2015). Data security challenges and its solutions in cloud security. *Procedia Computer Science*, *48*, 204-209. doi:10.1016/j.procs.2015.04.171

Rasheed, H. (2014). Data and infrastructure security auditing in cloud computing environments. *International Journal of Information Management*, *34*(3), 364-368. doi:10.1016/j.ijinfomgt.2013.11.002

Raymond-Choo, K. & Grabosky, P. (2013). Cybercrime. *Oxford Handbooks Online*, 1-31. doi:10.1093/oxfordhb/9780199730445.013.003

Reyns, B. W. (2015). A routine activity perspective on online victimisation. *Journal of Financial Crime*, *22*(4), 396-411. doi:10.1108/jfc-06-2014-0030

Reyns, B. W., & Henson, B. (2015). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*, *60*(10), 1119-1139. doi:10.1177/0306624x15572861

Reyns, B. W., Henson, B., & Fisher, B. S. (2015). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine

activity theory as it applies to online forms of victimization. *Journal of Contemporary Criminal Justice, 32*(2), 148-168. doi:10.1177/1043986215621378

Richardson, J. D., Hudspeth Dalton, S. G., Shafer, J., & Patterson, J. (2016). Assessment fidelity in aphasia research. *American Journal of Speech-Language Pathology*, *25*(4S), S788-S797. doi:10.1044/2016_ajslp-15-0146

Rid, T. & Buchanan, B. (2014). Attributing cyberattacks. *Journal of Strategic Studies*, *38*(1-2), 4-37. doi:10.1080/01402390.2014.977382

Rimando, M., Brace, A., Namageyo-Funa, A., Parr, T. L., Sealy, D., Davis, T. L., … Christiana, R. W. (2015). Data collection challenges and recommendations for early career researchers. *Qualitative Report*, *20*(12), 2025-2036. Retrieved from http://nsuworks.nova.edu/tqr/vol20/iss12/8

Rizvi, S. (2016). The essential aspects of building a therapeutic relationship. *Indian Journal of Positive Psychology*, *7*(3), 359-361. Retrieved from http://www.iahrw.com/index.php/home/journal_detail/19#list

Rohrmann, C. A., & Cunha, J. F. S. R. (2015). Some legal aspects of cloud computing contracts. *Journal of International Commercial Law and Technology*, *10*(1), 37-45. Retrieved from www.jiclt.com

Roy, B. (2016). Cyber security for virtual clinics. *Engineering & Technology Reference, 1*(1), 1-6. doi:10.1049/etr.2015.0125

Ruetzler, T., Taylor, J., Reynolds, D., Baker, W., & Killen, C. (2012). What is professional attire today? A conjoint analysis of personal presentation

attributes. *International Journal of Hospitality Management, 31*(3), 937-943. doi:10.1016/j.ijhm.2011.11.001

Ryan, J. (2013). Book Review: Karin Olson, Essentials of Qualitative Interviewing *Qualitative Research, 13*, 254. doi:10.1177/1468794112450832

Safa, N. S. & Solms, R. V. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442-451. doi:10.1016/j.chb.2015.12.037

Salah, K., Calero, J. M. A., Zeadally, S., Al Mulla, S., & Alzaabi, M. (2013). Using cloud security to implement a security overlay network. *IEEE Security & Privacy, 11*(1), 44-53. doi:10.1109/msp.2012.88

Santos, A., Macedo, J., Costa, A., & Nicolau, M. J. (2014). Internet of things and smart objects form health monitoring and control. *Procedia Technology, 16*, 1351-1360. doi:10.1016/j.protcy.2014.10.152

Santos, F. M. & Eisenhardt, K. M. (2004). Multiple case study. In *the Sage encyclopedia of social science research methods* (pp. 685-687). doi:10.4135/9781412950589.n596

Schniederjans, D. G. & Hales, D. N. (2016). Cloud security and its impact on economic and environmental performance: A transaction cost economics perspective. *Decision Support Systems, 86*, 73-82. doi:10.1016/j.dss.2016.03.009

Shaikh, R. & Sasikumar, M. (2015). Data classification for achieving security in cloud computing. *Procedia Computer Science, 45*, 493-498. doi:10.1016/j.procs.2015.03.087

Shannon, P. & Hambacher, E. (2014). Authenticity in constructivist inquiry: Assessing an elusive construct. *Qualitative Report, 19*(52), 1-13. Retrieved from http://nsuworks.nova.edu/tqr/vol19/iss52/3

Simou, E., & Koutsogeorgou, E. (2014). Effects of the economic crisis on health and healthcare in Greece in the literature from 2009 to 2013: A systematic review. *Health Policy, 115*(2-3), 111-119. doi:10.1016/j.healthpol.2014.02.002

Sindhuja, P. N. (2014). Impact of information security initiatives on supply chain performance. *Information Management & Computer Security*, *22*(5), 450-473. doi:10.1108/imcs-05-2013-0035

Singh, N. & Khurmi, S. S. (2015). Malware analysis, clustering and classification: A literature review. *International Journal of Computer Science and Technology*, *6*(1), 68-74. doi:10.4236/jis.2014.52006

Smith, J., & Noble, H. (2014). Bias in research. *Evidence Based Nursing, 17,* 100-101. doi:10.1136/eb-2014-101946

Soltani, E., Ahmed, P. K., Liao, Y. Y., & Anosike, P. U. (2014). Qualitative middle-range research in operations management: The need for theory-driven empirical inquiry. *International Journal of Operations & Production Management*, *34*(8), 1013-1027. doi:10.1108/IJOPM-11-2012-0486

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225. doi:10.1016/j.ijinfomgt.2015.11.009

Sotiriadou, P., Brouwers, J., & Le, T. (2014). Choosing a qualitative data analysis tool: a comparison of NVivo and Leximancer. *Annals of Leisure Research*, *17*(2), 218-234. doi:10.1080/11745398.2014.902292

Spoorthy, V., Mamatha, M., & Kumar, B. S. (2014). A survey on data storage and security in cloud computing. *International Journal of Computer Science and Mobile Computing*, *3*(6), 303-314. Retrieved from http://www.ijcsmc.com/docs/papers/June2014/V3I6201444.pdf

Stern, C., Jordan, Z. & McArthur, A. (2014). Developing the review question and inclusion criteria. *The American Journal of Nursing*, *114*(4), 53–56. doi:10.1097/01.NAJ.0000445689.67800.86

Subramanian, N., Abdulrahman, M. D., & Zhou, X. (2014). Integration of logistics and cloud computing service providers: Cost and green benefits in the Chinese context. *Transportation Research Part E: Logistics and Transportation Review*, *70*, 86-98. doi:10.1016/j.tre.2014.06.015

Sultan, N. (2014). Making use of cloud computing for healthcare provision: Opportunities and challenges. *International Journal of Information Management*, *34*(2), 177-184. doi:10.1016/j.ijinfomgt.2013.12.011

Svensson, L. & Doumas, K. (2013). Contextual and analytic qualities of research methods exemplified in research on teaching. *Qualitative Inquiry*, *19*, 441-450. doi:10.1177/1077800413482097

Tan, D. J. J., Chua, T., & Thing, V. L. L. (2015). Securing android: A survey, taxonomy, and challenges. *ACM Computing Surveys*, *47*(4). doi:10.1145/2733306

Taylor, G., McNeill, A., Girling, A., Farley, A., Lindson-Hawley, N., & Aveyard, P. (2014). Change in mental health after smoking cessation: systematic review and meta-analysis. *British Medical Journal, 348*(1151), 1-22. doi:10.1136/bmj.g1151

Teixeira, A., Shames, I., Sandberg, H., & Johansson, K. H. (2015). A secure control framework for resource-limited adversaries. *Automatica, 51,* 135-148. doi:10.1016/j.automatica.2014.10.067

Thamhain, H. J. (2014). Assessing the effectiveness of quantitative and qualitative methods for R&D project proposal evaluations. *Engineering Management Journal, 26*(3), 3-12. doi:10.1080/10429247.2014.11432015

The Office of the National Coordinator for Health Information Technology (ONC). (2016). Permitted uses and disclosures: Exchange for health care operations. *US Department of Health and Human Services*. 1-4. Retrieved from https://www.healthit.gov/sites/default/files/exchange_health_care_ops.pdf

Thilakanathan, D., Chen, S., Nepal, S., Calvo, R., & Alem, L. (2014). A platform for secure monitoring and sharing of generic health data in the cloud. *Future Generation Computer Systems, 35*, 102-113. doi:10.1016/j.future.2013.09.011

Tiira, K. & Lohi, H. (2014). Reliability and validity of a questionnaire survey in canine anxiety research. *Applied Animal Behaviour Science, 155*, 82-92. doi:10.1016/j.applanim.2014.03.007

Timande, N., Chandak, M. B., & Kamble, M. (2014). Document clustering with feature selection using Dirichlet process mixture model and Dirichlet multinomial allocation model. *International Journal of Engineering Research and*

Applications, 10-16. Retrieved from https://pdfs.semanticscholar.org/6a0f/2d593688780a73e12e171ee157bb94b037cc.pdf

Tobin, M., Nugroho, D., & Lietz, P. (2016). Large-scale assessments of students' learning and education policy: Synthesising evidence across world regions. *Research Papers in Education*, *31*(5), 578-594. doi:10.1080/02671522.2016.1225353

Tong, A. & Dew, M. A. (2016). Qualitative research in transplantation. *Transplantation, 100*(4), 710-712. doi:10.1097/tp.0000000000001117

Tran, V., Porcher, R., Falissard, B., & Ravaud, P. (2016). Point of data saturation was assessed using resampling methods in a survey with open-ended questions. *Journal of Clinical Epidemiology*, *80*, 88-96. doi:10.1016/j.jclinepi.2016.07.014

Tseloni, A., & Pease, K. (2014). Area and individual differences in personal crime victimization incidence. *International Review of Victimology*, *21*(1), 3-29. doi:10.1177/0269758014547991

Tu, M., Spoa-Harty, K., & Xiao, L. (2015). Data loss prevention and control: Inside activity incident monitoring, identification, and tracking in healthcare enterprise environments. *Journal of Digital Forensics, Security and Law*, *10*(1), 27-44. doi:10.15394/jdfsl.2015.1196

Turner, P., & Thompson, E. (2014). College retention initiatives meeting the needs of millennial freshman students. *College Student Journal, 48*(1), 94-104. Retrieved from https://eric.ed.gov/?id=EJ1034162

United States Department of Health and Human Services. (1979). *The Belmont report*. Retrieved from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. *Journal of Nursing Education and Practice*, *6*(5), 100-110. doi:10.5430/jnep.v6n5p100

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2015). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice, 32*(2), 169-188. doi:10.1177/1043986215621379

Vale, L. J. (2014). The politics of resilient cities: whose resilience and whose city? *Building Research & Information, 42*(2), 191-201. doi:10.1080/09613218.2014.850602

Van Kesteren, J. (2016). Assessing the risk and prevalence of hate crime victimization in Western Europe. *International Review of Victimology, 22*(2), 139-160. doi:10.1177/0269758015627046

Vecchio, J. M. (2013). Once bitten, thrice wise: The varying effects of victimization on routine activities and risk management. *Deviant Behavior, 34*(3), 169-190. doi:10.1080/01639625.2012.726167

Vohra, V. (2014). Using the multiple case study design to decipher contextual leadership behaviors in Indian organizations. *The Electronic Journal of Business Research Methods*, *12*(1), 54-65. Retrieved from http://ejbrm volume12 issue1-article334%20(2).pdf

Wang, W. & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. *Computer Networks*, *57*(5), 1344-1371. doi:10.1016/j.comnet.2012.12.017

Weber, V., & Carblanc, A. (2014). Cloud computing: The concept, impacts and the role of government policy. *OECD Digital Economy Papers*, 34. doi:10.1787/5jxzf4lcc7f5-en

Welch, D., Grossaint, K., Reid, K., & Walker, C. (2014). Strengths-based leadership development: Insights from expert coaches. *Consulting Psychology Journal: Practice and Research*, *66*(1), 20-37. doi:10.1037/cpb0000002

Whittemore, A. H. (2014). Phenomenology and city planning. *Journal of Planning Education and Research*, *34*(3), 301-308. doi:10.1177/0739456x14536989

Williams, M. L. (2015). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology*, *56*(1), 21-48. doi:10.1093/bjc/azv011

Wolfe, S. E., Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2016). Routine cell phone activity and exposure to sext messages: Extending the generality of routine activity theory and exploring the etiology of a risky teenage behavior. *Crime & Delinquency*, *62*(5), 614-644. doi:10.1177/0011128714541192

Yang, Z., Sun, J., Zhang, Y., & Wang, Y. (2015). Understanding SaaS adoption from the perspective of organizational users: A tripod readiness model. *Computers in Human Behavior, 45,* 254-264. doi:10.1016/j.chb.2014.12.022

Yfanti, F., & Sipitanou, A. A. (2016). The importance of involving nurses in continuing education programs. *European Journal of Education Studies*, *2*(12), 82-90. Retrieved from http://ozelacademy.com/ejes.htm

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education*, *48*(2), 311-325. doi:10.1111/ejed.12014

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). Thousand Oaks, CA: Sage

Younis, Y. A., Kifayat, K., & Merabti, M. (2014). An access control model for cloud computing. *Journal of Information Security and Applications, 19*(1), 45-60. doi:10.1016/j.jisa.2014.04.003

Yüksel, Buket, et al. "Research issues for privacy and security of electronic health services." *Future Generation Computer Systems*, vol. 68, 2017, pp. 1-13. doi:10.1016/j.future.2016.08.011

Zamawe, F. (2015). The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal*, *27*(1), 13-15. doi:10.4314/mmj.v27i1.4

Zang, W. L. (2014). Research of information security quantitative evaluation method. *Applied Mechanics and Materials, 513*(517), 369-372.

doi:10.4028/www.scientific.net/amm.513-517.369

Zota, R. D. & Petre, I. A. (2014). An overview of the most important reference architectures for cloud security. *Informatica Economica*, *18*(4/2014), 26-39. doi:10.12948/issn14531305/18.4.2014.03

Appendix A: National Institute of Health Office of Extramural Research

Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **Lamonte Tyler** successfully completed the NIH Web-based training course "Protecting Human Research Participants".

Date of completion: 09/10/2015

Certification Number: 1837821

Appendix B: Introductory E-mail to Participants

Hello Mr. XXXXX,

I'm working on my doctorate degree in information technology at Walden University. I'm studying “Exploring the Implementation of Cloud Security to Minimize Electronic Health Record (EHR) Cyberattacks”. Cyber is derived from cybernetics and cybersecurity is a state of being protected against the criminal or unauthorized use of electronic data. Cybercrime in healthcare can potentially upset the trust of the facility in perspective to the relationship with the patient.

I'm searching for an organization with a development staff of at least 4-10 people to participate in my study. These people could be a combination of developers, testers, analysts, managers, etc. within the organization. They do not need to be on the same team. The study would involve a short one-on-one interview with each person and a review of any documentation involving cloud security. All information about the organization and participants is confidential and not made public in any way. My study would simply refer to "the organization", "participant 1", etc. A confidentiality agreement can be provided. A copy of my study results will be provided to the organization.

Sincerely,

Lamonte Bryant Tyler

Appendix C: Interview Protocol

Interviewee (Title): _____

Interviewer: _____Lamonte Bryant Tyler_____

Background:

_____ A: Interviewee Background

_____ B: Demographics

Other Topics Discussed: _____

_____

Documents Obtained: _____

_____

Post Interview Comments or Leads:

_____

Introductory Protocol

To facilitate our note-taking, we would like to audio tape our conversations today. For your information, only researchers on the project will be privy to the tapes which will be eventually destroyed after they are transcribed. Essentially, this document states that: (1) all information will be held confidential, (2) your participation is voluntary, and you may stop at any time if you feel uncomfortable, and (3) we do not intend to inflict any harm. Thank you for your agreeing to participate. I have planned this interview to last no longer than 45 minutes. During this time, I will have several questions that I would like to cover.

Introduction

You have been identified as someone who has a great deal to share about Cyber Security. My research project as a whole focus on the implementation to minimize against EHR cyber security. My study does not aim to evaluate your techniques or experiences. Rather, I am trying to learn more about your strategies against EHR cyberattacks.

A. Interviewee Background

How long have you been …?

_____ in your present position?

_____ at this medical facility?

B. Demographics

Post Interview Comments and/or Observations:

Appendix D: Interview Questions

Demographic Questions

1. What is your role within your organization and do you have a team whose focus is primarily cloud security?
2. Describe the architecture of your EHR. Include if you have your cloud or use the third-party vendor. Describe the responsibility of a third-party vendor if applicable. What is your role in keeping EHR secure?

Interview Questions

1. What strategies have you used to implement cloud security to minimize EHR cyberattacks?
2. What are the challenges that you face that affect the security of patient EHR in the cloud?
3. What do you see as being the greatest motivation for those who wish to infringe on the facilities EHR?
4. How do you maintain the security of the EHR in the cloud?
5. What tools do you use to provide security of EHRs in the cloud? How do you use the tools? What do you do when vulnerability is identified?
6. What metrics do you use to assess the level in which the EHR is secure, at what frequency do you review these metrics, and who are these metrics reviewed with?
7. What is your role if a breach of the entire system is identified?
8. What is your role in the forensics of an identified breach of EHR as a suitable target for a cyberattack?