“I do it because they do it”: social-neutralisation in information security practices of Saudi medical interns

Saad Altamimi
Karen Renaud
Timothy Storer

This is the Author Accepted Manuscript of a conference paper published in Risks and security of internet and systems: 14th International Conference, CRiSIS 2019, Hammamet, Tunisia, October 29–31, 2019, proceedings

The final publication is available at Springer via http://dx.doi.org/10.1007/978-3-030-41568-6_15

"*I do it because they do it*": Social-Neutralisation in Information Security Practices of Saudi Medical Interns

Saad Altamimi[1], Karen Renoud[2], and Timothy Storer[1]

[1] School of Computing Science, University of Glasgow, Glasgow, UK
s.altamimi.1@research.gla.ac.uk,Timothy.Storer@glasgow.ac.uk
[2] School of Design and Informatics, University of Abertay, Dundee, UK;
University of South Africa, South Africa.
k.renaud@abertay.ac.uk

Abstract. Successful implementation of information security policies (ISP) and IT controls play an important role in safeguarding patient privacy in healthcare organizations. Our study investigates the factors that lead to healthcare practitioners' neutralisation of ISPs, leading to non-compliance. The study adopted a qualitative approach and conducted a series of semi-structured interviews with medical interns and hospital IT department managers and staff in an academic hospital in Saudi Arabia. The study's findings revealed that the MIs imitate their peers' actions and employ similar justifications when violating ISP dictates. Moreover, MI team superiors' (seniors) ISP non-compliance influence MIs tendency to invoke neutralisation techniques. We found that the trust between the medical team members is an essential social facilitator that motivates MIs to invoke neutralisation techniques to justify violating ISP policies and controls. These findings add new insights that help us to understand the relationship between the social context and neutralisation theory in triggering ISP non-compliance.

Keywords: Neutralisation Theory · Health care · Information Security Policies· Privacy · Medical Interns

1 Introduction

Many healthcare organisations have encountered security and privacy challenges due to the wide adoption of Healthcare Information Systems (HIS). Electronic Medical Records (EMR) or Electronic Health Records (EHR) are instances of HISs. In this context, a privacy breach is "*a situation where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirements*" [18]. Reports from information security agencies state that healthcare organisations are susceptible to internal and external security threats that can jeopardise the information security controls and policies of healthcare organisations and increase risks to EMRs. According to the Verizon 2019 Data Breach Investigation Report (DBIR) [35], there were 41,686 security incidents, of which 2,013 were data breaches. In the healthcare industry, a total

of 304 confirmed data breaches occurred, with 179 of these associated with employees. Several countries have developed strict information security and privacy regulations to force adherence by healthcare organisations in terms of collecting, processing and exchanging patient information to ensure privacy and confidentiality of patient data. These regulations, for instance, include the Health Insurance Accountability Act 1996 (HIPPA) in the US and General Data Protection Regulation (GDPR) in Europe in 2018.

Security and privacy breaches are costly to individuals and organisationals. The accidental or intentional disclosure of patient information can have consequences, such as employment termination, personal embarrassment, identity theft and loss of the health insurance [37]. Likewise, any breach within healthcare organisations could lead to legal liabilities, which could imply severe loss of trust and reputational damage, as well as financial penalties and pecuniary compensations [36].

In the information security literature, scholars have postulated that technology controls alone can not ensure integrity, availability and confidentiality of information held by an organisation without encouraging employees to to meet the organisation's information security goals [38, 31]. They call for more studies to explore the motivations behind individuals' intentions to violate or comply with ISPs. Instead of focusing on the effects or the consequences of the individual's ISP violations or compliance with organisational ISPs, there is a need take a step backwards to understand the factors that contribute to the intention to comply.

We extend previously published compliance-related research [31, 3, 34] which found that individuals would adopt cognitive justifications or embrace neutralisation techniques to overcome feelings of shame or guilt when they commit, or intend to commit, any particular violation.

This study investigates the impact of the social factors on **Medical Interns**' (MI) motivations to free themselves from the obligation to comply with the hospital's ISPs. We argue that the MIs ISP violations can originate from social aspects that influence them to employ neutralisation techniques and to behave insecurely. Here, we make a distinction between *malicious* and *non-malicious* violations of ISPs. A malicious violation involves an individual intentionally committing an act to harm the organisation's IT assets. This study, on the other hand, focuses on non-malicious behaviour, i.e. when an individual violates an ISP without intention to harm the hospital IT assets. In particular, they are likely to employ neutralisation techniques to justify their deviant behaviours [4]. Consequently, we sought to answer the following research questions:

RQ1: *What are the common neutralisation techniques that medical interns invoke to justify ISP violations?*

RQ2: *What are the social factor(s) that trigger invocation of such neutralisation techniques?*

To answer the questions, we conducted semi-structured interviews with MIs (n=21) and IT specialists (n=8) in a Saudi hospital. This study revealed that both peers and superiors influence MIs' misconduct and ISP breaches and that neutralisation techniques were used to justify their non-compliance. This paper is

organised as follows: Section 2 provides theoretical foundations for neutralisation theory, specifically individuals' deviant behaviour related to ISP non compliance. Section 3 details the study methodology, data collection and analysis. Section 4 reports on the study's findings and Section 5 presents the study conclusion and suggests directions for future work.

2 Theoretical Background

2.1 Information Security Policy Compliance and Privacy Protection

According to Parks *et al.* [25], privacy safeguards refer to the organisation's efforts to ensure personal information protection by implementing various types of security solutions, both technical and non technical. Despite these efforts to safeguard healthcare organisations' IT assets and information, security and privacy breaches by healthcare organisations keep occurring. For instance, in 2018, several healthcare organisations in the USA registered a new record of paying around 28 million dollars in fines and settlements due to HIPPA rule violations. This was 22% more than the fines paid in 2016 [19]. In response to the severe consequences of HIPAA non-compliance, healthcare organisations invested massively in strengthening technical controls to repel hacking attempts [28]. They adopted many IT and security "best practices" and developed a wide range of information security policies (ISPs) to assign responsibilities to employees and delineate their role in protecting organisations' information and technology resources [7]. Chan *et al.* [9] detail ISP compliance as "*core information security activities that need to be carried out by individuals to maintain information security as defined by ISP*". Thus, an internal security threat exists when an employee with legitimate access to the organisation's IT assets fails to comply with the organisation's ISPs [29]. In an effort to improve individual compliance and reduce undesirable behaviours, information security scholars have published a large number of studies that incorporate theories from sociology, criminology, psychology and other disciplines to achieve a deeper understanding of the antecedents of ISP non-compliance triggers [13, 12].

2.2 Neutralisation Theory

Sykes and Matza [33] introduced neutralisation theory to explain the deviant behaviour of juveniles. Deviant behaviour is any action that conflicts with the shared values of a social group; the group members consider the behaviour unacceptable. Rogers and Buffalo [27] defined neutralisation techniques as "*a method whereby an individual renders behavioural norms inoperative, thereby freeing himself to engage in behaviour which would otherwise be considered deviant*". These neutralisation techniques help the offender to balance and negate the impact of the inner feelings of shame or guilt and make it possible for an offender to commit the non-compliant behaviour without self-blaming. Sykes and Matza [33] list five neutralisation techniques: (1) denial of responsibility, (2) denial of

injury, (3) the appeal of higher loyalty, (4) denial of victim and (5) condemnation of condemners.

Further applications of Sykes' original work have identified additional neutralisation techniques that support the effort to explain different types of crimes and deviant behaviours. For instance, Klockars [20] added the "*metaphor of the ledger*". Minor [24] mentions the "*defence of necessity*". Others are "*claim of normalcy*" introduced by [10], the "emphclaim of individuality", the "*claim of relative acceptability*", the "*claim of entitlement*" [17], "*justification by postponement*" and "*justification by comparison*" [14]. Neutralisation theory was the basis for various criminological studies of criminal behaviours, such as hate crime [8], car theft [11] and drug addiction [26].

2.3 Neutralisation Theory in the IT and IS contexts

Given the theoretical explanation of neutralisation theory in terms of investigating deviant behaviours, several scholars propose the application of this theory as a suitable lens to understand computer abuse [16], cyber-loafing [21] and digital piracy [30]. Willison and Warkentin [38] stated that it was worth applying neutralisation theory to explore employees' deviant security behaviours within organizations. They argue that the employee might use neutralisation to offset feelings of guilt or shame when they intend to break organisational rules. In the IS context, ISPs are a set of essential roles and responsibilities that are encoded in ISPs to guide employee security behaviours in the workplace. Siponen and Vance's [31] study revealed that the organisations' deterrence measures were not effective in the face of neutralisation techniques. They concluded that neutralisation techniques were correlated with employee intentions to commit ISP violations regardless of the presence or absence of formal or informal organisational sanctions. Moreover, other empirical studies [2, 34] found that neutralisation theory is a significant predictor of individuals' intention to breach information security policies.

2.4 Medical Interns in Saudi Arabia

In Saudi Arabia, medical schools have designed their medical curricula to include a one year compulsory clinical training after the medical students complete their mandatory medical courses. During the internship year, MIs work in teams under close supervision of seniors, such as medical consultants and residents. This arrangement improves the MI's clinical and practical experience as they gain continuous feedback during involvement with patients' treatment. Every month, each intern works in different clinic in the hospital and engages in different medical teams. The aim is to help MIs to improve their learning and ability to identify their preferred future medical specialty. Although these monthly shifts between clinics allow the MIs to enhance their clinical training, it also expands other non medical or processional competencies such as improving communication skills. This year enhances their professional attitudes and ethics with respect to patient care and safety [1].

3 Methodology

The study conducted a series of semi-structured interviews to collect data and applied a thematic analysis approach based on [6] to obtain answers to the research questions. The research environment was a Saudi Arabian hospital which is considered one of the biggest academic hospitals. It has more than 1400 beds in various specialties and several medical research centers around the country. Every year, the hospital admits more than 30000 patients and provides health care services to more than 250000 registered patients. In the hospital, MIs have access to the hospital's IT systems. The MI's privileges include accessing the hospital health care systems (HIS), which allows them to enter, view and edit patients' medical records. Over the last few years, the hospital has been impacted by several security incidents from internal sources. Medical employees' noncompliance with the hospital's ISP was the primary cause of internal security incidents such as unauthorised access to the hospital HIS's and the use of infected USB devices. We sought to investigate whether neutralisation techniques were used by MIs to justify their ISP violations.

3.1 Data Collection

The interview protocol had three main parts. During the *first* part, the authors explained the purpose of the study and asked the interviewee to sign the consent form. The *second* part commenced with general questions, collecting demographics, job descriptions and information security backgrounds. The *last* part of the interview explored the information security environment in the hospital in five major areas: (1) ISP development, (2) implementation, (3) enforcement, (4) awareness & training, and (5) incident reporting. Specifically, we investigated the impact of the existing security policies on the health practitioners' daily practices and activities. The initial questions were revised after the first interview to include probing questions that were used to explore the reactions of MIs to ISPs. We also explored the drivers of neutralisation technique adoption. We interviewed in a total of twenty-nine participants, including MIs and eight IT staff members. Each interview lasted between 45 and 60 minutes. All interviews were conducted face-to-face in the hospital and carried out by the first author from Sep 2018 to Nov 2019.

3.2 Participants

IT participants: We wanted to interview IT managers and staff who directly interacted with the health practitioners in meetings or discussions. Specifically, those IT department employees who are responsible for developing, implementing and enforcing ISPs and controls to protect the hospital's IT infrastructure and patient record privacy. The Associate Executive Director of the IT department distributed the interview invitations to the department staff via email. A total of eight participants from the IT department volunteered to be interviewed

(six IT managers and two IT employees). The study aimed to explore their perceptions about the current ISP violations, and IT department efforts to ease the conflict between IT security needs and the impact of those policies on healthcare practitioners' duties. The IT department's awareness of the medical employee justifications (neutralisation techniques) for ISP violations were explored, as well as their mitigation solutions.

Medical Interns: The study recruited twenty-one MIs (10 Female, 11 Male) via snowball sampling [5], which allowed us to reach this group more efficiently. Each of the MIs was asked to refer the interview invitation to other colleagues. Our aim was to gain insights into the interactions between MIs, as a group, and the ISPs, during daily activities. Another aim was to investigate the social factors that influenced MIs to violate ISPs i.e. what prompts them to justify such non-compliance by invoking neutralisation techniques. We continued to collect data until we reached saturation i.e. no new themes emerged [22].

3.3 Data Analysis

The interviews' audio files and transcripts were analysed as advised by Braun and Clarke [6] (Fig.1). Thematic analysis is a method that searches for common patterns within a qualitative data set and systematically underlines repeated themes. This encourages a better understanding of the context and ensures a greater organisation of the dataset. We identified all the relative passages in the responses that revealed security policy violations and the corresponding neutralisation technique(s) used to justify such violations. Also, the study focused on the possible reasons that lead the MIs to invoke such techniques. The data relating to the neutralisation techniques and ISP violations were then analysed thematically by using an inductive approach to code any relevant information in the text excerpt. Afterward, all the codes that reflected a similar concept were grouped to create meaningful themes. A qualitative software QSR NVivo Version 12 was used to conduct the thematic analysis and facilitate the management of the audio files and transcripts.

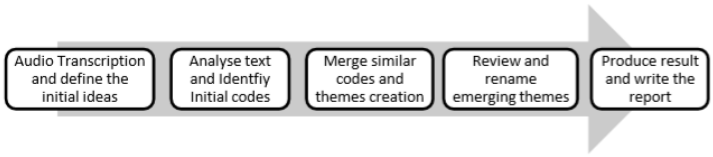

Fig. 1. Thematic analysis processes by Braun and Clarke [6]

4 Findings: Social Factors and Neutralisation techniques

Using thematic analysis, the study identified a number of social factors that motivated the MIs to justify their violations of the hospital ISPs. According to [23]

several neutralisation techniques might overlap, which may lead to inconsistent findings during technique identification. Thus, we used Fritsche's [15] typology as a guideline to improve our understanding of how to identify and select the neutralisation techniques, which improved our ability to reduce arbitrariness and inconsistent or overlapping techniques. We found that the social meta-categories influencing invoking of neutralisation techniques include: (1) peer influence, and (2) superior influence.

4.1 Peer Influence

Sutherland [32] stated that: "*An individual learns not only the techniques of committing the crime, no matter how complex or simple, but he/she learns specific motives, drives, rationalisations and attitude*" [p. 75].

The MIs are a subgroup of health care members who work to improve their practical healthcare skills. These interns share many individual characteristics such as age, medical experience, and educational background, which make their relationship and behaviours stronger and help them to solve work issues in similar ways. They are in an important stage of their medical education and perform medical duties within the healthcare teams during their clinic rotation. They get most of their training benefits from interacting with other peers and practitioners such as the medical residents, consultant and nurses. Interns are working hard to prove their medical competence and by so doing to gain a residency position after their internship year. This passion motivates tendencies to focus on medical training practices and duties more than anything else.

Several MIs indicated that accomplishing their medical responsibilities are prioritised over complying with ISPs. MI4: "*We take things based on the priorities, and we don't consider the information security a priority for us, and unfortunately, it might be considered the least of the priorities between our colleagues*".

Other MIs stated the importance of their medical duties compared to the hospital's concerns about compliance with ISPs: MI13: *"To be honest, we don't focus on this topic; we focus onpatient treatment management. For us, as MIs, we focus more on the medical skills and how to make a diagnosis or read its result, and so on. But the information security topics are not a priority for us."*

Many MIs indicated that the healthcare team norms impact their behaviour by imitating their colleagues non-compliance actions. Thus, they inherit and commit the same security policies violations and tend to evoke the same justifications. MI11:*"To be honest, I have not read a security policy document, but I have heard that from my colleagues about what I can do or not, all of my knowledge are pieces of advice that are coming from people in the practices*"; MI16:" *you see what people around you are doing, and you will do the same. Even though the person supposed to know the wrong or right by himself".*

MIs indicated that he and other peers heavily rely on each other to overcome their daily practices issues, especially these issue related to the security controls such as limited internet access. MI20: "*When I face a situation, I read about it or inquire from someone knows such as my colleagues. For instance, I need to*

print files in the hospital, so I ask my colleagues how to do that. Therefore, each one of them gives me his experience to solve my issue with controls here because we have limited internet access and we cannot open Gmail, Hotmail, etc. So, I get benefits from their feedback and experiences".

Therefore, the social impact of the peers' behaviour can form their perception as they followed and imitated each other actions and used the same justifications for their non-compliant behaviour with the hospital ISPs. We identified four neutralisation techniques that the MIs use to justify their non compliance behaviour under the influence of their peers: (1) defense of necessity, (2) appeal to higher loyalty, (3) everybody else is doing it, and (4) denial of injury.

Defense of Necessity: The majority of the MIs (N= 16), indicated that they used this technique to justify their behaviour when they share their passwords or healthcare system account itself with peers. The common belief between the participants who illustrated evidence of this technique was that complying with the ISP was not a matter of urgency to them. Thus, they focused their attention on their primary mission to provide treatment to the patients and deal with the clinical workload. Some of the MIs argued that they shared the password with a colleague when it was necessary. Therefore, being a part of a medical team required from them to tightly collaborate with other peers and force them to perform some acts regardless to comply with the ISPs.

They stated that if a MI in the team found it difficult to access his account, then this will impact the team performance. The argument, in this situation, was the necessity to improve work performance, which made it justifiable to share HIS password or account. As respondents reported: MI16:"*.... at the end, you have to see the big picture, there is a patient interests might disrupt or delay because one of the medical team members does not have access*"; MI9:"*if someone refuses to give you the password of his account, this would delay the work because I would wait until he comes and opens his account to complete the order. It would delay the work performance*".

Appeal to higher loyalty: Participants who used this technique tend to "*legitimise deviant behaviour when a non-conventional social bond creates more immediate and pressing demands than one consistent with conventional society*". [14]. This technique considered the second most neutralisation technique that being reported by the MIs with (n=15). The primary ISP violation that evoked "*appeal of higher loyalty*" was sharing the password or the HIS account between MIs, who started their internship without an active account to access the hospital health care system. It was not surprising, based on the close relationship between the MIs, who were working together to serve the clinical requirements and their practical goals. The MIs who indicated support for this technique felt that they were doing the right thing, in providing professional help to peers to accomplish team duties without disruption. Here, some of the participants argued that they were sharing the password or the HIS account and neutralising their behaviour by referring to the greater good. For instance, some MIs justified their password sharing behaviour as support and help, especially during the internship period where any disruption of performance can impact MI training and evaluation. MI17: "*I think it is a kind of that we need to get the work done. It is professional*

support."; MI23: "*To be honest, here we have this kind of behaviour that we like to help people sometimes more than what supposed to be. So, this is considered "help" in our culture*

Everybody else is doing it: This technique refers to the impression that the damaging behavior is common to the group, so there was no need to feel guilty or ashamed. Six MIs (N=6) justified their behaviour by saying "*everyone of my peers is doing it*", especially when they left their PCs without logging out, shared a password or account with others or used an external Internet router to bypass Internet access restrictions. The participants argued that their behaviour was normal because other team members were commonly doing the same thing: MI9: "*I mean, the behaviours of others because the majority are doing this thing; we will do the same, even if it is wrong.*".

Also, they argued their behaviour was acceptable and they referred to the fact that a large number of their colleagues commonly shared passwords, left their PC's unlocked or utilised their own Internet routers: MI14: " *I see the majority share the password, for example, and leave their account open without Log-out. Sometimes, I leave my account open to let my colleague work on the same note.*"; MI27:"*I have to use my mobile Internet router, which I bring with me. Actually, a lot of my colleagues do the same not only me*".

Also, they stated that no one got caught or punished for performing such actions, which implied that the IT department had not considered these acts to be information security breaches. They referred to the existence or absence of ISP violation sanctions to evaluate which of the typical behaviours in their peer groups was considered a breach of the hospital's ISPs or not. The MIs evoked this technique based on their observation of the social context that influenced their decision-making processes to decide which behaviour was acceptable: MI27: "*Also, as I have mentioned everybody doing it from the physicians to the nurses and residents. Everyone leaves their account open and there is no specific punishment*".

Denial of Injury: The offender who uses this technique claims that the outcomes of his/her deviant behaviour are harmless, and he/she does not show any concern about the expected consequences of non compliant behaviour [33]. More than half of the MIs (N=13) referred to this neutralisation technique when they revealed some of their daily practices. One MI who adopted this technique refused to acknowledge the fact that, by sending photos from patients' medical records via a social media application e.g "Whats-App" or sharing the password or the HIS account with a colleague, could cause any harm to the patient privacy or the hospital.

There were three main arguments behind these non-compliant actions; the first was that the MIs' HIS accounts had limited privileges as they could only access the patient records to write patients' diagnoses. They did not have any authority to issue medical orders such as prescribing medicines or conducting lab tests. The MI's judgment was concentrated on the physical harm that could impact the patients' health due to incorrect medical orders. Thus, they failed to pay attention to the information security risks that could originate from sharing passwords. They reported that: MI10: "*Technically speaking, my account is lim-*

ited as a medical intern, and we only can write notes. So, she is going to write notes like me, and she cannot do something major. There is no security breach in my perspective because we both know what the limit is"; MI7: "*We are not allowed, as medical interns, to make medical orders, so I'm not worried that the person who I share my account will do something that can harm me in future or the patient"*.

Some of the MIs conducted a type of risk comparison as a way to decrease the injury that could occur from sharing their HIS account password. The denial of the injury via reducing the impact and magnitude of the risk originated when they compared it to other team members in a higher position of authority, such as the consultant. So, they thought that sharing passwords would have a small negative impact on hospital's security. This thought affected the MIs' reporting of any observed violations of ISPs. A MI explained: MI15: "*.....what I'm saying is I know there is something that is important, but what interns think themselves that they are only interns !! So, Whatever threats that come from us, no one is going to consider it. threats coming from MIs are less impact than threats coming from CIOs or the heads of department. Because they have more responsibilities. So, their email is strong, if a CIO sent an email to a department, then it will be done and followed. But If I sent an email to a department no one is going to do anything. This is my belief"*.

The last argument was that several MIs habitually took pictures and shared these with peers via mobile social media applications. They believed that the recipient of the medical records photos was trusted, and would use these for medical purposes and keep them confidential. Some MIs confirmed that they had sent or received an image of a patient's records including lab results or x-rays, where the patients' information was clear. Others revealed that they had taken precautions to protect patient confidentiality by hiding the patient identifiable information such as the patient's name or Medical Record Number(MRN). This action was explained by different MIs, as follows: MI5:"*Today, one of my colleagues took a picture of a screen and all the information was there except the patient MRN. However, there were some cases where the MRN and the patient name have appeared."*; MI11:"*I have seen a lot of my colleagues do not pay attention to cover the MRN before they take a picture of the system screen, specifically the X-ray picture, for instance, always the patient information appears in the X-ray corner. They directly take a picture of the X-ray without considering covering the patient information located at the corner. They usually say we share it with our colleagues, so, they don't hide such information"*; MI16:"*Yes, I have sent some pictures for discussion with my medical team but without name or MRN of the patient"*.

4.2 Superior influence

The central role of the MIs during their monthly rotation was to learn from their superiors' including consultants or residents and working closely with them to provide healthcare services. During the internship, the interaction between the MIs and their superiors is considered an essential part of the learning process

for the MI. The consultant has the power to offer a residency position to any intern who successfully meets the practical training criteria. Thus, the superiors' decisions were a significant part of the evaluation process in subsequently gaining a residency position in the hospital.

The majority of the MIs explained that their superiors influenced their behaviours both directly and indirectly in several situations related to the ISPs. Therefore, this influenced their tendencies to invoke several neutralisation techniques as a part of the decision-making processes to deal with their superiors' requests. These orders could conceivably lead to an ISP violation.

In addition, the MIs provided evidence of several neutralisation techniques to justify their ISP violations and showed how the influence of their superiors had motivated them directly, and indirectly, to justify their abuse of the password and the HIS access policies. Thus, four main neutralisation techniques were identified and invoked due to the influence of the superiors: (1) *Denial of responsibility*, (2) *Denial of injury*, (3) *Defence of necessity*, and (4) *Defence of Convenience*.

Denial of Responsibility: Many MIs have cited their superiors' or seniors' authority as an essential factor that helps them to accomplish their aims, do their duties and gain better practical experience in the field. This close relationship might extend to informing ISP-related perceptions, as a MI indicated: M12:"*I observe what my seniors are doing regarding the information security and I do whatever they do"*.

The MI revealed that accountability towards the hospital's ISP had been influenced by the orders issued by their seniors, such as consultant or resident. Therefore, they shifted the responsibility of any potential harm of the ISP violations to their superiors. MI26: "*It is coming from the attending consultant, so usually people obey the person in authority even if it is the wrong action, they will follow it*".

Furthermore, they explained that their work environment was complex and required full collaboration from the entiure medical team to deliver health care services to the patients. So, being a trainee in a medical team made it difficult for any MI to deny to carry out an order from a consultant, even if the request could lead to ISP violation or privacy violation. For instance, an MI explained his fear of the consequences of a refusal on his application for a residency position when a consultant asked him to share his account with another intern: MI4: "*for seeking approval or recommendation from the supervisors. They might see you as a part of the team, which increase your chance about acceptance to be a resident. I will lose if I refuse to do it. If I say NO because I want to follow the rules, they might abuse you and isolate you from the team"*.

Besides, few MIs felt that their Seniors used their authority to violate the ISPs by delegating more responsibilities to the MIs than expected by the hospital management. For instance, some of the consultants shared their HIS accounts with MIs to allow them preform extra work duties, such as issuing medical orders. Thus, the MIs were forced to exceed their designated privileges to use the healthcare information system, which is considered a violation of the hospital's HIS access control policy: MI27: "*some physicians abuse the medical interns by letting them do more duties, so if medical Interns said that his/her account*

privileges are limited in order to conduct the requested order, the physician simply respond to that by saying that's ok, take my account or password and conduct the order."

Denial of injury: Several MIs reported evidence of using this neutralisation technique to justify their superiors' impact on the hospital's ISP non-compliance. For example, some of the MIs justified their use of the consultant's HIS account if the medical orders included only simple and routine procedures. In this case, the expected consequences of any wrong order on patient health were minor, regardless of the fact that the behaviour itself was a violation of any of the ISPs: MI5: "*It depends on the case. If the MI will use the consultant's account for minor order or routine medical procedure like order Paracetamol, X-ray, or blood test, the harm of these procedures such increasing the dose or asking for the X-ray is trivial".*

Two of the IT managers acknowledged the occurrence of this violation and described the consultants' perceptions as harmless when sharing HIS account credentials with others: ITE1:"*They say nobody will be harmed if I share my password, and I will simply change the password if there is a risk*"; ITD1:"*Also, the fact is the consultant and the resident don't see sharing the password as an issue for the email and [the health care system] and they think it is ok*".

Other MIs invoked this technique to justify their behaviour of sending a photo of the HIS screen to their seniors. They referred to this as a practical way of getting things done, enhancing convenience and not wasting the seniors' time. They sometimes received a request from a physician to send a photo of a patient record and sometimes they sent the picture to the physician's mobile seeking treatment advice. In fact, the MIs blamed the IT department's technical restrictions such as the lack of remote access (VPN) as being responsible for this type of security violation. Therefore, instead of verbally reading the patient information over the phone or asking the consultant to come to the clinic to read the patient's diagnoses or the lab results, they took photos of the patient records and sent them to the consultants' mobiles. They argued that they sent the photo to the consultants' phone directly, as requested, and only two people had the images. This reduced the changes that these pictures would be leaked: MI17:"*I understand there is a risk but what is the probability of happening. Your example has a very minimal chance to occur if any"*; M11: *"most of the people in the medical field are looking for practical rather than professional. They preferred practicality, so instead of asking the physician to come to the hospital, they take a picture and send him the findings and the lab results to let him gives his diagnoses or treatment plan. So, they think it is more practical and it is better to get the job done".*

MIs stated that their seniors had sent photos containing patients' records to their mobiles, where the identifiable patient information was clearly shown. The seniors took these pictures for some of the patients' unique case records and shared them with many MIs in the team, as a part of the learning process: MI9: "*It is the wrong behaviour, but they do it a lot. Also, the seniors might take a picture of the patient information that includes the name and the MRN and share it with others, they don't care about hiding this information that much.*

They do that for many reasons such as teaching or discussion. That's frequently occurred, even it is a wrong action".

Defence of Necessity: Several MIs reported that they had no choice in performing their work efficiently without sharing a password. Some of the MIs related situations where their seniors shared their HIS accounts with them temporarily. For instance, some had started their internship program without an active HIS account, which conflicted with their training objectives to gain practical experience. A significant part of the training consisted of writing patients' medical documentation. Thus, the consultant or the resident had to share their HIS account credentials until the IT department activated the intern's HIS account. MI09:"*The problem is that many medical interns don't receive their healthcare system account from the IT department before they start the program". If the resident realised that the medical intern does not have an account, in this case, the resident usually shares his/her health care system account with the medical intern and log out when he/she finished writing the notes*".

Another group of MIs reported on a situation where a large number of patients in some clinics created a significant burden on the physicians, which forced them to seek help from the team to provide the healthcare services and reduce treatment time. If the physician spent most of his/her time handling routine duties such as writing medical notes rather than examining the patients, treatment time would increase. M18: *"if the doctor strictly complies with security policies and does not share his account, I think that may impact his work performance.At the end, when the doctor stops dealing with the patient in order to do some simple tasks, that can impact the doctor's performance in the clinic".*

An IT security employee confirmed the previous justification from a consultant to share their password of the HIS account: ITE1:"*The doctor's justification for such behaviour, which I have heard that from them, here I will quote the doctors speech 'I'm here in the clinic for patient treatment and I have many patients to look after their health, so I don't have time to access the system each time to make medical orders or procedures such as lab orders or pharmacy orders and so on'. Thus, this is a part of the nurse duties as she is an assistant of the doctors, therefore, I give her my password to conduct such orders, while I'm doing my primary work to meet and examine the patients' end of quote".*

Also, several MIs justified the impact of their seniors' behaviours on them, which could lead to their violating the password policy. They indicated the importance of sharing passwords, especially when the consultant was too busy and tired dealing with patients all day or dealing with many urgent cases, which increased the risk of making mistakes in the HIS orders. Their argument was that the consultant benefits from sharing the HIS account credentials in this situation, and this offset the ISP violation behaviour. M12:"*Sometimes when a person is tired, he is more likely to do mistakes because he maybe does the medical orders quickly to finish the work. So, I think it is justifiable in this situation if the doctor gives others colleagues, a trusted person, his account to overcome the tiredness risk.*"; M18:"*Regarding sharing the password, the doctors share their passwords because there is a need for doing that....in the emergency clinic, several doctors*

have shared their passwords with me, so I can order anything for the patient and it comes directly without delay".

Defence of Convenience: This justification emerged from several MIs as a new neutralisation technique. They claimed that that the violation of the information security policy met the violator's needs. They considered ISP compliance a subjective matter based on their judgment and evaluation in the current situation. The MIs who engaged in this delinquent behaviour seemed in an intermediate position between a denial of injury and a defence of necessity. So, MIs who used this justification moved back and forth between ISP compliance and non-compliance to gain more personal and work benefits. They argued that they could use better ways to make their work more convenient or more effificent, while, in reality, they wanted to accumulate personal credits with work benefits. Some MIs reported that the consultants shared their passwordd because they wanted to stay home and made the interns perform their tasks. Some MIs stated that consultants were simply too lazy to do their duties: MI19:"*Because it is more convenient for the consultant to stay home and ask his juniors to complete a specific task"*.

5 Conclusion

Employees' adherence to ISPs cannot be taken for granted. They sometimes drift to non-compliance and adopt neutralization techniques to salve their conscience when they decide not to comply with ISP dictates. On the other hand, sometimes the environment and social norms explicitly encourage non-compliance: people follow the descriptive norms (what others are doing) rather than injunctive norms (what the ISPs tell them to do). We carried out a study that revealed a number of motivations that encourage MIs to invoke behavioral justifications when not complying with ISPs: neutralization techniques that helped them to feel better about not complying. As future work, we plan to consider amelioration techniques that could reduce the likelihood that medical interns will use neutralization techniques instead of complying with hospital ISPs.

References

1. M. S. Al-Moamary, S. Mamede, and H. G. Schmidt. Innovations in medical internship: benchmarking and application within the King Saud bin Abdulaziz University for Health Sciences. *Education for Health (Abingdon, England)*, 23(1):367, 2010.
2. Saad Altamimi, Timothy Storer, and Ahmed Alzahrani. The role of neutralisation techniques in violating hospitals privacy policies in saudi arabia. In *2018 4th International Conference on Information Management (ICIM)*, pages 133–140. IEEE, 2018.
3. Jordan B Barlow, Merrill Warkentin, Dustin Ormond, and Alan R Dennis. Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, 39:145–159, 2013.
4. Stefan Bauer and Edward WN Bernroider. An analysis of the combined influences of neutralization and planned behavior on desirable information security behavior. In *13th Annual Security Conference, Las Vegas, US*, 2014.

5. Patrick Biernacki and Dan Waldorf. Snowball sampling: Problems and techniques of chain referral sampling. *Sociological methods & research*, 10(2):141–163, 1981.
6. Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.
7. Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3):523–548, 2010.
8. Bryan Byers, Benjamin W. Crider, and Gregory K. Biggers. Bias Crime Motivation: A study of hate crime and offender neutralization techniques used against the Amish. *Journal of Contemporary Criminal Justice*, 15(1):78–96, 1999.
9. Mark Chan, Irene Woon, and Atreyi Kankanhalli. Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, 1(3):18–41, 2005.
10. James William Coleman. *The criminal elite: The sociology of white collar crime*. Macmillan, 2001.
11. Heith Copes. Streetlife and the rewards of auto theft. *Deviant Behavior*, 24(4):309–332, 2003.
12. W. Alec Cram, John D'Arcy, and Jeffrey G. Proudfoot. Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly*, 34(2):525–554, 2019.
13. W Alec Cram, Jeffrey G Proudfoot, John D 'arcy, and W Alec. Organizational information security policies: a review and research framework. *European Journal of Information Systems*, 26(6):605–641, 2017.
14. Paul Cromwell and Quint Thurman. The devil made me do it: Use of neutralizations by shoplifters. *Deviant Behavior*, 24(6):535–550, 2003.
15. Immo Fritsche. Account strategies for the violation of social norms: Integration and extension of sociological and social psychological typologies. *Journal for the Theory of Social Behaviour*, 32(4), 2002.
16. Susan J Harrington. The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly*, 20(3):257–278, 1996.
17. Stuart Henry and Roger Eaton. *Degrees of deviance: Student accounts of their deviant behavior*. Avebury, 1989.
18. ISO/IEC29100. ISO/IEC 29100:2011(en), Information technology Security techniques Privacy framework.
19. HIPAA Journal. Healthcare data breach statistics, 2018. `https://www.hipaajournal.com/healthcare-data-breach-statistics/`.
20. C B J Klockars. *The Professional Fence*. Tavistock Pubns, 1975.
21. Vivien KG Lim. The it way of loafing on the job: Cyberloafing, neutralizing and organizational justice. *Journal of organizational behavior: the international journal of industrial, occupational and Organizational Psychology and Behavior*, 23(5):675–694, 2002.
22. Martin N Marshall. Sampling for qualitative research. *Family Practice*, 13(6):522–526, 1996.
23. Shadd Maruna and Heith Copes. What Have We Learned from Five Decades of Neutralization Research? *Crime and Justice*, 32(July 2015):221–320, 2005.
24. W. W. Minor. Techniques of Neutralization: a Reconceptualization and Empirical Examination. *Journal of Research in Crime and Delinquency*, 18(2):295–318, July 1981.

25. Rachida Parks, Heng Xu, Chao-Hsien Chu, and Paul Benjamin Lowry. Examining the intended and unintended consequences of organisational privacy safeguards. *European Journal of Information Systems*, 26(1):37–65, 2017.
26. Nicole Leeper Piquero, Stephen G. Tibbetts, and Michael B. Blankenship. Examining the role of differential association and techniques of neutralization in explaining corporate crime. *Deviant Behavior*, 26(2):159–188, 2005.
27. Joseph W Rogers and MD Buffalo. Neutralization techniques: toward a simplified measurement scale. *Pacific Sociological Review*, 17(3):313–331, 1974.
28. Ganthan Narayana Samy, Rabiah Ahmad, and Zuraini Ismail. Security threats categories in healthcare information systems. *Health Informatics Journal*, 16(3):201–209, 2010.
29. Mario Silic, Jordan B Barlow, and Andrea Back. A new perspective on neutralization and deterrence: Predicting shadow it usage. *Information & Management*, 54(8):1023–1037, 2017.
30. Mikko Siponen, Anthony Vance, and Robert Willison. New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Information & Management*, 49(7):334–341, 2012.
31. 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.
32. Edwin H Sutherland, Donald R Cressey, and David F Luckenbill. *Principles of criminology*. Altamira Press, 1992.
33. Gresham M Sykes and David Matza. Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, 22(6):664–670, 1957.
34. 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.
35. Verizon. 2019 Data Breach Investigations Report. *Verizon Business Journal*, pages 1–77, 2019.
36. Jeffrey Wall, Paul Benjamin Lowry, and Jordan B Barlow. Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems*, 17(1):39–76, 2015.
37. Daniel Wartenberg and W. Douglas Thompson. Privacy versus public health: The impact of current confidentiality rules. *American Journal of Public Health*, 100(3):407–412, 2010.
38. Robert Willison and Merrill Warkentin. Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 37(1):1–20, 2013.