A Framework for Assessing Motivational Methods Towards Incentivizing Cybersecurity Practice in Healthcare

PROSPER K. YENG
prosper.yeng@ntnu.no
Norwegian University of Science and Technology
Gjøvik, Innlandet, Norway

BIAN YANG
bian.yang@ntnu.no
Norwegian University of Science and Technology
Gjøvik, Innlandet, Norway

MUHAMMAD ALI FAUZI
muhammad.a.fauzi@ntnu.no
Norwegian University of Science and Technology
Gjøvik, Innlandet, Norway

PETER NIMBE
peter.nimbe@uenr.edu.gh
University of Energy and Natural Resources
Sunyani, Ghana

DIAH PRIHARSARI
diah.priharsari@ub.ac.id
Universitas Brawijaya
Malang, Indonesia

ABSTRACT

Data breaches in healthcare have become common in recent times due to the weakness of the human element. As a result, intrinsic and extrinsic motivations were identified, analyzed, and assessed through a literature survey. After a critical gap analysis of the related studies, a framework was designed. This can be used to practically assess the effectiveness of various motivational methods for incentivizing healthcare staff toward strengthening the human aspect of security practice.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**.

KEYWORDS

Healthcare, Incentive, Motivation, Cybersecurity, Intrinsic, Extrinsic

ACM Reference Format:
PROSPER K. YENG, BIAN YANG, MUHAMMAD ALI FAUZI, PETER NIMBE, and DIAH PRIHARSARI. 2022. A Framework for Assessing Motivational Methods Towards Incentivizing Cybersecurity Practice in Healthcare. In *7th International Conference on Sustainable Information Engineering and Technology 2022 (SIET '22), November 22–23, 2022, Malang, Indonesia.* ACM, New York, NY, USA, Article 111, 6 pages. https://doi.org/10.1145/3568231.3568285

1 INTRODUCTION

Like any organization, addressing healthcare information security issues involve people, process, and technology [14, 15]. However, technological measures are often used to automate various security measures including patch management, antivirus update, intrusion detection and prevention, and other security policy configurations, aimed to reduce the knowledge and time burden on end-users [15]. However, over-reliance on technological measures cannot succeed in addressing all the emerging threats as some are dependent on human behaviour. For instance, behaviours such as appropriate password habits, appropriate use of networks, and other conscious care behaviour are more dependent on the users [15, 35, 37].

Security issues relating to the human element have become a major concern in recent times because millions of dollars and even human lives are being lost to security issues in healthcare. As humans are classified as the weakest link in the security chain [18, 30, 32], adversaries tend to manipulate them to complete their attack intentions in healthcare systems. Data breaches in healthcare spiked to 55% in 2020 in the US and counted up to 600 breaches with a relative increase in the cost of data breaches by 10% in comparison with that of 2019 [33]. Recently, various health providers including Ireland HSE and New Zealand hospitals went into Electronic Health Records downtime due to ransomware attacks. The HSE consists of over 100,000 workers who run the public health service in Ireland, focusing on patients and clients [17]. The root course of the attack was being investigated however, most ransomware attacks are caused by human susceptibilities. The attackers tend to lure the users to click on malicious links thereby enabling the cybercriminals to gain unauthorized access to healthcare systems.

To mitigate the trend of data breaches, various psychological, social and cultural theories [1, 2, 23, 29] have been adopted in field of information security (IS) towards motivating users to skew to good security practice. For instance, perceived severity (PS) is a construct within the theories of protection motivation theory, and the health believe model [21]. The motivation in PS in relation to health is that the tendency for people to change their health risk behaviour to avoid contracting a disease depends on how serious they perceive the severity of the impact of the disease. So in the context of IS, the probability for a user to violate security rules could depend on how serious they perceive the consequence of the data breaches within healthcare.

The general objective of this study is to therefore develop a framework that can be used to comprehensively and practically assess various motivational methods for improving security practices among healthcare staff. The specific objective and the contribution

SIET '22, November 22–23, 2022, Malang, Indonesia

ACM ISBN 978-1-4503-9711-7/22/11.
https://doi.org/10.1145/3568231.3568285

in this paper therefore aimed towards addressing the following research questions;

- What are the state-of-the-art motivational methods for incentivising security practices?
- How can these methods be assessed towards improving healthcare staff's security practice?

2 BACKGROUND

In the quest for incentive methods, for reducing susceptibility in the context of human behaviour, various theories, concepts, and constructs have been imported into the space of information security research. These include Health Belief Model (HBM), Protection Motivation Theory (PMT), Cognitive dissonance (CD), General deterrence theory (GDT), Social control (SC), and many more.

PMT deals with the ability to incentivize the individual themselves based on various perceptions such as a threatening event, perceiving the probability of the occurrence, or vulnerability, perceived impact of the recommended action, and perceived self-efficacy [29]. PMT relies on fear appeals and uses self-efficacy (SE), response efficacy, maladaptive response, and past behaviour factors. But PMT does not account for the influence of personal and demographic variables and it has been considered to have inflexible cues to action [23]. TPB/TRA adopts attitude, subjective norms, and perceived behavioural control to influence individual and organizational security culture [1, 2]. In addition, TPB accounts for social factors but it does not consider psychological effects such as mood as well as environmental factors, economic effects, and prior experience. GDT discourages information security malpractices of individuals through disciplinary actions of the offenders [27]. The debate as to whether to use intrinsic or extrinsic motivations to enhance security practice requires a variety of reflections.

These theories, concepts, and constructs are usually classified into intrinsic and extrinsic motivation. Intrinsic motivation tends to induce self-motivation and it is based on self-rewarding with inherent satisfaction. This type of motivation is independent of external reward [6, 18] and provides the freedom for employees to take their own internal decisions including their aspirations [18, 31]. Intrinsic motivations include but not limited to PS, SE, perceived vulnerability PV, and cognitive dissonance (CD). Extrinsic motivation is influenced by external rewards such as financial rewards or punishment towards inducing individuals to be conscious and careful of their security behaviour.

The term cognitive dissonance is used to describe the mental discomfort that results from holding two conflicting beliefs or values [16]. This theory was developed by Festinger, in the late 1950s within the field of social psychology [11]. The dissonance process begins at the moment that an individual realised a contradiction between two or more cognitions. Cognitions are seen to be in contradiction or in discrepancy if an individual observe that one cognition opposes the other. The are broad range of scenarios that cause this psychological discomfort. For instance, knowing that sharing a password violates security practices when one is confronted with the act to share a password. The negative effect of the dissonance motivates the individual, who is involved in the dissonance to change the cognition experience in order to maintain cognition consistency. This dissonance is often altered in two broad ways. For instance, in the case of a user who is caught up in sharing a password, having known that password sharing is not a good security practice, this individual can decline to share the passwords to reduce the dissonance effect. Alternatively, this individual can rationalized to share the password by reducing the negative effect of sharing the passwords. In such context, statement often use includes "Nothing will happen", "No one will know", "it is just once", and many more. In this study, a framework has therefore been developed to provide guidance for investigating the effect of CD in incentivizing security practice.

3 STUDY APPROACH

This study mainly assessed and developed a framework for modelling and analyzing various motivational methods for incentivizing security practices. As a result, steps in literature review process were followed as described in [7]. In addition, related studies were selected in GOOGLE Scholar, PUBMED, and SCOPUS with the search string of "Incentives OR motivation AND employee AND information security practice AND Healthcare". Literature such as peer-reviewed articles and published academic journals, relating to theoretical literature or research data-driven were included in the study. We considered this approach to meet the research objective. Related studies that followed similar approach includes [35–37].

4 RELATED STUDIES OF MOTIVATIONAL METHODS FOR ENHANCING INFORMATION SECURITY PRACTICE

Following the surge in data breaches, emanating from human behaviour, various research works have been conducted for motivational methods to incentivize security practices. For instance, Goel et al recently conducted research to assess the influence of financial motivation in incentivizing security practices across various organizations including healthcare staff. Participants were grouped into negative and positive frames [13]. The negative frame lost financial rewards if security policy violations were seen while participants in the positive frame were to gain financial incentives if they followed the security policy. Phishing attack with email use was adopted in this study as a security practice. Additionally, Goel et al. conducted an earlier study with smaller participants [12] where the participants gained 50 dollars per week for full compliance with the company's policies. 40 dollars were given if one violation was detected, and if 2 violations occurred, 30 dollars was offered and followed by 20 dollars offer on the count of three violations. However, no amount was given if more than three violations were detected in a week. Phishing email and password strength were used as security practices. The researchers also provided security training. Following that, the number of participants who set weak passwords was found to be greatly reduced.

Furthermore, Chen et al assessed punishment and reward to determine better incentive security practices. Three factors such as punishment, financial reward, and certainty of control were considered and these factors were administered to the participants at two levels thus severe and mild punishment, high and low reward, and high and low certainty. Security practices on password use, e-mail use, and Internet use were initially used. Oral praising was given to those who followed these policies while those who deviated,

were orally reprimanded and had some points reduced per the severity of the violations. These merit points were linked to their annual bonus which was added to their salary. General Deterrence Theory (GDT) combined with financial reward was hence used in this study [8]. Other extrinsic motivational methods which were assessed include penalties and pressures [15]. However, the severity of the penalty was assessed to have a negative effect on security compliance. The finding was realized in a questionnaire survey relating to subjective norms, peer behaviours influence, penalties with a certainty of detection, and severity of punishment in relation to IS violations.

Besides, protection motivation theory (PMT) [25, 34] is one of the intrinsic methods which has been widely assessed to incentivize human behaviour. In the context of information security compliance, Posey et al used PMT to survey the impact of organizational motivation on individual behaviour. The study realized that the influence of PMT is much reliant on the employee's organizational commitment level. Similarly, PMT and habit were used to assess the influence of past behaviours concerning security practices. The survey employed sharing passwords, workstation locking, and logging behaviour and copying sensitive information to a USB stick without encryption, were assessed. Perceived severity (PS) was claimed to have a positive influence on security practice [25]. However, John et al claimed that cognitive effect (thus individual feeling state or how one feels at a point in time) such as the individual mood has a significant impact on security behaviour which is independent of their past habits. In this study, the theory of recent action (TRA) and the theory of planned behaviour (TPB) were used with daily information security compliance [10].

Moreover, Safa et al conducted a study and found out that increasing the effort, increasing the risk, and removing excuses and rewards towards information security misbehaviour improves information security practice [28]. Their study was conducted by observing security practices that have increased the difficulty of violating information security policy such as strengthening access control, preventing unauthorized data exfiltration, and strong enforcement of passwords, among others. A similar issue emerged when Renaud et al had an intensive interview with the national health service (NHS) workers in the UK to find out what motivates or demotivates them in terms of information security practice in healthcare [26]. What came to light was that operational requirements for security conflicted with intrinsic motivational needs for staff, thereby causing stress and non-compliance. Staff also felt subdued to following security requirements, and that following security policy was challenging, citing concerns for patients and their desire to work efficiently and effectively. In addition, studies by Lebek et al. opined that the motivation for security practice also depends on the leadership style [18]. Therefore, they conducted research into the transformational type of leadership. Transformational leaders believe in societal values and influence their followers as such. A survey was therefore conducted by using transformational leadership attributes from the multifactor leadership questionnaire to assess the security policy compliance of staff. The findings showed a positive correlation between security practice and transformational leadership.

Additionally, cognitive dissonance theory was also assessed in a related study [24] for mitigating insider threat neutralization. A Honey port and a honey token were used to bait insiders to attack the honey port in this experiment, rather than attacking real data. Factors such as the removal of excuses were used to decrease rationalizations. In the same vein, Barlow et al., analyzed denial of injury, the metaphor of the ledger, and the defence of necessity aspects of rationalization for non-compliance with password security measures [5]. The findings showed that focusing on neutralization techniques is as effective as those of deterrence sanctions.

In the exploration of effective incentive methods, Ng et al also investigated into computer behaviour of users, using the health belief model (HBM) [22]. Their study found perceived susceptibility, benefits, and self-efficacy to be determinants of email-related security behaviour. Anwar et al. also showed that gender has an effect on security self-efficacy [3]. In summary, the motivational theories and concepts which were identified are shown in Table1.

5 MOTIVATIONAL METHODS, GAP ANALYSIS AND DISCUSSION

In efforts to strengthen human efforts in security requirement compliance, various motivational methods for incentivizing security practices were explored. The identified theories include but are not limited to HBM, PMT/TRA, CD, and GDT as shown in Table 1. The related theories and constructs were classified into intrinsic and extrinsic incentives. The intrinsic motivations include PMT, Perception of IS governance [26], individual mood, habits, the perceived intention of users' behaviour, and cognitive dissonance.

TPB, GDT, pressure, the increasing complexity of security behaviour [28] and financial rewards are some of the extrinsic motivations. Extrinsic motivations include the use of resources such as financial rewards. While considering the adoption of extrinsic motivation, it is vital to recognize that the healthcare environment is characterized by varying stresses that is usually originated from workload and work emergencies. For instance, during an emergency, the healthcare provider is time-bound. Therefore, incentive measures need to be carefully assessed while taking into consideration, the healthcare work-related factors. Reflecting on Goel et al study "Understanding the role of incentives in security behaviour", the study [12, 13] provided preliminary knowledge on financial incentives to enhance security however, the introduction of financial incentives for security compliance can raise the financial burden of the healthcare facility. Already, the healthcare sector has been observed to be chronically underfunded, and that has created huge burdens such as understaffing, inadequate patient care, and lack of medical equipment and consumables. As a result, the financial incentive, even if effective, may not be sustainable. Besides, bearing in mind that resources are limited, especially in organizations with many users, the adoption of financial motivation can have a huge burden on the organization such that if financial promises are not paid for for good security practices, the staff me tend to misbehave. Moreover, when thinking about assessing, punishment in GDT as an extrinsic measure, there is the need to be aware that maladaptive behaviour can set in such that the healthcare staff can also tend to not follow security practices. Healthcare staff may also feel subjugated by authorities to comply with security practices. Aside, punishment may be the last option for an organization to strictly adopt to induce sound security practices. The reason is that

Table 1: Motivational Concepts or Theories

No	Concept/Theories	Category	Count #
1	Financial Incentive [8, 12, 13]	Extrinsic	3
2	GDT [8]	Extrinsic	1
3	PMT [25, 34]	Intrinsic	2
4	Habit	Intrinsic	1
5	Perception of IS governance [26]	Intrinsic	1
6	Theory of Planned Behavior (TPB) or theory of recent action (TRA) [10]	Extrinsic	1
7	Individual mood [10]	Intrinsic	1
8	Penalties [15]	Extrinsic	1
9	Pressures [15]	Extrinsic	1
10	Perceived effect of user's action [15]	Intrinsic	1
11	Transformational leadership [18]	Intrinsic	1
12	The increasing complexity of security behaviour [28]	Extrinsic	1
13	HBM [3, 22]	Intrinsic	2
14	CD [5, 24]	Intrinsic	2

healthcare staff can be faced with stress from patients' conditions, emergency cases, and high workloads that can be contributing factors affecting security practice. Therefore, healthcare workers may feel unappreciated if they are punished due to unintentional security violations.

In the case of intrinsic motivations, studies have pinpointed leadership style and the lack of consideration of healthcare operational requirements to have a negative correlation with conscious care security practice [18, 26]. For example, Renaud et al found that security policy requirements interfered with the staff' intrinsic motivational needs, which led to their stress and non-compliance. Due to the leadership style, staff often felt suppressed with policies, with no support. Additionally, the motivations of IT security officers to ensure security was often in conflict with that of the operational staff who were more concerned about their patients and the need to complete their tasks.

To this end, various studies called for the adoption of both intrinsic and extrinsic motivation in the incentivization scheme for conscious care behaviour [18, 26] Safa et al., also advised management to consider the environmental factors that encourage employees to engage in information security misbehaviour and dealing with these environmental factors by putting in appropriate measures to decrease their negative effects on employees' security behaviour to mitigate the risk of insider threats. Virtual reality (VR) technology can also be assessed in this context [19, 20] where for instance, intrinsic factors are simulated with these devices to induce other psychological effects on healthcare staff such as fear appeals, perceived severity, perceived vulnerability, and low-risk rationalization of cognitive dissonance. The framework in Figure **??** can be followed to assess and incorporate both intrinsic and extrinsic incentives toward enhancing security practice.

From the existing studies, a control experiment method [8, 13] and field observations [3, 5, 18, 22, 24, 28] were the identified methods often use to assess the effect of the motivation factors to incentivize security practice. With regards to a control experiment, the participants are usually assigned into groups followed by administering a treatment or an intervention to one of the groups, while the other groups (controlled group) are not provided with any intervention [9]. Even if an intervention is provided in the controlled group, that intervention is varied across the groups. In that the observational study, participants are surveyed with the aim to observe some factors without varying interventions among the participants. The controlled experiment has been considered to be useful in determining the cause-and-effect relationship between variables [4]. Hence, we adopted a control experiment in determining the influence of motivational factors on incentivising security practice.

6 A CONTROL EXPERIMENT FRAMEWORK FOR ASSESSING MOTIVATIONS IN SECURITY PRACTICE

The healthcare staff, including the doctors and nurses, are usually required to follow security practices including password management, incident reporting, and email use as shown in Figure 1. Additionally, the knowledge, attitude, and behaviour (KAB) of users with these security practices in TPB are usually essential in their actual security practice. The security practices combined with the KAB of the healthcare staff can be related to the various constructs such as PV, PS, SE, and RE to form a study scope.

A control experiment can then be conducted to assess the effectiveness of these constructs. For instance, the control experiment could have two levels, thus, a control group and an experiment group. The experiment group will then be treated with various theories, constructs, or concepts such as cognitive dissonance. The effect of the treatment can then be measured with the study scope. The assessment can be done with survey instruments, practical assessment with attack and defence simulation or directly observing the two groups to determine the effect of the treatment on the security practice of the participants. The treatment can be done by exposing participants in the experiment group to the independent variable through training, gamification, and the use of virtual augmented or mixed reality.

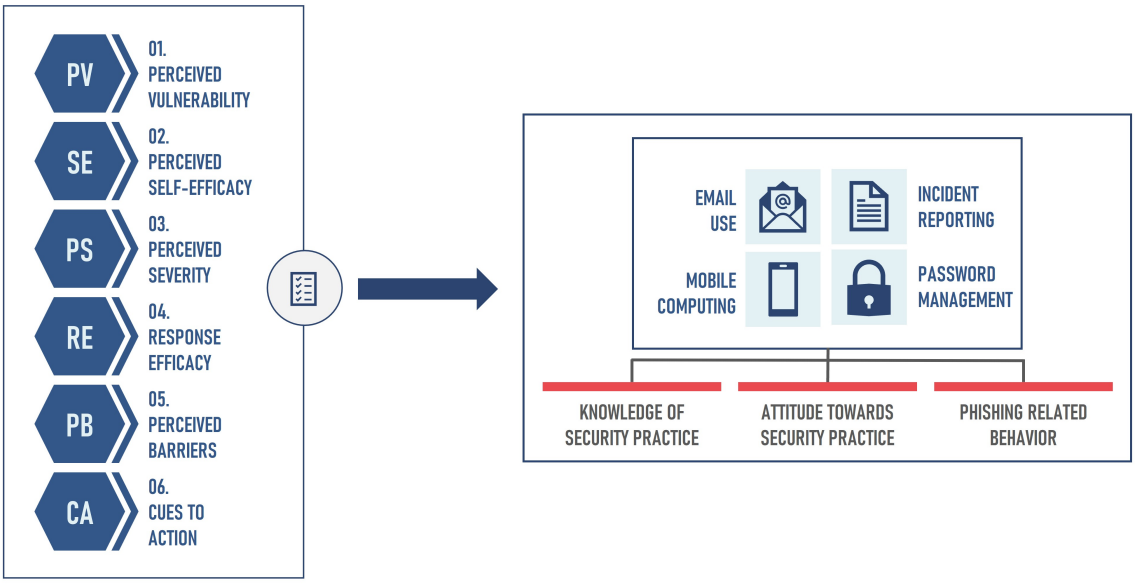

Figure 1: A framework for assessing motivational methods toward incentivizing security practice.

7 CONCLUSION

In search of ways to enhance security practices in healthcare, a survey was conducted to identify and assess various motivational methods. Extrinsic motivational methods such as financial incentives and deterrence methods were found. Also, other intrinsic methods were identified to include fear appeals from protection motivation theory, cognitive dissonance, leadership style, and preventing conflict between healthcare operational goals and required security practice of healthcare staff. To this end, a framework was proposed for assessing the efficacy of the various motivational constructs for enhancing healthcare security practice.

REFERENCES

[1] Icek Ajzen. 1991. The theory of planned behavior. *Organizational behavior and human decision processes* 50, 2 (1991), 179–211.

[2] Icek Ajzen and Thomas J Madden. 1986. Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of experimental social psychology* 22, 5 (1986), 453–474.

[3] Mohd Anwar, Wu He, Ivan Ash, Xiaohong Yuan, Ling Li, and Li Xu. 2017. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior* 69 (2017), 437–443.

[4] Ina Asklund, Emma Nyström, Malin Sjöström, Göran Umefjord, Hans Stenlund, and Eva Samuelsson. 2017. Mobile app for treatment of stress urinary incontinence: a randomized controlled trial. *Neurourology and urodynamics* 36, 5 (2017), 1369–1376.

[5] Jordan B Barlow, Merrill Warkentin, Dustin Ormond, and Alan Dennis. 2018. Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems* 19, 8 (2018), 3.

[6] Lois V Brown. 2007. *Psychology of motivation.* Nova Publishers.

[7] Darren N Caulley. 2007. Conducting research literature reviews: From the internet to paper. *Qualitative Research Journal* 7, 2 (2007), 103–105.

[8] Yan Chen, K Ramamurthy, and Kuang-Wei Wen. 2012. Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems* 29, 3 (2012), 157–188.

[9] Hugh Coolican. 2017. *Research methods and statistics in psychology.* Psychology press.

[10] John D'Arcy and Paul Benjamin Lowry. 2019. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal* 29, 1 (2019), 43–69.

[11] Leon Festinger. 1962. *A theory of cognitive dissonance.* Vol. 2. Stanford university press.

[12] Sanjay Goel, Kevin Williams, Jingyi Huang, and Merrill Warkentin. 2020. Understanding the role of incentives in security behavior. (2020).

[13] Sanjay Goel, Kevin J Williams, Jingyi Huang, and Merrill Warkentin. 2021. Can financial incentives help with the struggle for security policy compliance? *Information & Management* 58, 4 (2021), 103447.

[14] J Todd Hamill, Richard F Deckro, and Jack M Kloeber Jr. 2005. Evaluating information assurance strategies. *Decision Support Systems* 39, 3 (2005), 463–484.

[15] Tejaswini Herath and H Raghav Rao. 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems* 47, 2 (2009), 154–165.

[16] Amanda S Hinojosa, William L Gardner, H Jack Walker, Claudia Cogliser, and Daniel Gullifor. 2017. A review of cognitive dissonance theory in management research: Opportunities for further development. *Journal of Management* 43, 1 (2017), 170–199.

[17] HSE. 2021. *HSE Code of Governance.* Retrieved August 18 2022 from https://www.hse.ie/eng/about/who/directoratemembers/codeofgovernance/governance.html

[18] Benedikt Lebek, Nadine Guhr, and Michael Breitner. 2014. Transformational leadership and employees' information security performance: the mediating role of motivation and climate. (2014).

[19] Guido Makransky, Stefan Borre-Gude, and Richard E Mayer. 2019. Motivational and cognitive benefits of training in immersive virtual reality based on multiple assessments. *Journal of Computer Assisted Learning* 35, 6 (2019), 691–707.

[20] Guido Makransky, Thomas S Terkildsen, and Richard E Mayer. 2019. Adding immersive virtual reality to a science lab simulation causes more presence but less learning. *Learning and instruction* 60 (2019), 225–236.

[21] Amy C McPherson, Miriam L Gofine, and Jennifer Stinson. 2014. Seeing is believing? A mixed-methods study exploring the quality and perceived trustworthiness of online information about chronic conditions aimed at children and young people. *Health Communication* 29, 5 (2014), 473–482.

[22] Boon-Yuen Ng, Atreyi Kankanhalli, and Yunjie Calvin Xu. 2009. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems* 46, 4 (2009), 815–825.

[23] PAUL Norman and P Conner. 2005. Predicting health behaviour: a social cognition approach. *Predicting health behaviour* 1 (2005).

[24] Keshnee Padayachee. 2015. An insider threat neutralisation mitigation model predicated on cognitive dissonance (ITNMCD). *South African Computer Journal*

56, 1 (2015), 50–79.
[25] Clay Posey, Tom L Roberts, and Paul Benjamin Lowry. 2015. The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems* 32, 4 (2015), 179–214.
[26] Karen Renaud and Wendy Goucher. 2012. Health service employees and information security policies: an uneasy partnership? *Information Management & Computer Security* (2012).
[27] Edward Alsworth Ross. 1896. Social control. *Amer. J. Sociology* 1, 5 (1896), 513–535.
[28] Nader Sohrabi Safa, Carsten Maple, Tim Watson, and Rossouw Von Solms. 2018. Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of information security and applications* 40 (2018), 247–257.
[29] Nader Sohrabi Safa, Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani, and Tutut Herawan. 2015. Information security conscious care behaviour formation in organizations. *Computers & Security* 53 (2015), 65–78.
[30] Mikko Siponen, Seppo Pahnila, and Adam M Mahmood. 2006. A new model for understanding users' is security compliance. (2006).
[31] Mikko T Siponen. 2000. A conceptual foundation for organizational information security awareness. *Information management & computer security* (2000).
[32] Janine L Spears and Henri Barki. 2010. User participation in information systems security risk management. *MIS quarterly* (2010), 503–522.
[33] Anuja Vaidya. 2021. *Report: Healthcare data breaches spiked 55% in 2020.* Retrieved August 18 2022 from https://medcitynews.com/2021/02/report-healthcare-data-breaches-spiked-55-in-2020/#:~:text=There%20were%20nearly%20600%20healthcare,breach%20increased%20by%20about%2010%25
[34] Anthony Vance, Mikko Siponen, and Seppo Pahnila. 2012. Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management* 49, 3-4 (2012), 190–198.
[35] Prosper Yeng, Bian Yang, and Einar Snekkenes. 2019. Observational measures for effective profiling of healthcare staffs' security practices. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 2. IEEE, 397–404.
[36] Prosper Kandabongee Yeng, Bian Yang, and Einar Arthur Snekkenes. 2019. Framework for healthcare security practice analysis, modeling and incentivization. In *2019 IEEE International Conference on Big Data (Big Data)*. IEEE, 3242–3251.
[37] Prosper Kandabongee Yeng, Bian Yang, and Einar Arthur Snekkenes. 2019. Healthcare staffs' information security practices towards mitigating data breaches: a literature survey. *pHealth 2019* (2019), 239–245.