


## Article

# A comprehensive assessment of human factors in relation to cyber security compliance of healthcare staff in a paperless hospital

Prosper Kandabongee Yeng<sup>1,†,‡</sup>, Muhammad Ali Fauzi<sup>1,\*</sup> and Bian Yang<sup>1,\*</sup>

<sup>1</sup> Norwegian University of Science and Technology; prosper.yeng;muhammad.a.fauzi; bian.yang@ntnu.no

\* Correspondence: prosper.yeng@ntnu.no

† Current address: NTNU, Teknologivegen 22, 2815 Gjøvik

‡ These authors contributed equally to this work.

**Abstract:** Recent reports have it that over 85% of data breaches are still caused by the human element, of which healthcare is one of the suitable organizations mostly targeted by cyber criminals. The work of healthcare staff is often associated with high workloads, high emergency cases, and a broad range of psychological, social, and cultural factors. The significance of these factors could undermine conscious care information security (IS) practice leading to serious violations. This study comprehensively examined the correlation between the psycho-social-cultural factors, work factors with IS and privacy behaviour in a hospital that has fully adopted electronic health records (EHR) management system. The findings are to facilitate decision making process towards improving on the cyber-security practice in healthcare. A quantitative approach was adopted where we collected responses from 212 healthcare staff through an online questionnaire survey. A broad range of constructs were selected from psychological, social, cultural perception and work factors based on earlier review work. These were therefore related with some security practices, to assess the IS knowledge, attitude and behaviour gaps among healthcare staff in a comprehensive way. From the study, IS self-reported conscious care behaviour (ISCCB) risk was relatively higher as compared to information security knowledge (ISK) risks and information security attitude (ISA) risk. Furthermore, the study revealed that work emergency has a positive correlation with ISCCB ( $r=1.95$ ,  $p\text{-value}=0.001$ ) risk. Conscientiousness also had positive correlation with ISCCB risk ( $r=0.157$ ,  $p\text{-value}=0.05$ ) however agreeableness negatively correlated with ISK risk ( $r=-0.166$ ,  $p\text{-value}=0.05$ ), and ISA risk ( $r=-0.140$ ,  $p\text{-value}=0.05$ ). Based on these findings, intrinsic and extrinsic motivation methods combined with cutting-edge technologies can be explored to discourage IS risks behaviours while enhancing conscious care security practice.

**Keywords:** Security practice; Healthcare; Questionnaire design; Questionnaire pretesting

## 1. Introduction

Paperless or folder-less systems is a common term used to denote the adoption of full electronic health records (EHR) systems by hospitals in Ghana. In paperless systems, the hospitals do not use hard copy papers or folders to document and store patient care processes. Instead, all the patient activities at the healthcare facility (such as OPD visits, medical investigations, diagnosis and treatments, inpatient and outpatient documentation, referrals, and ordering of tests ) are carried out in the EHR system [1,2]. The benefits of paperless systems cannot be overemphasized as the systems improve the efficient management of patients information, reduce physical storage space for medical records, and improve clinical decision support [3–5].

In the hindsight, cyber security incidents remain a threat to the use of these ICT systems [6–9,10] of which healthcare systems are among the most targeted systems. Several reasons account for this. Firstly, information security solutions have traditionally been focused on technical measures such as firewall configurations, demilitarise zone (DMZ), Intrusion detection and prevention systems (IDS), authentication, and authorizations in mitigating risks however, the human aspect of IS management

(also called the human firewall) has been given less attention as an important factor in mitigating security issues[11,12]. Meanwhile, current dynamics in security issues can not be resolved with only technical measures especially, in an era where humans are considered the weakest link in the security chain[12–14]. Secondly, healthcare is most suitable for cyber-criminals due to urgency requirement by healthcare staff to access patients records. For instance, in ransomware attack scenario, the healthcare, the authorities would be willing to pay for the ransoms for timely access of patients records.

In view of the above, the goal of this study is to comprehensively assess work factors, psychological, social, and cultural factors that have influence in IS behaviour among healthcare staff. Factors that are found to have significant risks on conscious care security practices can be discouraged with extrinsic motivation(motivations based on external factors eg financial or punishment)[15–17] and intrinsic motivations (incentives that stem out of one's self) [18,19] while promoting factors that have positive impact in IS security practice.

### *1.1. Prior research in security behaviour in healthcare*

Healthcare staff play a vital role in the space of information security as they are required to abide by end user security policies amidst their core duties [20,21]. Failure of that can lead to vulnerabilities that can be exploited to cause internal or external breaches. Therefore in efforts to improve upon the conscious care behaviour of the healthcare staff, it is important to identify and assess a broad range of factors that affect the staff's security behaviour to enable management to "push" the right incentive "buttons" towards improving conscious care security practice. Information security conscious care behaviour of healthcare staff refers to the active compliance with the information security policies and ethics by the healthcare workers in order to safeguard the confidentiality, integrity, and availability (CIA) of the organisational assets [10,22]. Having conducted a study into security requirement Yeng2022Legal, some compliance measures were identified and adopted in this work. These include internet use, email use, social media use, password management, incident reporting, information handling, and mobile computing. These measures were considered because they are more prone to security violations by the human element [10,13].

Prior to this empirical study, various reviews pointed out theory of plan behaviour (TPB), protection motivation theory (PMT), health belief model (HBM), social control (SC), technology acceptance theory (TAT) and personality traits as some of the psychological, social and cultural factors that are used to investigate into information security practices [9,10,23]. Whiles these studies presented knowledge on the overview of all the necessary theories for incentive factors, these methods were not practically assessed in a holistic fashion, but provided a foundation for empirical assessments. Fernandez-Aleman et al evaluated the security practice of healthcare staff in an actual healthcare facility [24]. The study tried to cover this gap and the authors reviewed IS security governance tools such as standards, guidelines and best practices and used that to develop a questionnaire instrument. The instrument was then used to survey 180 healthcare staff to determine their compliance with information security. The study found weak passwords among 62.2% proportion of the staff, half of the respondents failed to protect unauthorised access to patients information and 57% did not also know of the procedure to report security violations. A related study, also assessed healthcare staff security practices with a total of 554 completed questionnaires to understand the security behaviour of healthcare workers in a real hospital. The study also identified significant security gaps among the hospital staff including sharing of computers and passwords [25]. While these studies [24,25] pointed out that the staff of the respective facilities needed both preventive and corrective measures to prevent them from causing security violations, the studies did not pinpoint the exact factors that are influencing these IS security misbehaviour.

Comprehensive factors need to be examined among healthcare workers in relation to their cyber security behaviour. That will give a sense of direction as to how to improve upon the conscious care behaviour of the workers. To this end, Anwar et al conducted a study to find out if gender differences play a role in cyber-security behaviour. Psychological and social factors of PMT and TPB were adopted

as mediating variables. The findings revealed that gender has a significant effect on self-efficacy, prior experience, and computer skills. This was also the right step towards a holistic approach however, other factors relating to knowledge and attitude towards IS security practice were not examined. Additionally, work factors such as workload, and work emergency in healthcare were not as well considered meanwhile all these are important factors that can have a significant effect on IS conscious care behaviour[10,21]. Based on these gaps we empirically assessed the IS self-reported conscious care behaviour (ISCCB) in a holistic way by considering factors from PMT, TPB, HBM, SC, personality traits, and work factors such as workload, work emergency, work experience and IS experience. Additionally, security practices relating to email use, internet use, incident reporting, mobile computing, password management, and information handling [10,13] were adopted in this work.

### *1.2. Problem statement, scope and contribution*

Human factors that contribute to security malpractices are broad. These include psychological, social, cultural, work factors and individual factors. These factors are often investigated into by security researchers towards enhancing security practices. The gap is that the investigations are not comprehensively performed, leaving possible gaps of vulnerabilities in the human element. For instance, Anwar et al investigated into the significance of gender factors in security practice [26]. While this is essential, other variables such as work factors, social, cultural and psychological effect were not examined. Meaning that in enhancing security practice in a typical hospital, issues on individual difference in terms of gender among healthcare staff will be detected and resolved. However, issues relating to other factors of the human element will not be considered that may still leave a security foot-hole among the staff. This study contributed in bridging this gap having adopted a comprehensive approach where a broad range of factors including psychological, social, cultural, individual and work factors were assessed in a comprehensive way.

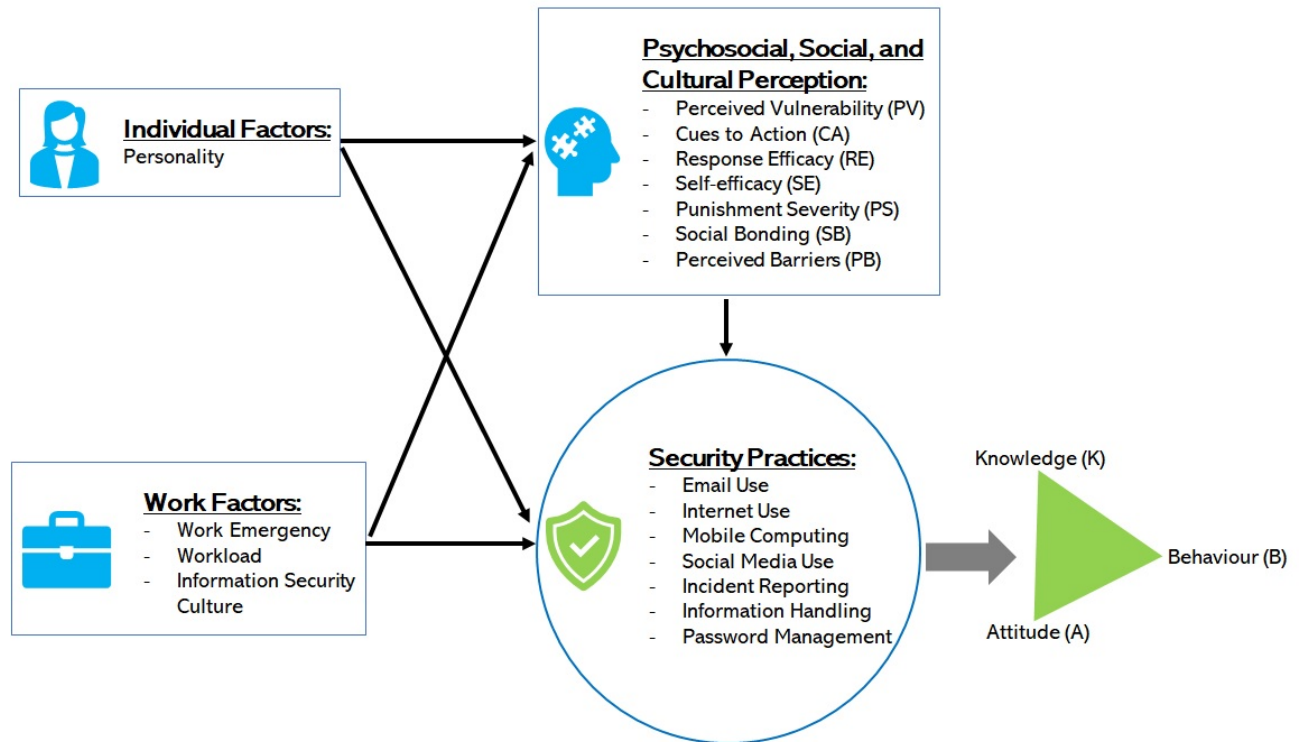
### *1.3. Theory and hypotheses*

Information security (IS) risk behaviour is a security practice by healthcare workers that has the propensity to violate and compromise organisational security measures [22]. So for a healthcare facility to enjoy the benefits that are associated with the use of information systems, it needs to work to reduce these healthcare staff behavioural risks by improving upon their conscious care behaviour. Security practices are lay down rules by leaders in healthcare facilities that require the healthcare staff to abide by these in order to enhance the CIA of the healthcare systems and assets. The compliance can be influenced by the knowledge, attitude, and behaviour of the healthcare staff among other factors. Adapting from PMT, TPB, HBM, SC, personality traits, and work factors we investigated into broad range of constructs as shown in Table 1. These factors were related to the security practice measures as shown in figure 1, having associated the measures with both the IS risk of perception as independent variables and the risk of the knowledge, attitude, and behaviour (KAB) as dependant variables.

This approach is more comprehensive and covers healthcare staff behavioural factors that commonly have an effect on IS security[9,10,21] in healthcare. Though other factors such as organizational factors, and leadership play significant effects in IS security, our scope and focus are on factors that relates to the healthcare staff in this work.

#### *1.3.1. Theory of planned behaviour and Knowledge, attitude and behaviour*

The theory of planned behaviour was proposed by Ajzen et al and it explains the effect of attitude, subjective norms and behavioural control on the behaviour of individuals [22,27]. Attitude relates to a person's beliefs and feelings which are directly influenced by what they know(K) of the IS measures. Both attitude and knowledge can have a direct and indirect effect on the individual's security practice [22,28]. So the conscious care behaviour is a function of the knowledge and attitude towards the security policies that are kept in place by the healthcare management. Information security conscious care behaviour (ISCCB) is actually the level of compliance with the IS policy by healthcare staff. The



model.jpg

Figure 1. study model

behaviour, knowledge, and attitude of the healthcare staff tend to be risky if the compliance level tends to compromise confidentiality, integrity, or availability of healthcare systems and assets. Healthcare staff's knowledge of the security policies also has a direct effect on their attitude. The knowledge is often acquired through their experience, observations, training, and awareness [29]. The attitude of the healthcare staff towards IS policies refers to their positive or negative intentions towards a specific behaviour. It is a learned tendency to behave in a particular way towards a security policy [30]. As the knowledge of a particular policy influences attitude, the relative behaviour in that context is adjusted accordingly. Attitude has explicit and implicit dimensions. In explicit attitude, the individuals are aware of the effect of their behaviour while in implicit attitude, the individuals are unconscious of the effect of their behaviour [31]. Various studies showed significant correlations between these constructs in the context of IS behaviour [13,32].

In this study, we therefore hypothesize that

- H1: Low risk of the hospital's healthcare staff's IS knowledge (ISK) risk and attitude (ISA) risk respectively have a positive correlation with their IS self-reported behavioural (ISCCB) risk.

Furthermore, the healthcare environment is associated with work emergencies such as accident cases and other life-threatening health conditions [10,33,34]. These cases mostly require urgent and timely interventions from the healthcare professionals without which the patient condition could worsen. This is important that hospitals have dedicated units or departments for emergency cases equipped with resources to provide timely interventions for emergency patients. Additionally, a high workload on healthcare personnel has become a huge burden on the few staff which is threatening the effectiveness of health delivery [35]. This has been attributed to various reasons including funding gaps and an increase in patients to clinicians ratio [9,36]. The spontaneous question is, how do healthcare

**Table 1.** Study constructs and their theoretical origin

No.	Construct	Theory
1	Perceived vulnerability risk	PMT
2	Cues to action with risk	HBM
3	Response efficacy risk	PBM,PMT
4	Self efficacy risk	PMT,HBM
5	Punishment severity risk, Social bonding risk	Social control
6	IS culture risk	TPB
7	Perceived barriers risk	HBM, PMT
8	Agreeableness, Conscientiousness, Extraversion, Openness, Neurotism	Personality
9	Workload, work emergency	
10	Information security knowledge (ISK) risk	
11	Information security attitude (ISK) risk	
12	Information security self-reported conscious care behaviour (ISCCB)risk	

workers observe good security practice amidst work emergencies and high workloads? To this end, our second hypothesis (H2) is that

- Work-related factors (work emergency and workload) and security culture have influence on the hospital staff’s self-reported ISCCB.

1.3.2. Personality and KAB

Personality traits are inherent characteristics of individuals which are developed from biological and environmental factors [37,38]. It is a psychological attribute that has been studied to have an influence on security practice [39]. Others have the view that personality traits are more stable over time when compared with attitude construct [10,39–41]. Essentially, there are five common personality traits as outlined and defined below [39–41]:

- Agreeableness is a measure of an individual’s tendencies with respect to social harmony. This trait reflects how well the individual gets along with others, how cooperative or sceptical they are, and how they might interact within a team.
- Conscientiousness is a measure of how careful, deliberate, self-disciplined, and organized an individual is. Conscientiousness is often predictive of employee productivity, particularly in lower-level positions.
- Extraversion is a measure of how sociable, outgoing, and energetic an individual is. Individuals who score lower on the extraversion scale are considered to be more introverted, or more deliberate, quiet, low key, and independent. Some types of positions are better suited for individuals who fall on one side of the spectrum or the other.
- Openness measures the extent to which an individual is imaginative and creative, as opposed to down-to-earth and conventional.
- Nerotism or Stress Tolerance measures the ways in which individuals react to stress.

In measuring the security practice of healthcare staff, we hypothesize that (H3):

- H3: Healthcare staff personality traits of agreeableness, conscientiousness, neuroticism, openness and extraversion have a significant correlation with their information security risk of knowledge, Attitude and behaviour (KAB).



### 1.3.3. Perception

Psychological, social, and cultural perception in relation to information security effects has largely been considered to be very important in the assessment of human factors in IS [15,22,26]. Therefore, we included perceived vulnerability risk (PV), perceived cues to action risk (CA), response efficacy risk (RE), perceived self-efficacy (SE), punishment severity risk (PS), social bonding, or informal social control risk (SB) and perceived barrier risk (PB). These were drawn from HBM [42], PMT [26,43] and social control[44]. These variables were in line with the study objectives and were formed from various psychological, social, and cultural theories. In this regard, we hypothesized that:

- H4: personality and work factors have a significant effect on the perceived risk of PV, CA, RE, SE, PS, SB and PB.

## 2. Our Approach

### 2.1. Participants and data collection

Convenience sampling was adopted in the recruitment process of the hospitals and their participants. First, healthcare facilities that adopted "folder-less" systems were invited to join the survey. Some health facilities in Ghana volunteered to take part in the study. Based on ethical, privacy and security reasons, the names and locations of these facilities have not been mentioned in this paper but ethical clearance was duly obtained in Ghana. Following that, research coordinators were appointed to liaise with the management of these hospitals (ie the administrators and medical directors) to form social network groups where the healthcare staff were invited to fill the online survey. Specifically, WhatsApp application [45] group was created by the coordinators. The healthcare staff was then invited to join these groups in order to fill out the questionnaire instrument relating to IS security practice of the hospital. The link to the questionnaire instrument was posted in the group. Due to the high cost of the internet data bundles in Ghana, the participants were to fill out the questionnaire and receive a reimbursement of their internet data of an estimated amount of GHS 10.00 ( which is about 1.67 United States dollars). There was a consent form to which each participant agreed prior to taking part in the survey. The survey started in March 2021 and was closed in May 2021 of which a total of 233 (Female=114, Male = 119) delivered their responses.

### 2.2. Instrument and measurements

This statistical survey was conducted based on earlier studies [9,10,21,46], where a comprehensive security practices were identified [10,28,46] and psychological, social and cultural factors[10,21] were also identified. The questionnaire instrument was therefore developed with 44 security practice measures to measure the knowledge, attitude and behaviour (KAB) risk in relation to other factors of the healthcare staff [28]. The structure for the questionnaire items is shown in ?? The questionnaire items were also developed to measure the psychological, social, and cultural perceptions of the end users in the hospital. Seven questions also covered the staff demographics, and two items each were also developed to respectively measure the workload, work emergency, and personality constructs of the healthcare staff. The brief version of personality items were used [47] because the healthcare workers do not have much time to answer the entire 240 items of the long personality scale. In addition to that, as the main focus of this study is not about personality, the short version has been assessed to meet the scale requirements [24,26,28,47]. The entire instrument for this study was pretested by combining conventional pretesting [48–50] and behaviour coding method[51,52]. The issues with the questionnaire were then identified to include unclear questions, the insignificant differences between questions, problematic questions, inadequate questions, complex terms, and many questionnaire items. A total of 50 questionnaire items were identified to have problems after the pretesting was conducted with a total of 36 respondents in behaviour coding and 21 respondents in conventional pretesting.

**Table 2.** Rule of Thumb on Cronbach Alpha [59,60]

Alpha Coefficient Range	Strength of association
<0.6	Poor
0.6 to < 0.7	Moderate
0.7 to <0.8	Good
0.8 to <0.9	Very Good
0.9	Excellent

The synergy of the pretesting was necessary to ensure a thorough assessment of the questionnaire for effective correction prior to actual use. So the identified errors were corrected prior to the actual use of the instrument.

Three attention checkers were introduced in the study and required the respondents to select specific answers. Respondents who answered at least two of these checkers wrongly suggest that they did not really pay attention while responding to the instrument. This is one of the common methods being used in surveys and it does not affect the validity of the instrument [13,47,53–56].

2.3. Statistical analyses

Pearson’s correlation, descriptive statistics, and statistical hypothesis testing methods were used in the analysis and tests. The choice was based on the specific characteristics of the data set being involved. For instance, aside from the IS risk behaviour, the skewness of IS knowledge risk and IS attitude risk were slightly skewed as shown in figure 5, and table 5. Therefore, Pearson’s correlation was adopted as the distribution was approximately normal [32,57]. Furthermore, t-test and Kruskal Wallis non-parametric one way ANOVA methods were adopted based on the nature of the data-set in the test scenario. Levene’s tests were performed when required to determine the variation significance among the test groups[24]. IBM SPSS statistical package version 7 was used for the data analysis. The reliability of the constructs was measured using Cronbach alpha. Reliability is the extent to which the items are measuring the same underlying construct[58]. Mostly, the coefficient of the Cronbach alpha value is expected to be above 0.6 but these values are dependent on the number of items in the scale [59–63].

If the number of items in a scale are 10 or more, it is reasonable to record the coefficient of Cronbach alpha to be 0.6 or higher (as shown in Table 2) [59,60] else, it is normal to record the Cronbach alpha values to be lower with an optimal range of 0.2 to 0.4.

3. Results

This section presents the findings of the analysis. As shown in Table 3, the reliability statistics of the Cronbach alpha of all the constructs were within the range of moderate and good strength. Those scales in which the number of items were less than 10 also fell within the optimal range of 0.2 to 0.4 alpha coefficient. To this end, the results of the various factors are presented in the subsequent subsections.

The normality of the distribution of the responses was also checked to guide in the choice of methods for the analysis. Absolute skewness of less than 0.5, suggests that the distribution is pretty symmetric but if the skewness is between 0.5 and 1, then it is slightly skewed [64]. Skewness that is greater than 1 or less than -1, means that it is highly skewed. Additionally, a perfect normal distribution has a kurtosis of zero. Considering means of the distributions in figure 5 (1.59) and figure 5 (1.88) of IS risk knowledge and IS risk attitude of the responses, more healthcare workers tend to have less risky IS practice knowledge and attitude however, the security practice pattern in the IS risk behaviour showed fairly uniform distribution, suggesting that distribution of healthcare workers in terms of their risk behaviour is uniform in both high risk and low-risk regions.

**Table 3.** Reliability statistics

Constructs	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
Psycho-socio-cultural cyber security practice	0.739	0.729	44
Information Security Risk Knowledge (ISK)	0.551	0.566	9
Information Security Risk (ISA)	0.652	0.654	13
Information Security Risk Conscious care behaviour (ISCCB)	0.622	0.612	10
Perceived Barriers (PB)	0.769	0.776	3
Perceived Vulnerability (PV)	0.021	0.018	3
Cues to Action (CA)	0.505	0.543	5
Response Efficacy (RE)	0.481	0.472	3
Perceived self-efficacy (PSE)	0.413	0.406	3
Punishment certainty (PC)	0.600	0.585	6
Social Bonds and Pressure (SBP)	0.633	0.645	7
Cultural factors (CF)	0.462	0.518	5



3.0.1. Nature of the respondents

With reference to figure 2 and Table 4, the participants of the study included various groups such as administrative officers (including CEO, top-level management, etc.), pharmacists (including dispensing personnel), doctors (all physicians and physician assistants), nursing (all categories of nurses including nurse assistant), IT Personnel (Including all IT staff), researcher/research assistant and statisticians. Other groups who also took part in the study were public health officers, claims officer, health information officers, physiotherapists, records officers, clinical laboratory personnel, and internal auditor. These were categorised into Operational staff (Doctors, Nurses, IT staff, equipment engineers, etc.), managers and supervisors and executive category (including CEO, director, top-level management, etc.).

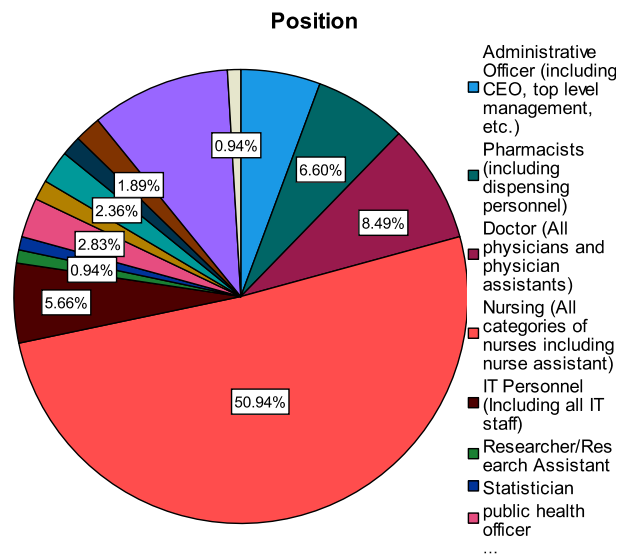


Figure 2. Role Categories of Respondents

The total valid participants who were included in the analysis were 212 with averagely, the same proportion of representation of males (50.5%) and females (49.5%) as shown in table 4. Out of this, nurses constituted the majority proportion of 50.9% followed by clinical laboratory personnel (9.9%) and followed by doctors (8.5%). Additionally, both gender constituted the majority of the young population from 21 years to 40 years as shown in figure 4. In terms of gender among the hospital roles, female nurses were more dominant and constituted about 68.7% of the female working population followed by 33.34% of male nurses among the males' healthcare workers as shown in figure 3. Comparatively, few of the workers (8.9%) had less than 1-year healthcare work experience as a higher proportion of the workers (39.15%) had between 1 to 5 years experience and beyond as shown in table 4.

From the total number of 42 questionnaire items which were measuring the intended security practice in terms of knowledge (K), attitude (A), and behaviour (B) risks, the information security knowledge (ISK) risk was averagely lower, followed by the information security attitude (ISA) risk however, the information security behaviour (ISCCB) risk was comparatively higher as shown in figure4.

The figure5, ?? and 5respectively showed the distribution of responses of the intended security practice in terms of knowledge, attitude and behaviour. The number of respondents (frequency) was distributed over the IS security risk intention practices from low (1=Agree) to high risk IS practice (5=Disagree). Knowledge and attitude related risks construct were positively skewed as shown in the table5, figure5 and ??, while behaviour risks showed uniform distribution as shown in the figure??.

**Table 4.** Participants demographics

Variable	Category	N	%
Gender	Male	107	50.5%
	Female	105	49.5%
Age	17-20	2	0.9%
	21-30	77	36.3%
	31-40	104	49.1%
	41-50	20	9.4%
	51-60	8	3.8%
	Over 60	1	0.5%
Position	Administrative Officer (including CEO, top level management, etc.)	12	5.7
	Pharmacists (including dispensing personnel)	14	6.6
	Doctor (All physicians and physician assistants)	18	8.5
	Nursing (All categories of nurses including nurse assistant)	108	50.9
	IT Personnel (Including all IT staff)	12	5.7
	Researcher/Research Assistant	2	0.9
	Statistician	2	0.9
	public health officer	6	2.8
	Claims Officer	3	1.4
	Health Information Officer	5	2.4
	Physiotherapist	3	1.4
	Records officer	4	1.9
	Clinical laboratory personnel	21	9.9
	Internal auditor	2	0.9
	Total	212	100.0
Position Level	Operational staff (Doctors, Nurses, IT staff, equipment engineer, etc.)	165	77.8%
	Managers and supervisors	44	20.8%
	Executive (including CEO, director, top level management, etc.)	3	1.4%
	Less than 1 Year	19	9.0%
Experience	1-5 Years	83	39.2%
	6-10 Years	53	25.0%
	11-15 Years	40	18.9%
	16-20 Years	9	4.2%
	21-25 Years	5	2.4%
	Greater than 25	3	1.4%

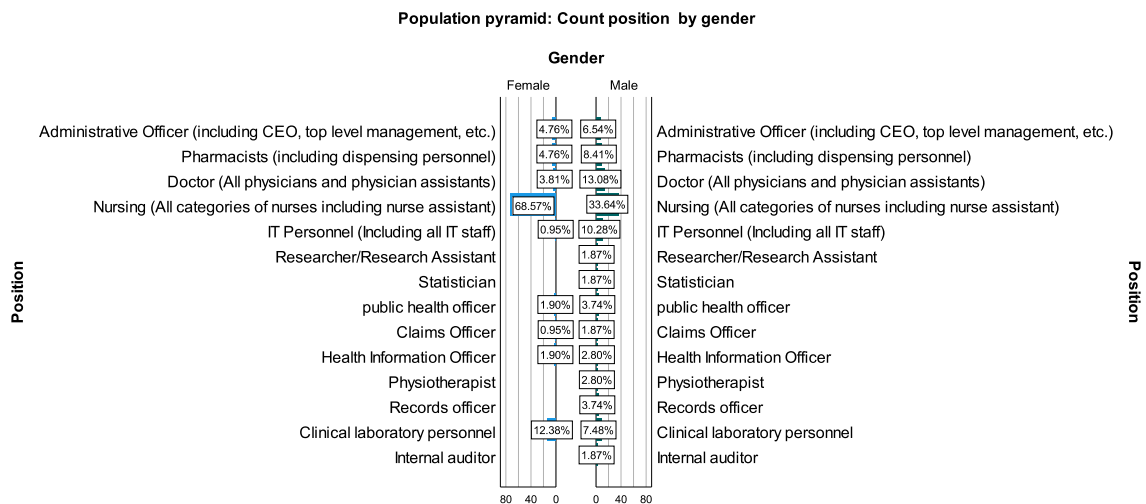


Figure 3. Position distribution among gender

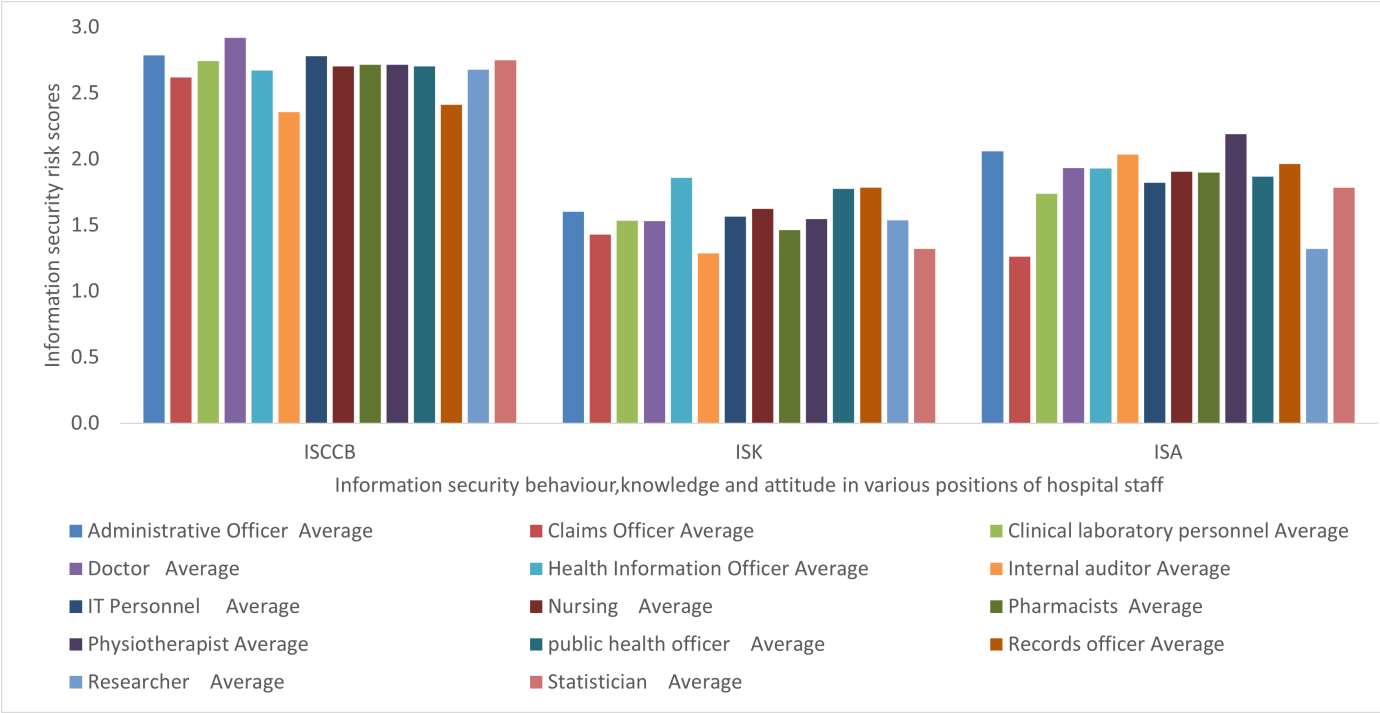
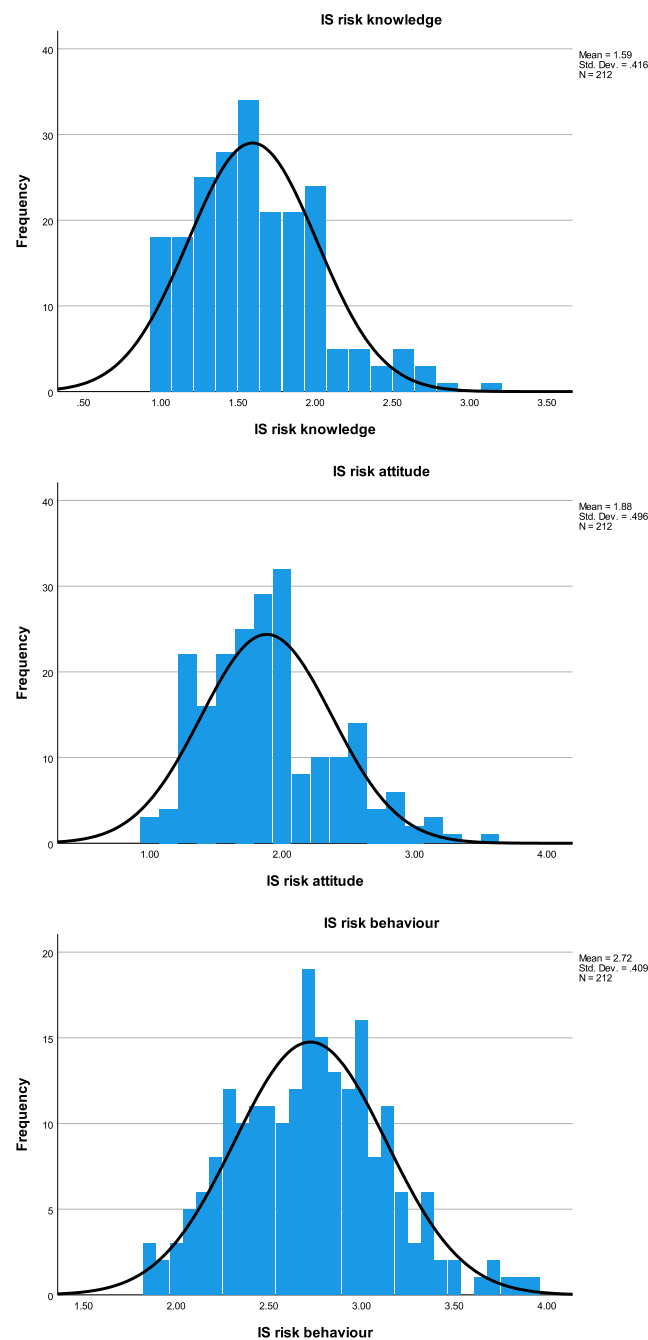


Figure 4. Comparison of KAB security practice risk among healthcare staff

3.0.2. Work factors in relation to security risk knowledge, attitude and behaviour (KAB)

In assessing the correlation of work factors (workload and work emergency) as shown in the table6, on one hand, information security risk knowledge, information security risk attitude, and information security risk behaviour (KAB) on the other hand, Information security (IS) risk behaviour has a significant positive correlation with work emergency ( $r=0.195$ ,  $p=0.01$ ), IS knowledge risk ( $r=0.287$ ,  $p=0.01$ ) and IS risk attitude ( $r=0.380$ ,  $p=0.01$ ), however, the workload had insignificant correlation ( $r=0.011$ ,  $r=0.005$ , and  $r=0.011$ ) with any of the KAB risk variables.

[!h]



**Figure 5.** Distribution of knowledge IS practice

### 3.0.3. Correlations between personality traits and security risk of KAB

In the analysis of personality traits and security risk of knowledge, attitude, and behaviour, agreeableness has a significant negative correlation with both IS risk knowledge (-0.166) and IS risk attitude (-0.140) at a p-value of 0.05 but it had no significant correlation with IS risk behaviour as shown in the Table 7. So Staff's who have agreeableness personality have low-risk security practices in terms of knowledge and attitude. However, conscientiousness showed a positive significant correlation (0.157) at a p-value of 0.05, suggesting that healthcare workers with conscientiousness traits tend to be in the high-risk category of IS risk behaviour.

**Table 5.** Skewness of IS security practice

		IS risk knowledge	IS risk attitude	IS risk behaviour
N	Valid	212	212	212
	Missing	0	0	0
Mean		1.5947	1.8841	2.7244
Std.		.41645	.49570	.40940
Deviation				
Skewness		.765	.657	.238
Std.		.167	.167	.167
Error of Skewness				
Kurtosis		.562	.155	-.050
Std. Error of Kurtosis		.333	.333	.333

**Table 6.** Correlations between work load, work emergency and security risk of knowledge, attitude and behaviour

	Work load	Work Emergency	ISK	ISA	ISCCB
Workload	1	.420**	.011	.005	.011
Work Emergency	.420**	1	-.040	-.042	.195**
ISK	.011	-.040	1	.578**	.287**
ISA	.005	-.042	.578**	1	.380**
ISCCB	.011	.195**	.287**	.380**	1

\*\*. Correlation is significant at the 0.01 level (2-tailed).

**Table 7.** Correlations between personality traits and security practice

	IS knowledge	IS risk attitude	IS risk behaviour
Extraverted	-0.042	-0.043	0.022
Agreeableness	-.166*	-.140*	0.124
Conscientiousness	-0.049	0.033	.157*
Neurotism	0.054	0.047	0.132
Openess	-0.027	-0.128	-0.110

\*\*. Correlation is significant at the 0.01 level (2-tailed).

\*. Correlation is significant at the 0.05 level (2-tailed).

### 3.0.4. Correlations between perception and personality traits

From Table 8, healthcare staff with agreeable traits have significant positive correlation ( $r=0.163$ ,  $p\text{-value}=0.05$ ) with self-efficacy risk, but showed negative correlation ( $r=0.147$ ,  $p\text{-value}=0.05$ ) with punishment severity risk. In addition, cue to action risk showed positive correlation with conscientiousness ( $r=0.159$ ,  $p\text{-value}=0.05$ ) and Neuroticism ( $r=0.152$ ,  $p\text{-value}=0.05$ ). Meanwhile, openness has a significant negative correlation with social bonding ( $r=-0.170$ ,  $p\text{-value}=0.05$ ).

### 3.0.5. Perception in relation to work factors

The analysis of the psychological, social, and cultural perceptions in relation to work factors such as workload, hospital security culture, and work emergency are shown in Table 9. The perception variables have an insignificant correlation with work emergency and workload with the exception of response efficacy and punishment severity risks which respectively have a significant negative

**Table 8.** Correlations between perception and personality

	Extraverted	Agreeableness	Conscientious	Neurotism	Openess
Cues to action risk	0.123	0.069	.159*	.152*	-0.092
Response efficacy risk	-0.096	0.060	-0.057	0.063	-0.078
Self efficacy risk	0.069	.163*	0.122	0.146	0.027
punishment severity risk	-0.029	-.147*	-0.018	0.019	-0.087
Social bonding risk	-0.002	-0.129	0.115	0.027	-.170*
IS culture risk	0.045	-0.070	-0.009	0.044	-0.130
Perceived barriers risk	-0.023	-0.039	0.044	0.090	0.003

\*. Correlation is significant at the 0.05 level (2-tailed).

correlation with hospital IS the culture of ( $r=-0.182$ ,  $p\text{-value}=0.05$ ) and ( $r=-0.177$ ,  $p\text{-value}=0.01$ ) respectively.

**Table 9.** Correlations between perception and work factors

	Work Load	Work emergency	Hospital IS Culture
Cues to action risk	-0.028	0.015	-0.007
Response efficacy risk	-0.044	0.026	-.182*
Self efficacy risk	-0.023	0.079	-0.076
punishment severity risk	0.040	-0.028	-.177**
Social bonding risk	-0.011	0.004	-0.034
IS culture risk	0.001	0.106	-0.068
Perceived barriers risk	0.019	0.127	-0.064

\*\* Correlation is significant at the 0.01 level (2-tailed).  
\* Correlation is significant at the 0.05 level (2-tailed).

### 3.0.6. statistical tests of IS risk knowledge, attitude and behaviour (KAB) with categorical variables

Statistical tests were conducted to test the distribution of IS risk knowledge, attitude, and behaviour across categorical variables including gender, position levels, hospital IS experience, age group, and healthcare work experience. T-test was used for the hypothesis between gender and KAB risk variables since t-test is normally used for testing 2-level categorical variables with continuous variables. Additionally, Levene's test, which was analysed, did not show significant variances among the group's population of the three KAB variables ( $r=0.412$ ,  $r=0.406$ ,  $r=0.632$ ) at a  $p\text{-value}$  of 0.05.

Furthermore, Kruskal Wallis non-parametric one way ANOVA was used in the hypothesis testing with the remaining variables such as position levels, hospital IS experience, age group, and healthcare work experience as these variables were more than two levels. Aside from work experience in healthcare, the statistical tests show that the distribution of IS risk of KAB is the same across all variables. With regards to experience in healthcare, the distribution of IS risk knowledge and IS risk attitude were uniform across all the healthcare experience groups but the distribution of IS risk behaviour across all the work experience groups did not show uniform distribution with a significance level of ( $r=-0.00$ ,  $p\text{-value}=0.05$ ) as shown in the table??.



**Table 10.** Kruskal Wallis non parametric one way ANOVA with work experience and KAB

	Null Hypothesis	Test	Sig.a,b	Decision
1	The distribution of IS risk behaviour is the same across categories of 5_experience_healthcare.	Independent-Samples Kruskal-Wallis Test	0.000	Reject the null hypothesis.
2	The distribution of IS risk knowledge is the same across categories of 5_experience_healthcare.	Independent-Samples Kruskal-Wallis Test	0.624	Retain the null hypothesis.
3	The distribution of IS risk attitude is the same across categories of 5_experience_healthcare.	Independent-Samples Kruskal-Wallis Test	0.582	Retain the null hypothesis.

Therefore, the post-hoc pairwise test was analysed to determine the distribution among the groups. The results indicate that there are significant difference (p-value=0.05) of IS security behaviour among various groups such as 7(>25years)-2(1 to 5 years)= (0.019), 7(>25)-4(11 to 15 )= 0.013, 7(>25)-3(6 to 10)=0.003, 7(>25)-5(16 to 20years)=0.001, 7(>25)-6(21-25years)=0.002 and others as shown in table 11 at Significance level of 0.05 or less.

#### 4. Discussion

This study assessed various factors that affect sound security and privacy behaviour among healthcare workers. The purpose was to determine gaps in their security practice and to find out if some of the factors have negative effects on the security practices. This would provide guidance for the choice of better mitigation strategies such as incentive measures to improve security practices. This study is much centred on the human element among the three pillars of effective cyber-security practice thus processes, technology, and the people[65,66].

##### 4.0.1. Principal findings

The study was characterised by almost equal proportion of both male and female participants and was also dominated by nurses by more than half (50.9%) of the total participants. In terms of distribution of the risk of security practice in the aspect of knowledge, attitude, and behaviour (KAB), there was generally uniform distribution of the behaviour risk while knowledge and attitude risks slightly skewed to the positive side as shown in figure 5. The results further showed a significant positive correlation between information security knowledge (ISK) risk, information security attitude (ISA), work emergency, and information security-conscious care behaviour (ISCCB) as shown in Table 6 and Table 12. Additionally, while agreeableness had a negative correlation with ISK and ISA,

**Table 11.** Post-hoc pairwise test with null hypothesis: Sample 1 and sample 2 distribution are the same

Sample 1(Year)-Sample 2(Year)	Test Statistic	Std. Error	Std. Test Statistic	Sig.
7(>25)-1(<1 )	55.263	38.080	1.451	0.147
7(>25)-2(1 to 5 )	84.476	36.022	2.345	0.019
7(>25)-4(11 to 15 )	91.550	36.692	2.495	0.013
7(>25)-3(6 to 10)	109.623	36.376	3.014	0.003
7(>25)-5(16 to 20)	130.667	40.863	3.198	0.001
7(>25)-6(21-25)	137.700	44.763	3.076	0.002
1(<1)-2(1 to 5)	-29.213	15.589	-1.874	0.061
1(<1)-4(11 to 15)	-36.287	17.078	-2.125	0.034
1(<1)-3(6 to 10)	-54.359	16.390	-3.317	0.001
1(<1)-5(16 to 20)	-75.404	24.803	-3.040	0.002
1(<1)-6(21-25)	-82.437	30.808	-2.676	0.007
2(1 to 5)-4(11 to 15)	-7.074	11.798	-0.600	0.549
2(1 to 5)-3(6 to 10)	-25.147	10.777	-2.333	0.020
2(1 to 5)-5(16 to 20)	-46.191	21.511	-2.147	0.032
2(1 to 5)-6(21-25)	-53.224	28.225	-1.886	0.059
4(11 to 15)-3(6 to 10)	18.073	12.838	1.408	0.159
4(11 to 15)-5(16 to 20)	-39.117	22.614	-1.730	0.084
4(11 to 15)-6(21-25)	-46.150	29.075	-1.587	0.112
3(6 to 10)-5(16 to 20)	-21.044	22.098	-0.952	0.341
3(6 to 10)-6(21-25)	-28.077	28.676	-0.979	0.328
5(16 to 20)-6(21-25)	-7.033	34.189	-0.206	0.837

conscientiousness had a significant positive correlation with ISCCB as shown in Table 9 and Table 12. Essentially, Table Table 12 consists of a gist of the study results that showed significant correlations. These are further discussed in the subsequent subsections.

#### 4.1. Risk of knowledge, attitude and behaviour(KABs)

Security practice by end users is required to be observed by the healthcare workers in a bit to enhance the confidentiality, integrity, and availability (CIA) of the systems. The most common measures include password management, incident reporting, email use, social media use, mobile computing, and information handling [13,67]. Mostly, these security practices are observed based on the healthcare facility's security policies which are literally the "law" to be followed by the healthcare workers in order to avoid security breaches. From our assessment, ISCCB risk positively correlated with both ISK risk and ISA risk as shown in the Table 12. Additionally, ISK and ISA also have a positive

Table 12. Summary of results

No	Varaible 1-Variable 2	Value
1	Work Emergency-ISCCB	.195**
2	ISA-ISK	.578**
3	ISA-ISCCB	.380**
4	ISK-ISCCB	.287**
5	ISCCB-Conscientiousness	.157*
6	ISA-Agreeableness	-0.1407*
7	ISK-Agreeableness	-.166*
8	Self Efficacy-Agreeableness	.163*
9	Punishment severity-Agreeableness	.163*
10	Cuest to action-Conscientiousness	.159*
11	Cuest to action-Neurotism	.152*
12	Social bonding-Openness	-0.170*
13	Response efficacy risk-Hospital IS Culture	-.182*
14	Formal social control risk-Hospital IS Culture	-.177**

significant correlation. This could mean that better ISK and ISA risks of the staff could significantly influence better conscious care behaviour which supports our first hypothesis (H1). Related studies by [13,67] found a similar pattern. Management can therefore use various state-of-the-arts methods to influence the ISCCB of healthcare workers by improving upon heir knowledge and attitude.

Additionally, the findings also showed a significant positive correlation between work emergency and ISCCB but not workload. It is possible that workload does not create urgency and does not interfere much with the healthcare security practice as compared to work emergency does[68–73]. In a healthcare emergency situation, the main goal of the medical staff is to save the life of the patient or to prevent the worsening of the patient condition. Observing good information security practice might be the least priority by the healthcare staff [72,73] and they may tend to circumvent some of the security and privacy measures just to enable them to perform their core duties if those measures obstruct their work. As healthcare emergency correlated with the risk of ISCCB in the positive direction, incentive measures including usable security measures are required to promote sound security practice. Otherwise, with all the urgency in healthcare, the severity of the impact of security breaches in healthcare would be much higher in incident situations [74].

Individual differences were also assessed with the KAB variables as our third hypothesis(H3). The findings showed that agreeableness has a significant negative correlation with ISK risk and ISB risk but not ISCCB. However, healthcare workers with high conscientiousness trait tend to have a significant positive correlation with the risk of ISCCB but not ISK and ISA risks as shown in Table 12. With a negative correlation, between the risks of ISK and agreeableness as well as ISA and agreeableness, it implies that the risk of cyber security practice of knowledge and attitude tend to reduce with healthcare workers who have higher scores with agreeable personalities and vice versa. This could be the case because healthcare staff with a high score of agreeableness characteristics tend to easily agree with cyber security education and training, enabling them to have low risk in ISk and ISA. This finding is in line with previous studies [75,76]. Conversely, the healthcare workers with a high risk score of conscientiousness showed higher ISCCB risk which is in contrast to our hypothesis and previous studies[75,76]. Our assumption was that a higher score of conscientiousness would have translated into less risk ISCCB. It is possible that the workers with a high risk score of conscientiousness equally have high self-esteem, giving them false confidence of conscious care security practice[77].

#### 4.2. Personality and psycho-socio-cultural security behaviour

The healthcare workers (just like any person) are complex in nature and this is exhibited in their security-conscious care behaviour. For instance, healthcare workers are social beings [78], who work with friends, family members, and other relations which can have an impact on security measures. This expresses the need to consider social factors in an effort to estimate the security behaviour of a hospital [15,22,44,75,76].

The results showed that only extroversion did not have a significant correlation with any of the psycho-social-cultural traits but agreeableness was a significant positive predictor of self-efficacy risk and punishment severity risks. This translates that healthcare workers with agreeable characters tend to have high-risk behaviour in terms of self-efficacy and punishment severity. Related studies found significant correlations among agreeableness versus self-efficacy risk [75,76] but not self-efficacy and agreeableness. Agreeable personality traits are very cooperative, helpful, and kind but require similar treatment [76] and such personalities may feel they will not be punished and would be treated with kindness if they violate security and privacy policies regarding self-efficacy and punishment severity.

Also, conscientiousness and neuroticism had a significant positive correlation with cues to action. This implies that higher risks of cues to action behaviour corresponded to staff with higher scores in neuroticism and conscientiousness traits. The finding of higher risk of security practice in relation to neuroticism traits is in line with earlier studies [13,41,75,76] of self-reported cyber security behaviour. Staff with neuroticism traits tend to have higher risk behaviour, suggesting that, staff with emotional stability is a predictor of low cues to action security risk behaviour. Furthermore, self-reported hospital information culture was found to have a significant negative correlation with both response efficacy and punishment severity risks behaviour as shown in table 12 and table 8. This can be interpreted to be the case that, higher scores or better hospital security culture predicts low risk of both response efficacy and punishment severity risks. This finding is similar to a related study in which subjective norms were found to be significant to self-reported cyber security behaviour [22]. In this vein, healthcare facility management can improve upon the cyber security practice in the area of response efficacy and punishment severity by improving upon the security culture of the hospital through self-efficacy and punishment severity related incentives.

#### 4.3. Implication of the study

The study has various implications. Firstly, the security knowledge among healthcare staff can be improved to enhance their attitude and behaviour. Secondly, usable security measures can be assessed and implemented such that amidst work emergency, the healthcare staff can subconsciously comply with security and privacy measures. Finally, psychological perceptions in relation to individual factors such as personality, can be influenced with the state-of-the-arts training, education and learning (TEL) to improve on security practice. For instance, state-of-the-arts approaches such as Virtual reality (VR) is able to elicit 27% higher emotional engagement than television. Also, learners who use VR retain 75% of what they are taught as compared to 10% of that of the traditional methods. Additionally, surgeons trained using VR make less errors and spent less time in cases as compared to surgeons who are conventionally trained [79,80].

### 5. Conclusion

Digitising hospital operations into paperless systems has a lot of benefits for management, staff, and the patients. But this also comes with its associated risks including the threats of cyber security. Therefore, the security behaviour of healthcare staff was assessed to determine gaps and variables that can be improved towards enhancing conscious care security practice.

A survey was therefore conducted in a typical, paperless hospital in Ghana by collecting self-reported cyber-security practices of healthcare staff in psychological, social, and cultural aspects in addition to work-related factors such as workload and work emergency.

The findings showed that work emergency, information security knowledge risks, and information security attitude risks have significant positive correlation with their self-reported information security-conscious care behaviour risks. In the aspect of psycho-socio-cultural behaviour, the study showed that healthcare staff with the higher scores in agreeableness, openness and hospital information security culture tend to respectively have low cyber security risk behaviour in ISK and ISA, social bonding and response efficacy as well as punishment severity. However, consciousness correlated with high risks of information security-conscious care behaviour and punishment severity which is in contradiction with other studies.

Inference from the findings suggests that cutting-edge technologies such as mixed and extended reality, and usable security solutions can be explored to improve security practice amidst emergency situations that are characterised in healthcare. Future studies can explore qualitative approach to obtain the nuances of security gaps and factors towards improved decision making for better security countermeasures.

## Appendix A.

### References

- Schumaker, R.P.; Reganti, K.P. Implementation of electronic health record (EHR) system in the healthcare industry. *International Journal of Privacy and Health Information Management (IJPHIM)* **2014**, *2*, 57–71.
- Zandieh, S.O.; Yoon-Flannery, K.; Kuperman, G.J.; Langsam, D.J.; Hyman, D.; Kaushal, R. Challenges to EHR implementation in electronic-versus paper-based office practices. *Journal of general internal medicine* **2008**, *23*, 755–761.
- Miriovsky, B.J.; Shulman, L.N.; Abernethy, A.P. Importance of health information technology, electronic health records, and continuously aggregating data to comparative effectiveness research and learning health care. *Journal of Clinical Oncology* **2012**, *30*, 4243–4248.
- Hossain, A.; Quaresma, R.; Rahman, H. Investigating factors influencing the physicians' adoption of electronic health record (EHR) in healthcare system of Bangladesh: An empirical study. *International Journal of Information Management* **2019**, *44*, 76–87.
- Dagliati, A.; Malovini, A.; Tibollo, V.; Bellazzi, R. Health informatics and EHR to support clinical research in the COVID-19 pandemic: an overview. *Briefings in bioinformatics* **2021**, *22*, 812–822.
- Rahman, T.; Rohan, R.; Pal, D.; Kanthamanon, P. Human Factors in Cybersecurity: A Scoping Review. The 12th International Conference on Advances in Information Technology, 2021, pp. 1–11.
- Pollini, A.; Callari, T.C.; Tedeschi, A.; Ruscio, D.; Save, L.; Chiarugi, F.; Guerri, D. Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work* **2021**, pp. 1–20.
- Van Deursen, N.; Buchanan, W.J.; Duff, A. Monitoring information security risks within health care. *computers & security* **2013**, *37*, 31–45.
- Yeng, P.K.; Yang, B.; Snekenes, E.A. Framework for healthcare security practice analysis, modeling and incentivization. 2019 IEEE International Conference on Big Data (Big Data). IEEE, 2019, pp. 3242–3251.
- Yeng, P.K.; Yang, B.; Snekenes, E.A. Healthcare Staffs' Information Security Practices Towards Mitigating Data Breaches: A Literature Survey. *pHealth 2019* **2019**, pp. 239–245.
- Furnell, S.; Clarke, N. Power to the people? The evolving recognition of human aspects of security. *computers & security* **2012**, *31*, 983–988.
- Wiley, A.; McCormac, A.; Calic, D. More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security* **2020**, *88*, 101640.
- Parsons, K.; Calic, D.; Pattinson, M.; Butavicius, M.; McCormac, A.; Zwaans, T. The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security* **2017**, *66*, 40–51.
- Van Niekerk, J.; Von Solms, R. Information security culture: A management perspective. *Computers & security* **2010**, *29*, 476–486.

15. Herath, T.; Rao, H.R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems* **2009**, *47*, 154–165.
16. D'Arcy, J.; Lowry, P.B. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal* **2019**, *29*, 43–69.
17. Safa, N.S.; Maple, C.; Watson, T.; Von Solms, R. Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of information security and applications* **2018**, *40*, 247–257.
18. Posey, C.; Roberts, T.L.; Lowry, P.B. The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems* **2015**, *32*, 179–214.
19. Vance, A.; Siponen, M.; Pahnila, S. Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management* **2012**, *49*, 190–198.
20. Grassegger, T.; Nedbal, D. The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. *Procedia Computer Science* **2021**, *181*, 59–66.
21. Yeng, P.K.; Szekeres, A.; Yang, B.; Snekenes, E.A. Mapping the Psycho-social-cultural Aspects of Healthcare Professionals' Information Security Practices: Systematic Mapping Study. *JMIR Human Factors* **2021**, *8*, e17604.
22. Safa, N.S.; Sookhak, M.; Von Solms, R.; Furnell, S.; Ghani, N.A.; Herawan, T. Information security conscious care behaviour formation in organizations. *Computers & Security* **2015**, *53*, 65–78.
23. Lebek, B.; Uffen, J.; Breitner, M.H.; Neumann, M.; Hohler, B. Employees' information security awareness and behavior: A literature review. 2013 46th Hawaii International Conference on System Sciences. IEEE, 2013, pp. 2978–2987.
24. Fernández-Alemán, J.L.; Sánchez-Henarejos, A.; Toval, A.; Sánchez-García, A.B.; Hernández-Hernández, I.; Fernandez-Luque, L. Analysis of health professional security behaviors in a real clinical setting: An empirical study. *International journal of medical informatics* **2015**, *84*, 454–467.
25. Albarrak, A.I. Evaluation of Users Information Security Practices at King Saud University Hospitals. *Global Business & Management Research* **2011**, *3*.
26. Anwar, M.; He, W.; Ash, I.; Yuan, X.; Li, L.; Xu, L. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior* **2017**, *69*, 437–443.
27. Ajzen, I.; Madden, T.J. Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of experimental social psychology* **1986**, *22*, 453–474.
28. Parsons, K.; McCormac, A.; Butavicius, M.; Pattinson, M.; Jerram, C. The development of the human aspects of information security questionnaire (HAIS-Q) **2013**.
29. Abawajy, J. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology* **2014**, *33*, 237–248.
30. Leonard, L.N.; Cronan, T.P.; Kreie, J. What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management* **2004**, *42*, 143–158.
31. Albrechtsen, E. A qualitative study of users' view on information security. *Computers & security* **2007**, *26*, 276–289.
32. Thirumalai, C.; Chandhini, S.A.; Vaishnavi, M. Analysing the concrete compressive strength using Pearson and Spearman. 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA). IEEE, 2017, Vol. 2, pp. 215–218.
33. DeVita, T.; Brett-Major, D.; Katz, R. How are healthcare provider systems preparing for health emergency situations? *World Medical & Health Policy* **2021**.
34. Khalid, M.; Awais, M.; Singh, N.; Khan, S.; Raza, M.; Malik, Q.B.; Imran, M. Autonomous Transportation in Emergency Healthcare Services: Framework, Challenges, and Future Work. *IEEE Internet of Things Magazine* **2021**, *4*, 28–33.
35. Asamani, J.A.; Amertil, N.P.; Chebere, M. The influence of workload levels on performance in a rural hospital. *British Journal of Healthcare Management* **2015**, *21*, 577–586.
36. Nyamtema, A.S. Bridging the gaps in the Health Management Information System in the context of a changing health sector. *BMC medical informatics and decision making* **2010**, *10*, 1–6.
37. Gratian, M.; Bandi, S.; Cukier, M.; Dykstra, J.; Ginther, A. Correlating human traits and cyber security behavior intentions. *computers & security* **2018**, *73*, 345–358.



38. omsorgsdepartementet . How does personality influence your cyber risk?, 2021. <https://www.cybsafe.com/community/blog/how-does-personality-influence-your-cyber-risk/>.
39. McCormac, A.; Zwaans, T.; Parsons, K.; Calic, D.; Butavicius, M.; Pattinson, M. Individual differences and information security awareness. *Computers in Human Behavior* **2017**, *69*, 151–156.
40. Uffen, J.; Guhr, N.; Breitner, M.H. Personality traits and information security management: An empirical study of information security executives **2012**.
41. Shropshire, J.; Warkentin, M.; Sharma, S. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *computers & security* **2015**, *49*, 177–191.
42. Prentice-Dunn, S.; Rogers, R.W. Protection motivation theory and preventive health: Beyond the health belief model. *Health education research* **1986**, *1*, 153–161.
43. Rosenstock, I.M. The health belief model and preventive health behavior. *Health education monographs* **1974**, *2*, 354–386.
44. Cheng, L.; Li, Y.; Li, W.; Holm, E.; Zhai, Q. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security* **2013**, *39*, 447–459.
45. Whatsapp. About WhatsApp. <https://www.whatsapp.com/about>, 2021.
46. Yeng, P.; Yang, B.; Snekenes, E. Observational Measures for Effective Profiling of Healthcare Staffs' Security Practices. 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC). IEEE, 2019, Vol. 2, pp. 397–404.
47. Gosling, S.D.; Rentfrow, P.J.; Swann Jr, W.B. A very brief measure of the Big-Five personality domains. *Journal of Research in personality* **2003**, *37*, 504–528.
48. Drennan, J. Cognitive interviewing: verbal data in the design and pretesting of questionnaires. *Journal of advanced nursing* **2003**, *42*, 57–63.
49. Schechter, S.; Beatty, P.; Block, A. Cognitive issues and methodological implications in the development and testing of a traffic safety questionnaire. Proceedings of the Survey Research Methods Section of the American Statistical Association, 1994, pp. 1215–1219.
50. Martin, E.; Schechter, S.; Tucker, C. Interagency collaboration among the cognitive laboratories: past efforts and future opportunities. Statistical Policy Working Paper 28: 1998 Seminar on Interagency . . . , 1999.
51. Reeve, B.B.; Mâsse, L.C. Item response theory modeling for questionnaire evaluation. *Methods for testing and evaluating survey questionnaires* **2004**, pp. 247–273.
52. Biemer, P. Modeling measurement error to identify flawed questions. *Methods for testing and evaluating survey questionnaires* **2004**, pp. 225–246.
53. Berinsky, A.J.; Margolis, M.F.; Sances, M.W. Separating the shirkers from the workers? Making sure respondents pay attention on self-administered surveys. *American Journal of Political Science* **2014**, *58*, 739–753.
54. Curran, P.; Hauser, D. Understanding responses to check items: A verbal protocol analysis. Philadelphia, PA: Paper presented at the 30th Annual Conference of the Society for Industrial and Organizational Psychology, 2015.
55. Huang, J.L.; Bowling, N.A.; Liu, M.; Li, Y. Detecting insufficient effort responding with an infrequency scale: Evaluating validity and participant reactions. *Journal of Business and Psychology* **2015**, *30*, 299–311.
56. Kung, F.Y.; Kwok, N.; Brown, D.J. Are attention check questions a threat to scale validity? *Applied Psychology* **2018**, *67*, 264–283.
57. Hauke, J.; Kossowski, T. Comparison of values of Pearson's and Spearman's correlation coefficient on the same sets of data **2011**.
58. Arachchilage, N.A.G.; Love, S. A game design framework for avoiding phishing attacks. *Computers in Human Behavior* **2013**, *29*, 706–714.
59. Shah, M. PERCEPTION OF MANAGERS ON THE EFFECTIVENESS OF THE INTERNAL AUDIT FUNCTIONS: A CASE STUDY IN TNB.
60. Hair, J.F.; Page, M.; Brunsveld, N. *Essentials of business research methods*; Routledge, 2019.
61. Pallant, J. SPSS survival manual: a step by step guide to data analysis using SPSS, 2010.
62. Briggs, S.R.; Cheek, J.M. The role of factor analysis in the development and evaluation of personality scales. *Journal of personality* **1986**, *54*, 106–148.
63. Vaske, J.J.; Beaman, J.; Sponarski, C.C. Rethinking internal consistency in Cronbach's alpha. *Leisure Sciences* **2017**, *39*, 163–173.

64. Groeneveld, R.A.; Meeden, G. Measuring skewness and kurtosis. *Journal of the Royal Statistical Society: Series D (The Statistician)* **1984**, *33*, 391–399.
65. Fairburn, N.; Shelton, A.; Ackroyd, F.; Selfe, R. Beyond Murphy's Law: Applying Wider Human Factors Behavioural Science Approaches in Cyber-Security Resilience. *International Conference on Human-Computer Interaction*. Springer, 2021, pp. 123–138.
66. Bowen, B.M.; Devarajan, R.; Stolfo, S. Measuring the human factor of cyber security. 2011 IEEE International Conference on Technologies for Homeland Security (HST). IEEE, 2011, pp. 230–235.
67. Parsons, K.; McCormac, A.; Butavicius, M.; Pattinson, M.; Jerram, C. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security* **2014**, *42*, 165–176.
68. Torres, H.G.; Gupta, S. The misunderstood link: information security training strategy **2018**.
69. Zafar, H. Cybersecurity: Role of behavioral training in healthcare **2016**.
70. Ghazvini, A.; Shukur, Z. Review of information security guidelines for awareness training program in healthcare industry. 2017 6th International Conference on Electrical Engineering and Informatics (ICEEI). IEEE, 2017, pp. 1–6.
71. Alami, H.; Gagnon, M.P.; Ahmed, M.A.A.; Fortin, J.P. Digital health: Cybersecurity is a value creation lever, not only a source of expenditure. *Health Policy and Technology* **2019**, *8*, 319–321.
72. Koppel, R.; Smith, S.; Blythe, J.; Kothari, V. Workarounds to computer access in healthcare organizations: you want my password or a dead patient? In *Driving Quality in Informatics: Fulfilling the Promise*; IOS Press, 2015; pp. 215–220.
73. Stobert, E.; Barrera, D.; Homier, V.; Kollek, D. Understanding cybersecurity practices in emergency departments. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–8.
74. Middaugh, D.J. Cybersecurity Attacks during a Pandemic: It Is Not Just IT's Job! *Medsurg Nursing* **2021**, *30*, 65–66.
75. Shappie, A.T.; Dawson, C.A.; Debb, S.M. Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media* **2020**, *9*, 475.
76. Halevi, T.; Memon, N.; Lewis, J.; Kumaraguru, P.; Arora, S.; Dagar, N.; Aloul, F.; Chen, J. Cultural and psychological factors in cyber-security. *Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services*, 2016, pp. 318–324.
77. Skorek, M.; Song, A.V.; Dunham, Y. Self-esteem as a mediator between personality traits and body esteem: path analyses across gender and race/ethnicity. *PloS one* **2014**, *9*, e112086.
78. Box, D.; Pottas, D. Improving information security behaviour in the healthcare context. *Procedia Technology* **2013**, *9*, 1093–1103.
79. Gurusamy, K.; Aggarwal, R.; Palanivelu, L.; Davidson, B. Systematic review of randomized controlled trials on the effectiveness of virtual reality training for laparoscopic surgery. *Journal of British Surgery* **2008**, *95*, 1088–1097.
80. Larsen, C.R.; Oestergaard, J.; Ottesen, B.S.; Soerensen, J.L. The efficacy of virtual reality simulation training in laparoscopy: a systematic review of randomized trials. *Acta obstetricia et gynecologica Scandinavica* **2012**, *91*, 1015–1028.