THE ROLE OF NEUTRALIZATION TECHNIQUES AND ORGANIZATIONAL FACTORS IN INFORMATION PRIVACY POLICES VIOLATION

SAAD ALTAMIMI

SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF
Doctor of Philosophy

SCHOOL OF COMPUTING SCIENCE

COLLEGE OF SCIENCE AND ENGINEERING
UNIVERSITY OF GLASGOW

OCTOBER,2016

Abstract

This is a dissertation outline using the style guidelines defined by the University of Glasgow.

Dedication. (Is what you need.)

Table of Contents

List of Tables

List of Figures

Chapter 1

First Year report

1.1 Introduction

1.2 Literature Review:

In this section, I have explored several relevant works and articles related to healthcare security, which is my research interest. The main objective is to get deeper insights of information technology trends, and their associated security challenges and opportunities in the healthcare industry. Specifically, how these technologies can harm or preserve patient information privacy.

1.2.1 Health Information Technologies (HIS):

Healthcare industry is considered one of the most sophisticated businesses that interacts with a complex network of entities. Therefore, the use of information and communication technologies (ICT) in the healthcare sector has become imperative to support the activities of healthcare organisations. Hospitals often collect huge amounts of data to support their daily medical activities, as well as financial and managerial transactions, which have grown rapidly. Data at hospitals is generated from several sources, including patients, insurance companies, labs,pharmacy, etc. Thus, the management of such huge amounts of data requires an effective IT solutions that can satisfy many critical requirements such as easily accessible, cost-effective, reliable services and high quality.

The need for technological advancements to improve healthcare services delivery, quality and performance have attracted the industry stakeholders to implement several health information technologies. ISO 27799:2016 has defined Health Information Systems (HIS) as " *a repository of information regarding the health of a subject of care in computer-processable*

form, stored and transmitted securely, and accessible by multiple authorised users" [23]. Another definition of the HIS is based on the fact that it is a computer program, which includes " a set of standards based on healthcare diagnosis, symptoms, cause, healthcare target and measurements" [37]. The adoption of HIS have improved the compliance with the health care standards and disease control, which affect the overall quality delivery of healthcare services. Also, the implementation of clinical decision support tools have improved the diagnoses efficiency, which as a result have reduced significantly the total rate and time of healthcare utilisation. [11, 4].Currently, many healthcare organizations are utilizing the HIS as a backbone of their operational services because it ability to be integrated with hospital clinical care and administrative systems[44].

In this direction, several health information systems (HIS) have impacted positivity healthcare organisations such as E-Health, Electronic Mealth Records (EMR), Mobile health (mHealth), and Telemedicine, cloud computing in healthcare, big data analysis, health exchange and health sensing [60, 61].

1.2.2 Electronic Medical Records (EMRs) systems:

The Electronic Medical Records(EMR) replaced paper-based charts in hospitals and medical clinics to an electronic version that may allow the patient information to be integrated, transmitted, stored and shared in different systems and locations [44]. It is difficult to find a stander definition for the EMR because the same meaning may refer to another term based on the perception of the EMR in a country or a healthcare sector.Thus,the EMR is considered a synonymous with abbreviations used elsewhere such as Electronic Health Records(EHR)[60, 44, 1], CPR (Computerized Patient Record),Protected Health Records (PHI) or Personal Health Records (PHR). In the other hand, several scholars have provided definitions that differentiated between those terms EMR, EHR and PHR [27, 16] . According to [61, 55], three main differences of those terms as the following:

- **Electronic Medical Record (EMR):** a health organisation is responsible to generate and control the EMR. Each EMR is a legal and digital record that includes all the patient medical history during inpatient and outpatient visits. Basically, the EMR data are used for diagnoses purposes and shared locally within one health organization or institution[61].

- **Electronic Health Record (EHR):** several health organisations are responsible to create,collect and maintain EHR data that are related to the patient healthcare.Thus, the EHR may includes more comprehensive information as many sources contribute to it. Each EHR can be shared across different healthcare members , providers, regions, etc. When the EMR data are exchanged with external health organizations or entities, then

they are considered EHR data and the EMR will be the main source of the transferred EHR[61].

- **Personal Health Record (PHR)**: Each PHR record contains the same amount of EHR information, but the PHR data can be managed and accessed by individuals[61, 55].

The World Health Organization (WHO) [60] describes the Electronic Health Record systems (EHRs) as " real-time, patient-centred records that provide immediate and secure information to authorized users. EHRs typically contain a patients medical history, diagnoses and treatment, medications, allergies, immunizations, as well as radiology images and laboratory results". Another report [59] stated that the implementation of the clinical decision tools, laboratory and pharmaceutical systems in poor African country such as Kenya, have reduced the practitioners errors and have enhanced both healthcare diagnoses and follow-up services. According to [36], the implementation of EMR has provided healthcare organizations with significant advantages and can gain one or more of the following benefits:

- **Better quality of care:** the EMR has improved the concept of information exchanging between doctors, healthcare team members and departments as well as off-site health providers. As a result, the patient information can be accessed easily if a patient needs an emergency care or requires a specific medication. Like any computer system, the system administrators can make a full backup of the EMR, which can decrease the risk and cost of losing data if a disaster accrued [36].

- **Improved care efficiency:** the EMRs is receiving data from different health information systems, so the patient information can be modified from different sources and locations. This means that the patient data are available to several health practitioners, and each of them can communicate through the EMR. Thus, it can give doctors a simple way to review the patient medical history or request a specific test or task from others. Such communications way can reduce the side effects of repeating some medical procedures such as X-rays as well as the time and cost associated with it [36].

- **Improved care convenient:** the patient history can be exchanged and accessed easily, which are the basic principles of the EMR. So, no need of physical carriage for the paper records or filling more paper forms, which in return can reduce the waiting time for both the patients and doctors to receive or review the medical records[36].

1.2.3 Mobile Health (mHealth):

TBD

1.2.4 Cloud computing in Healthcare

Cloud computing is one of the newest IT paradigms, which emerged in 2007, and it allows customers to use many advanced IT services and resources through the internet at the cloud service providers data centre [50]. According to Buyya et al. [10], the importance of cloud computing will increase and soon be considered a fifth utility after water, gas, electricity, and telephone. Using a pay-per-use model, several organisations can improve their business services and IT functions performance, efficiency and quality, by paying for what they are using of the IT resources and services [2]. Virtualization, utility computing, grid computing and internet services are the fundamental concepts of the cloud computing evolution. Thus, cloud technology is considered a solution that is applying new forms of IT outsourcing [52, 12].

There is not a universal definition or clear description for cloud computing, and according to some studies, there are more than 22 definitions for it [50]. The ISO/IEC 17788 defines cloud computing as "Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand". According to [9], Cloud computing consists of seven services categories: Communications as a Service (CaaS), Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Network as a Service (NaaS), Compute as a Service (CompaaS), Data Storage as a Service (DSaaS)and Infrastructure-as-a-Service (IaaS). These categories required several cloud deployment models to organise, control and share the physical and virtual resources such as the following:

- **Public cloud**: it is a cloud deployment model, where the cloud service provider keeps the cloud services on premises and has full control on all physical and virtual resources related to the services[9].
- **Private cloud:** it is a cloud deployment model, where a single cloud service customer accesses the cloud services exclusively and has a control on all resources related to the services [9].
- **Community cloud**: it is a cloud deployment model, where a small number of cloud service customers access the cloud services exclusively, and at least one of customers can control resources, and it may exist on or off premises[9].
- **hybrid cloud:** it is a combination of two cloud deployment models, where appropriate technologies are in place to ensure the cloud services interoperability. A hybrid cloud may exist in or off premises and can be owned, operated and managed by a third party or an organisation itself[9].

In the healthcare industry, cloud computing has many promises. Due to the complexity of hospital information systems (HIS), cloud computing is a solution that opens a new horizon for patients records to be accessible via a secure authentication by authorised healthcare providers[18].Also, it will help healthcare providers to gain important cost reductions and save money that is usually spent in buying and maintaining the needed hardware and software [3, 33].

However, many organisations in different industries worldwide are still not ready to adopt cloud computing services. According to a recent report [32], the healthcare cloud computing market is predicted to grow nearly 9.48 billion dollars between 2015 to 2020, and only 4 percent of prospective cloud customers are healthcare organisations.The reasons for low adoption of cloud computing technology in healthcare industry are attributed to security and privacy fears, IT regulations compliance burdens, resource control and vendor lock-in concerns, as well as the lack of understanding of the technological, organisational and environmental factors that affect the decision makers when considering such technological shift [32, 54].

1.2.5 Internet of Thing (IoT) in Healthcare

1.2.6 Information Security Managment(ISM) In Healthcare:

Nowadays, Information and Communication Technologies (ICT) an important success factor within any modern society. Many new technologies have emerged and have improved people lives and organizations services including governments, worldwide. The significant shift in the business environment, economic instability, and customers desires and expectations, increase the need to develop and adopt new IT innovations. Over the last decades, several strategic transformations in enterprises and the governmental sectors are based on ICT applications, which brought a lot of benefits. Consequently,the need for Information Security (InfoSec) becomes an essential matter as thousands of organizations worldwide are heavily dependent on information process systems to perform their daily tasks. Thus, it is a critical role to ensure that the information technology assets are secured and protected against IT threats. Many scholars have defined ”information security” from different perspectives as it includes multidimensional factors that are concentrated on the preservation and protection of information assets via the implementation of security technical,operational and physical controls [19, 42]. While those controls need to be improved, reviewed and monitored in regular bases to ensure that the organizations' business and security objectives are achieved[24].

The national institute of Standard and Technology (NIST)[30] has defined information security as ”the protection of information and information unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity,

and availability ". Zafar and Clark [62], they incorporate more components to InforSec definition in order gain a holistic view. These components are: establishing security policies and procedures, understanding and assessing potential security threats and risks, implementing and monitoring security controls, educating and training personnel in security awareness, performing permanent technology assessment and integrating information security governance. Information security mainly aims to preserve information confidentiality, unauthorised integrity and availability, which is known as (CIA) security triad[40].Also [24] adds authenticity, accountability, non-repudiation and reliability . According to European Network and information Security Agency (ENISA)[17],information confidentiality means "The protection of communications or stored data against interception and reading by unauthorized persons" . Integrity is refereed to "The confirmation that data which has been sent, received, or stored are complete and unchanged." Availability is defined as "The fact that data is accessible and services are operational".

The sensitive nature of health information over other personal information and the growth rate of dependency on health care information systems, have increased the need to robust information Security Management (ISM). If patients' information has been compromised, then the health organisation may suffer from lots of legal issues, which may turn to financial losses as well as a huge damage to the organisation reputation. Furthermore,the HIS now have been shifted from stand-alone system with specific end-users to includes patients at homes via the internet. This development in network and information exchange technologies have increased the type and capacity of the HIS threats and challenges.Such development in network and information exchange technologies have increased the type and capacity of the HIS threats and challenges [21]. In response to these security risks, initiatives from several countries and institutions have been launched to improve ISM practices, procedures and guidelines by developing many generic and specific security standards. These standards aim to help the organisations in several industries to utilise their resources and efforts efficiently in order to gain an adequate security level via the adoption of best security practices [44, 4].

Akowuah et al. [4] in their literature survey have reviewed several security standards including NIST Special Publication 800-53 , HITRUST Common Security Framework (CSF), Control OBjective for Information and related Technology (COBIT), ISO/IEC27002:2005, ISO/IEC27001:2005, ISO27799:2008, ISO17090:2008,ISO/TS 25237:2008. [4] aim was to facilitate the choosing process for a suitable security standard that can guide information security management practices in the healthcare industry.In this survey, many standards were reviewed and analysed in order to assist IT management in their initial steps toward security programs implementation. Akowuah et al. [4] suggested that ISO 27799:2008 and its associated series ISO 17090:2008 and ISO/TS 25237:2008 were more suitable of all size organizations in the healthcare industry as they were tailored to handle various security aspects and technical issues within healthcare environment. Moreover, Health Information

Trust Allianc (HITRUST) is a specific health security standard that can satisfy many big size organizations security needs. It requires a subscription with HITRUST to get an access for health information security materials and training courses.In the other hand, some security standards such as NIST SP 800-53, ISO 27002:2005, and COBIT were more generic standards that provide holistic security approaches and procedures. Thus, they can be used as a alternative reference during the implementation of security programmes in the healthcare organizations[4].

1.2.7 Privacy In Healthcare:

One of the most important security concerns of adopting the HIS applications such as EMR is the patient information privacy [31]. In healthcare sector , information privacy is "*the ability of healthcare employees to control EMR during collection, maintaining the accuracy of EMR during manipulation, ensuring the confidentiality of EMR during transferring, and understanding the duration of EMR retention in the organisation.*" [44].The sensitive nature of the patient health information and the widespread usage of EMR/EHR in healthcare organisations have increased the fears related to security and privacy risks and vulnerabilities.Those security fears can originate from internal sources related to types of intentional and unintentional behavior such as employee ignorance, curiosity, misuse of password, social engineering, etc. External threats may include intruder and hacker attempts, malicious software, spy ware and viruses attacks [47]. A privacy breach is "*a situation where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirements*"[25].
Securing patient sensitive information from any security and privacy breaches is essential as any violation to these confidential information may harm both the individuals and organizations. If patient confidential information disclosed intentional or unintentional, the harm on the patient could include employment termination, loss of healthcare insurance, identity theft and embarrassment. On the other hand, the healthcare organisation may suffer from several losses including reputation and income, along with authorities penalty and a huge number of individuals lawsuit [58, 14].

In an effort to preserve the EHR integrity, confidentiality and availability from the potentials security and privacy breaches, many countries have conducted security laws and enforced compliance from all healthcare parties that store, process and exchange EHR electronically[21, 48, 44]. For instance, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the USA, the Personal Information Protection and Electronic Documents Act (PIPEDA Act) in Canada, the EU Cross-Border Health Care Directive 2011/24/EU1, Personal Data Protection Act (PDPA) in Malaysia and (Ley de Proteccin de Datos) law in Spain, etc [8, 57].

The aim of HIPPA, for example, is ensuring the confidentiality, availability and integrity of Protected Health Information (PHI), while being stored, exchanged and processed by any formats (electronic, on the document or oral) between one or several healthcare providers. The PHI include individuals' mental and physical health history, health providers information including bills and any other information that can reveal patient identity [57, 44, 5]. Moreover, the U.S. Department of Health and Human Services (HHS) produced the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) as a way to guide the actions during the implementation of (HIPAA). According to [57], the Pivacy Rule main objective " is to assure that individuals health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being ."
However, information privacy concerns and threats have been largely discussed by scholars and professionals as result of the enormous development in information technologies. The emerging technological trends such as social network, e-commerce, e-government, e-health, cloud computing, etc are based on the online services,thus, share common and several perspectives of security and privacy fears related to their operations and consumers. In healthcare context, a recent study by Papoutsi et al. [38] examined the perceptions of patient and public of security and privacy as a result of the widespread adoption of EHR in the UK. The authors used a sequence of research mix methods, a survey questionnaire and focus group discussions. The survey questioner was disseminated in General practices (GP)surgeries and NHS hospitals in West London, and a sample of 2761 participants was included in the final analysis including patients and members of the public.Then, a total of 17 focus group discussion were conducted, 13 of the focus groups with 114 patients having different health conditions and 4 of the focus groups with healthcare members including NHS managers, health researchers and professionals.The study found that the ability of the NHS for properly securing EHR was the main concern of 71% of the respondents. Almost 50% thought that the integrated EHRs would decrease the security level, in contrast, 43.3% believed that the security risks would not change. Moreover,78.9% of respondents unwillingness the idea of allowing their health information to be a part of national EHR system. Papoutsi et al. [38]study concluded that sharing information in wide scale via integrated EHR systems has raised patient and public concerns of security and privacy risks, therefore, more initiatives are required to increase public awareness and trustworthy security along with the establishment of stronger techniques for maintaining privacy.

Mahfuth et al. [31] conducted a systematic literature review with objectives to examine the security and privacy concerns and challenges related to the Electronic Health Record Systems (EMRs) within the healthcare industry. Another objective was identifying and analysing the current security solutions to overcome the confidentiality violation concerns as a result of EMRs adoption, which includes various range of security frameworks, con-

trols, and policies. The findings showed that there was an increasing rate of EMRs adoption in developed and developing countries worldwide. Therefore, seeking and maintaining an optimal level of the EMR privacy against unauthorized access was a serious security challenge for the healthcare team members, patients, IT experts and stakeholders. Mahfuth et al. [31] argued that the developing countries had greater privacy risks regarding EMRs than the developed. This is due to poor IT experience and infrastructure, insufficient security awareness level, and inadequate financial resource as well as the absence of clear security laws and regulations there. Moreover, the authors noted that the existing security solutions and policies insufficient to ensure a comprehensive protection of the EMR's health data privacy, which as a result may affect the healthcare Quality of Service (QoS) [31].

Rahim et al. [44] conducted a systematic literature review followed by a qualitative study.The aim was identifying and understanding healthcare employees perspective of Information Privacy Concerns(IPC) and its influential factors when using the EMR. Afterwards, nine interviews have been conducted in order to validate literature review findings with three groups from different backgrounds include HIS users, experts and legal professionals. The authors, based on the literature review and the quantitative study, have identified three factors that significantly influence IPC, which were privacy awareness, privacy policy and privacy risk.

As an effort to overcome privacy concerns, Bensefia and Zarrad [8] proposed a novel EMRs privacy layered Architecture model. It aimed to make a balance between maintaining the EMR privacy and at the same time ensuring EMR availability for other authorised health providers. Bensefia and Zarrad [8] model encompassed of three main layers, administrative decisions, the hardware infrastructure and technological issues. The administrative decisions layer includes security rules, regulations and standards to be satisfied from all healthcare parties. The hardware infrastructure includes all the physical types of equipment that were involved in handling EMR. The last layer was technological issues, which was responsible to distinguish the EMR sensitive data set from the common EMR information and then placed it to private database with restricting security access controls.Thus, this private database and it sensitive EMR data will be accesses and shared via a proxy server that can grant IP addresses to authorized clients.

Park et al. [39] proposed a research model to examine the relationship between Health Information Security Awareness (HISA), individuals characteristics and the intention of nursing students naive behaviour to disclose patients health information. In the model, HISA constitute of three awareness learning constructs General Information Security Awareness(GSA), Health Information Security Regulation Awareness (HRA) and Punishment Severity Awareness (PSA). The individual factors including personal norm and self-control are placed between the HISA and the nursing intention to disclose patient information. The model empirically tested through a survey questionnaire of 123 nursing students within an urban university in South Korea. Park et al. [39] study findings revealed that the GSA, HRA and

PSA were essential awareness learning elements to improve overall HISA and compliance with HIPPA. Moreover, the GSA, HRA and PSA positively affect individual personal norms and self-control, and as a consequence inhibiting deviant behaviour of nursing students to disclose patient information. Also, the study emphasised on the importance of upgrading information security awareness of nursing students by updating the education curriculum to include more detailed topics in security policies and practices in medical context.

1.3 Pilot study (First Year Experiment):

1.3.1 Introduction:

Several advanced security incidents have occurred and been largely explained and linked to technology problems; however, this traditional idea has refuted by many scholars and IT experts, who argue that technology-based solutions are not solely sufficient to mitigate or reduce various types of security threats [29, 6, 46]. Recently, humans' behaviour becomes a hot topic in the information security literature, which force organisations to adopt managerial and technical solutions that include implementing various security standards and polices to protect their IT assets and infrastructure. In this direction, the importance of compliance with information security policies has increased to govern security initiatives, specifically that is related to human behavior.

Siponen and Vance [49] and [43] reported that one of the critical security concerns within the organizations is the ability of employees to comply with the organization's information security policies.According to Ponemon Institute [41] survey, over 75% of data breach were linked directly or indirectly to employees' poor behaviors such negligence, maliciousness or ignorance and only 43% of IT security practitioners respondents believed that their technological countermeasures partially effective to protect their organization's sensitive and confidential data.Furthermore, [7] reported that 80% of the chief information security officers considered that employees non-compliance actions may harm their data more than outsider hackers .Thus, employees' intentional and unintentional violations of security policies consider as insider threats, which add more burden on the organizations to safeguard their IT infrastructure against the potential consequences of such acts. However, in effort to reduce information security violation as a common security issue, many scholars have provided reasons that explained why the formal and informal sanctions as well as awareness of polices and security education and training programs were not successful ways to prevent information security policies violation [49, 15, 13, 1].Thus, several security scholars argued that employees often utilized moral cognition or neutralization techniques to hinder the impact of punishment, guilt, policy and law enforcement or shame when they intend to commit crimes

or to misuse or violate security polices [49, 7, 53, 51, 29, 20, 22].

1.3.2 Study Background:

In healthcare industry, hospitals collect, store and process various types of medical data that related to the patients' health status and treatments. According to HIPPA, patient EMR can be accessed by several covered entities such as physicians, nurses, administrative, researchers, etc for justifiable purposes.Thereby,those personnels with EMR access privileges must comply with the Privacy Rule to protect patient's EMR integrity, privacy and confidentiality against any internal or external threats.Poor compliance from health care personnels with the security regulations and organization information security policies may lead to EMR misuse, losses,and leakage.

Kamoun and Nicho [26] argued that despite all the physical, technical and administrative controls and security laws, human behavior was the main reason behind serious data breach incidents in health care organizations, which accidentally or intentionally compromised information security and patient privacy. Based on Human Error Theory,Kamoun and Nicho [26] categorized healthcare employee errors to slip, lapse, mistake, routine/situational violation, optimizing violation.In addition,employees negligence , carelessness and the misuse of access privileges were the sources for several data breach incidents in healthcare organizations.According to [26], between 2008 and 2011, 102 healthcare employees have been discharged from National health Service and trust(NHS) in the UK as a result of 806 data breach incidents.Some of these incidents include sharing Patient Health Information (PHI) in the social networks (23 incidents), and forget unencrypted PHI or theft (57 incidents).furthermore, 41% of major healthcare data breaches in Europe were due to healthcare employees negligence and carelessnesses when handling or dealing with PHI[28, 26]. Table 1 presents a total of 277 reported incidents, causes and the number of affected individuals after major data breaches. These security incidents have occurred in healthcare organisations in the US and have compromised patient health information(PHI) privacy for more than 500 individuals between 2013 to 2014.

Table1.Data breaches involving more than 500 individuals in the USA [56]

Cause	*Number of Incidents Reported*	*Number of Affected Individuals*
Theft of electronic equipment/portable devices or paper containing PHI	**105**	**6,615,929**
Unauthorized access or disclosure of records containing PHI	**72**	**6,976,208**
Loss of electronic media or paper records, containing PHI	**21**	**174,074**
Hacking/IT incident of electronic equipment or a network server	**50**	**7,144,137**
Other causes of breaches of PHI	**16**	**318,296**
Improper disposal of PHI	**13**	**116,596**

Medical interns is

1.3.3 Study problem:

In healthcare sector, there is a rare knowledge about how neutralization techniques are utilized by medical interns in the Saudi's hospitals as they have access privileges to the patient's Electronic Medical Records (EMR). Also, a little is known to which extent neutralization techniques can participate in the violation intention of privacy polices during medical internship period.This empirical study aims at bridging the gap in the literature by considering and evaluating the current security awareness of medical interns in Saudi hospitals and to which extent they adhere to the hospital's policies that are existed to protect patients information privacy. Furthermore, the role of the neutralization techniques on the hospitals' security posture and the ability of these techniques to predict medical interns' intention to violate patient privacy.

1.3.4 Theoretical Background:

Neutralisation Theory:

In 1957, Techniques of Neutralization was firstly introduced by Sykes and Matza [51] in criminology field in order to understand juvenile delinquency. According to [45], Neutralization is "a method whereby an individual renders behavioural norms inoperative,thereby

freeing himself to engage in behaviour which would otherwise be considered deviant." The theory postulated that offenders employed one or more techniques as defence mechanisms to justify their deviant behaviour prior or after they committed a violence or crime, thereby they convince them self that their deviant behaviour is acceptable regardless of social norm principles [53].In their original work, Sykes and Matza [51]have proposed five neutralisation (rationalisation) techniques that juvenile criminals may use to explain their deviant behaviour.

- **The Denial of responsibility:** The centre principle of this technique is that the offender refuse to accept the blame of his/her deviant behaviour and redirect the responsibility of action in question to alternative source.Here, the offender may claim that his/her deviant behaviour had occurred due to accident or lack of control[51].
- **The Denial of Injury:** the offender considers that the result of his/her potential deviant action is harmless, thus, no worry that anyone could get hurt badly if he/she engaging in it[51].
- **The denial of a victim:** the offender claims that the injury resulted from the deviant action is a kind of rightful punishment or retaliation as the victim deserve his/her action consequences[51].
- **The condemnation the condemner:** In this techniques, the offender tend to develop "a rejection of the rejectors" and "shifts the focus of attention from his own deviant acts to the motives and behaviour of those who disapprove of his violations. His condemners, he may claim, are hypocrites, deviants in disguise, or im subtle alchemy the delinquent moves him impelled by personal spite."[51].
- **The appeal to higher loyalty:**The offender employed this neutralization technique in order to escape a dilemma that force him/her to choose between confronting with small group interests such as friends, family members, etc or violating a law[51].

Later on, criminology scientists Rogers and Buffalo [45] and Minor [34] introduced two techniques as extensions to Sykes and Matza [51] theory, which are:

- **Metaphor of the ledger:** the offender argues that his/her previous good acts and rules compliance recompense his/her occasional wrongdoing behaviourRogers and Buffalo [45].
- **Defense of necessity:** Here, the offender argues based on the idea that nobody should feel shame or guilt if the situation requires an act that can result breaking rules[34].

In the information security context Siponen and Vance [49]conducted an empirical study, and they argue that the employee intention to violation information security policies can be explained by neutralisation factors. The study proposed a theoretical model to test the impact of formal and informal sanctions along with shame on the employee violation intention and the effect of neutralisation factors to rationalise such behaviour. The finding revealed that the organization sanctions alone were not enough to decrease or prevent information policies violation intention as the employees tend to utilise neutralisation techniques to minimise the perceived harm of sanctions. Based on the findings, authors suggested that the management should consider the importance of neutralisation factors during their efforts to develop and implement information security policies and security awareness champagnes.

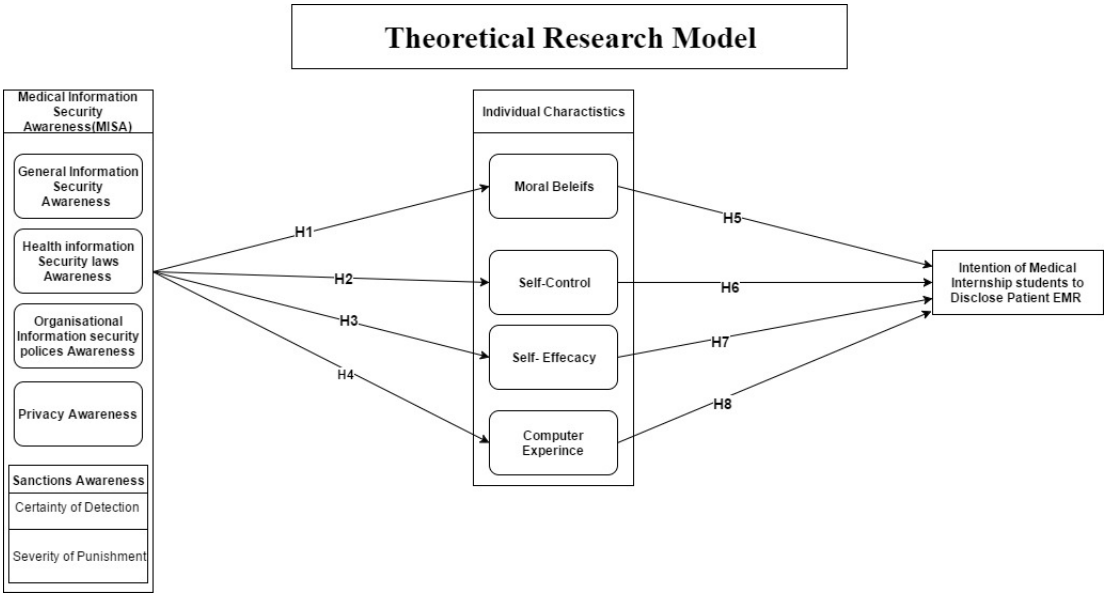
Further empirical study in Malaysia by Teh et al. [53], aimed to investigated the organizational factors that influence employees neutralization behavior toward information security polices violations. The study model contains four main factors include role conflict and role ambiguity from the security literature as well as tow factors drawn form social exchange theory, which were job satisfaction and organizational commitment. A total sample of 246 employees, working in nine Malaysian banks, participated in this study. The results showed that role conflict had a positive influence on employees neutralization techniques toward ISP violation. In contrast , organization commitment, job satisfaction and role ambiguity had insignificant affect on neutralization techniques toward information security policy violation.

Another empirical study byKim et al. [29] proposed an integrative behavioural model based on theory planned behaviour, protraction motivative theory and rational choice theory from social psychology science and neutralization theory from criminology field. The goal was to understand the behavioural factors that affected the employee actions toward compliance with organization information security polices. The authors used survey disseminated to 32 companies within 10 industries and a sample of 194 participants was collected. The results showed that neutralization techniques significantly weaken employee intention toward information security policies compliance. Also, response efficacy and normative beliefs positively impacted employees' intention to comply with the organization's security policies.

Morris and Higgins [35] examined digital piracy as an illegal behaviour via several theories applied in criminology field. Using retrospective(self-reported) and prospective (willingness to engage) models, authors explored the role of Neutralisation techniques when controlling variable from well-known criminology theories such Self-Control (SC), social learning (SL) and microanomie (strain).They found, using a sample of 585 undergraduate students from two universities, that techniques of neutralisation had a positive and direct effect on students willingness to participate in illegal downloading of music CD over video piracy. Also, from the retrospective model point view, the role of neutralisation had modest effect on music and video piracy over software piracy and can consider as a theoretical predictor for students potential digital piracy. These findings consistent with [22] study about the impact

of neutralisation techniques on on-line music piracy, who found that those techniques were statistically important to predict students' potential involvement in copying online music. In contrast, [20] found that a weak relationship between online software piracy and the role of neutralization techniques.

1.3.5 Study Model hypotheses:



Initial Research Model

1.3.6 Study Methodology:

TBD

1.3.7 Data Analisis and discussion:

TBD

1.3.8 Study Conclusion:

TBD

1.4 Plan and Future Work:

this section illustrates my following steps in my PhD theses. The results from the first year experiment will be the foundation to understand the current level of medical interns' overall security awareness about privacy polices as well as the potential role of neutralization techniques in the intention to breach patient privacy.Thereafter, based on the results, I will extend my current work by examining the antecedents factors of neutralization techniques in health care context.Also,I Intend to have an access to security polices and security incident reports from one or more Saudi hospitals in order to understand and analyze the current state of security design for the favor of medical interns. My aim in the second year is to determine security policies deficiencies and preform privacy analysis in order to make a formal approach to link each policy to a potential security incident.

1.5 Activities in First Year:

TBD

1.6 First Year Summary:

Bibliography

[1] full-text.

[2] Azam Abdollahzadehgan, Ab Razak Che Hussin, Marjan Moshfegh Gohary, and Mahyar Amini. The Organizational Critical Success Factors for Adopting Cloud Computing in SMEs. *Journal of Information Systems Research and Innovation*, 4(1):67–74, 2013. ISSN 2289-1358.

[3] Sanjay P Ahuja, Sindhu Mani, and Jesus Zambrano. A survey of the state of cloud computing in healthcare. *Network and Communication Technologies*, 1(2):p12, 2012.

[4] F Akowuah, X Yuan, J Xu, and H Wang. A survey of security standards applicable to health information systems. *International Journal of Information Security and Privacy*, 7(4):22–36, 2013. ISSN 19301650 (ISSN). doi: 10.4018/ijisp.2013100103. URL `https://www.scopus.com/inward/record.uri?eid=2-s2.0-84945184880{&}partnerID=40{&}md5=6f3ace7594a81b127b494447eebe0ab1`.

[5] Katherine P. Andriole. Security of electronic medical information and patient privacy: What you need to know. *Journal of the American College of Radiology*, 11(12):1212–1216, 2014. URL `http://dx.doi.org/10.1016/j.jacr.2014.09.011`.

[6] Debi Ashenden. Information Security management : A human challenge ? *Information Security Technical Report*, 13(4):195–201, 2008. ISSN 1363-4127. doi: 10.1016/j.istr.2008.10.006. URL `http://dx.doi.org/10.1016/j.istr.2008.10.006`.

[7] Jordan B Barlow, Merrill Warkentin, Dustin Ormond, and Alan R Dennis. Don't make excuses! Discouraging neutralization to reduce IT policy violation. 2013. doi: 10.1016/j.cose.2013.05.006. URL `http://ac.els-cdn.com/S0167404813000898/1-s2.0-S0167404813000898-main.pdf?{_}tid=7323926e-250f-11e7-b0b9-00000aab0f6b{&}acdnat=1492613574{_}70b359db1f35b3b04587c787538336af`.

[8] Ameur Bensefia and Anis Zarrad. A Proposed Layered Architecture to Maintain Privacy Issues in Electronic Medical Records. *E-Health Telecommunication Systems and Networks*, 03(04):43–49, 2014. ISSN 2167-9517. doi: 10.4236/etsn.2014.34006. URL http://www.scirp.org/journal/PaperDownload.aspx?DOI=10.4236/etsn.2014.34006.

[9] BSI. BSI Standards Publication Information technology Security techniques Information security management systems Overview and vocabulary. (September), 2014.

[10] Rajkumar Buyya, Rajkumar Buyya, Chee Shin Yeo, Chee Shin Yeo, Srikumar Venugopal, Srikumar Venugopal, James Broberg, James Broberg, Ivona Brandic, and Ivona Brandic. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(June 2009):17, 2009. ISSN 0167-739. doi: 10.1016/j.future.2008.12.001. URL http://portal.acm.org/citation.cfm?id=1528937.1529211.

[11] Medical Care. Annals of Internal Medicine Improving Patient Care Systematic Review : Impact of Health Information Technology on. *Most*, 144:742–752, 2006. ISSN 15393704. doi: 0000605-200605160-00125[pii]. URL http://www.ncbi.nlm.nih.gov/pubmed/16702590.

[12] Byeong Yun Chang, Pham Hoang Hai, Dong Won Seo, Jong Hun Lee, and Seung Hyun Yoon. The determinant of adoption in cloud computing in Vietnam. In *2013 International Conference on Computing, Management and Telecommunications, ComManTel 2013*, pages 407–409, 2013. ISBN 9781467320870. doi: 10.1109/ComManTel.2013.6482429.

[13] Yan Chen, K. Ramamurthy, and Kuang-Wei Wen. Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems*, 29(3):157–188, 2012. ISSN 0742-1222. doi: 10.2753/MIS0742-1222290305.

[14] Mary J Culnan, Cynthia Clark Williams, and Cynthia Clark Williams. Quarterly ^^^ m. 33(4):673–687, 2009.

[15] John D 'arcy and Anat Hovav. Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. doi: 10.1007/s10551-008-9909-7.

[16] Eva Deutsch, Georg Duftschmid, and Wolfgang Dorda. Critical areas of national electronic health record programs. Is our focus correct? *International Journal of Medical Informatics*, 79:211–222, 2010. ISSN 1872-8243. doi: 10.1016/j.ijmedinf.2009.12.002.

[17] ENISA. Risk Management : Implementation principles and Inventories for Risk Management / Risk Assessment methods and tools. (June):177, 2006. URL https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/files/deliverables/risk-management-principles-and-inventories-for-risk-management-

[18] Mark Grindle, Jitendra Kavathekar, and Dadong Wan. A new era for the healthcare industry - Cloud computing changes the game. *Accenture*, page 24, 2013. URL http://www.accenture.com/us-en/Pages/insight-healthcare-industry-cloud-computing.aspx.

[19] Habiba Hamid and Akram M. Zeki. Users' awareness of and perception on information security issues: A case study of kulliyyah of ICT postgraduate students. *Proceedings - 3rd International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2014*, pages 139–144, 2014. doi: 10.1109/ACSAT.2014.31.

[20] Sameer Hinduja. Neutralization theory and online software piracy: An empirical analysis. *Ethics and Information Technology*, (3):187–204, nov 2007. ISSN 1388-1957. doi: 10.1007/s10676-007-9143-5.

[21] Chien-Lung Hsu, Ming-Ren Lee, and Chien-Hui Su. The Role of Privacy Protection in Healthcare Information Systems Adoption. doi: 10.1007/s10916-013-9966-z.

[22] Jason R. Ingram and Sameer Hinduja. Neutralizing Music Piracy: An Empirical Examination. *Deviant Behavior*, 29(4):334–366, 2008. ISSN 0163-9625. doi: 10.1080/01639620701588131.

[23] ISO 27799:2016. BSI Standards Publication Health informatics Information security management in health using. 27002, 2016.

[24] ISO/IEC. INTERNATIONAL STANDARD ISO / IEC Information technology Security techniques Information security management systems Overview and. 2014:38, 2014.

[25] ISO/IEC29100. ISO/IEC 29100:2011(en), Information technology Security techniques Privacy framework.

[26] Faouzi Kamoun and Mathew Nicho. Human and Organizational Factors of Healthcare Data Breaches: The Swiss Cheese Model of Data Breach Causation And Prevention. *International Journal of Healthcare Information Systems and Informatics*, 9(1):42–60. doi: 10.4018/ijhisi.2014010103.

[27] Patrick Kierkegaard. Electronic health record: Wiring Europe's healthcare. 2011. doi: 10.1016/j.clsr.2011.07.013.

[28] Patrick Kierkegaard. Medical data breaches : Notification delayed is notification denied. *Computer Law & Security Review*, 28(2):163–183, 2012. ISSN 0267-3649. doi: 10.1016/j.clsr.2012.01.003. URL http://dx.doi.org/10.1016/j.clsr.2012.01.003.

[29] Sang Hoon Kim, Kyung Hoon Yang, and Sunyoung Park. An integrative behavioral model of information security policy compliance. *The Scientific World Journal*, 2014: 463870, 2014. ISSN 2356-6140. doi: 10.1155/2014/463870.

[30] Richard Kissel. Glossary of Key Information Security Terms Glossary of Key Information Security Terms. *Nist*, NISTIR 729(Revision 2), 2013. doi: 10.6028/NIST.IR.7298r2.

[31] Amjad Mahfuth, Jaspaljeet Singh Dhillon, and Sulfeeza Mohd Drus. a Systematic Review on Data Security and Patient Privacy Issues in Electronic Medical Records. *Journal of Theoretical and Applied Information Technology*, 3190(2):106–116, 2016. ISSN 1817-3195. URL www.jatit.org.

[32] MarketsandMarkets. Healthcare Cloud Computing Market by Application (PACS; EMR; CPOE; RCM; Claims Management); Deployment (Private; Public); Service (SaaS; IaaS); Pricing (Pay as you go) & by End-User (Providers; Payers) - Analysis and Global Forecasts to 2020. Technical report.

[33] Maslin Masrom and Ailar Rahimli. A review of cloud computing technology solution for healthcare system. *Research Journal of Applied Sciences, Engineering and Technology*, 8(20):2150–2153, 2014. ISSN 20407467.

[34] W. W. Minor. Techniques of Neutralization: a Reconceptualization and Empirical Examination. *Journal of Research in Crime and Delinquency*, 18(2):295–318, jul 1981. ISSN 0022-4278. doi: 10.1177/002242788101800206.

[35] Robert G Morris and George E Higgins. Neutralizing Potential and Self-Reported Digital Piracy A Multitheoretical Exploration Among College Undergraduates. doi: 10.1177/0734016808325034. URL http://journals.sagepub.com/doi/pdf/10.1177/0734016808325034.

[36] Department of Health, Human Services USA, USA Department of Health and Human, and Services. OFFICE RIGHTS FOR CIVIL Privacy, Security, and Electronic Health Records 1 PRIVACY, SECURITY, AND ELECTRONIC HEALTH RECORDS. URL https://www.hhs.gov/sites/

default/files/ocr/privacy/hipaa/understanding/consumers/privacy-security-electronic-records.pdf.

[37] Fan-Yun Pai and Kai-I Huang. Applying the Technology Acceptance Model to the introduction of healthcare information systems. 2011. doi: 10.1016/j.techfore.2010.11.007. URL http://ac.els-cdn.com/S0040162510002714/1-s2.0-S0040162510002714-main.pdf?{_}tid=7f09d7b8-08aa-11e7-909a-00000aab0f26{&}acdnat=1489491582{_}187baf56aaebd3a39a2d6c3ff39b5648.

[38] Chrysanthi Papoutsi, Julie E Reed, Cicely Marston, Ruth Lewis, Azeem Majeed, and Derek Bell. Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: results from a mixed methods study. *BMC medical informatics and decision making*, 15: 86, 2015. ISSN 1472-6947. doi: 10.1186/s12911-015-0202-2. URL http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=4607170{&}tool=pmcentrez{&}rendertype=abstract.

[39] Eun Hee Park, Jongwoo Kim, and Young Soon Park. The role of information security learning and individual factors in disclosing patients' health information. *Computers & Security*, 65:64–76, 2017. ISSN 0167-4048. doi: http://dx.doi.org/10.1016/j.cose.2016.10.011.

[40] CP Pfleeger, SL Pfleeger, and Jonathan Margulies. Security in computing. 4th, 2007.

[41] Ponemon Institute. The Human Factor in Data Protection. (January), 2012.

[42] S Posthumus and R Von Solms. A framework for the governance of information security. *Computers & Security*, 2004. URL http://www.sciencedirect.com/science/article/pii/S0167404804002639.

[43] Petri Puhakainen and Mikko Siponen. Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study1. *Source: MIS Quarterly*, 34(4):757–778, 2010. URL http://www.jstor.org/stable/25750704http://about.jstor.org/terms.

[44] Fiza Abdul Rahim, Zuraini Ismail, and Ganthan Narayana Samy. A Review on Influential Factors of Information Privacy Concerns in the Use of Electronic Medical Records. *IJCSIS) International Journal of Computer Science and Information Security*, 14 (7), 2016. URL http://search.proquest.com/docview/1815514566/fulltextPDF/CA216B5E5BD1429EPQ/1?accountid=142908.

[45] Joseph W Rogers and M D Buffalo. Neutralization Techniques: Toward a Simplified Measurement Scale Toward a Simplified Measurement Scale. *Source: The Pacific Sociological Review*, 17(3):313–331, 1974. URL http://www.jstor.org/stable/1388569http://www.jstor.org/stable/1388569?seq=1{&}cid=pdf-reference{#}references{_}tab{_}contentshttp://about.jstor.org/terms.

[46] Nader Sohrabi Safa, Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani, and Tutut Herawan. Information security conscious care behaviour formation in organizations. *Computers & Security*, 53:65–78, 2015. ISSN 01674048. doi: 10.1016/j.cose.2015.05.012.

[47] G N Samy, R Ahmad, and Z Ismail. Security threats categories in healthcare information systems. *Health Informatics Journal*, 16(3):201–209, 2010. ISSN 1460-4582. doi: 10.1177/1460458210377468.

[48] Ganthan Narayana Samy, Rabiah Ahmad, and Zuraini Ismail. Security threats categories in healthcare information systems, 2010. ISSN 1460-4582. URL http://www.ncbi.nlm.nih.gov/pubmed/20889850http://jhi.sagepub.com.

[49] Mikko T Siponen and Anthony Vance. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly: Management Information Systems*, 34(SPEC. ISSUE 3):487–502, 2010. ISSN 02767783. doi: 10.2460/javma.228.4.578. URL http://www.scopus.com/inward/record.url?eid=2-s2.0-77957068563{&}partnerID=40{&}md5=c6ecfa7e63590aa13b8e6870bbc9c576.

[50] Nabil Sultan. Making use of cloud computing for healthcare provision: Opportunities and challenges. *International Journal of Information Management*, 34(2):177–184, 2014. ISSN 02684012. doi: 10.1016/j.ijinfomgt.2013.12.011.

[51] Gresham M Sykes and David Matza. Techniques of Neutralization: A Theory of Delinquency. *Source: American Sociological Review*, 22(6):664–670, 1957. URL http://www.jstor.org/stable/2089195http://www.jstor.org/stable/2089195?seq=1{&}cid=pdf-reference{#}references{_}tab{_}contentshttp://about.jstor.org/terms.

[52] AlAlaa N Tashkandi and Ibrahim M Al-Jabri. Cloud computing adoption by higher education institutions in Saudi Arabia: an exploratory study. *Cluster Computing*, 18 (4):1527–1537, 2015.

[53] Pei-Lee Teh, Pervaiz K. Ahmed, and John D'Arcy. What Drives Information Security Policy Violations among Banking Employees? Insights from Neutralization and Social Exchange Theory. *Journal of Global Information Management*, 23(1):44–64, 2015. ISSN 1062-7375. doi: 10.4018/jgim.2015010103.

[54] Abdeneaser Tweel. *Examining the Relationship between Technological, Organizational, and Environmental Factors and Cloud Computing Adoption*. PhD thesis, Northcentral University, 2012.

[55] U.S. Department of Health and Human Services. What is the difference between a Personal Health Record, an Electronic Health Record, and an Electronic Medical Record?, 2015. URL https://www.healthit.gov/providers-professionals/faqs/what-are-differences-between-electronic-medical-records-electro

[56] U.S. Department of Health and Human Services Office of Civil Rights. Annual Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Years 2013 and 2014. Technical report, 2014. URL https://www.hhs.gov/sites/default/files/rtc-breach-20132014.pdf?language=en.

[57] U.S. Department of Health and Human ServicesHHS. SUMMARY OF THE HIPAA PRIVACY RULE HIPAA Compliance Assistance O C R P R I V A C Y B R I E F SUMMARY OF THE HIPAA PRIVACY RULE. 2003.

[58] Daniel Wartenberg and W. Douglas Thompson. Privacy versus public health: The impact of current confidentiality rules, 2010. ISSN 00900036.

[59] World. WHO — The World Health Report 2008 - primary Health Care (Now More Than Ever). *WHO*, 2013. URL http://www.who.int/whr/2008/en/.

[60] World Health Organization. WHO — Global diffusion of eHealth: Making universal health coverage achievable. Technical report, 2016. URL http://www.who.int/goe/publications/global{_}diffusion/en/.

[61] Ji Jiang Yang, Jianqiang Li, Jacob Mulder, Yongcai Wang, Shi Chen, Hong Wu, Qing Wang, and Hui Pan. Emerging information technologies for enhanced healthcare. *Computers in Industry*, 69:3–11, 2015. ISSN 01663615. doi: 10.1016/j.compind.2015.01.012. URL http://dx.doi.org/10.1016/j.compind.2015.01.012.

[62] Humayun Zafar and Jan Guynes Clark. Communications of the Association for Information Systems Current State of Information Security Research In IS. 24(34): 557–596, 2009. URL http://aisel.aisnet.org/caishttp://aisel.aisnet.org/cais/vol24/iss1/34.