How do the protection motivation theory and the self-determination theory influence healthcare employees' intention to perform safe cyber behaviour?

Koen Jannink

University of Twente

Faculty of Behavioural Management and Social Sciences (BMS)

Psychology - Conflict, Risk and Safety

Master's thesis

First supervisor: Dr. I. Van Sintemaartensdijk

Second supervisor: Dr. S.J. Watson

Supervisor Acute Zorg Euregio: R. Schär

February 13, 2025

Abstract

With the increasing threat of cyberattacks in healthcare, preventive measures should focus more on the behaviour of healthcare employees, as they are the weakest link contributing to security breaches. This study uses the protection motivation theory (PMT), the self-determination theory (SDT) and response performance motivation to explain the motivational drivers of healthcare employees' security behaviour. Using an online questionnaire, 231 healthcare employees from organisations associated with the Regional Acute Care Consultation (ROAZ) shared their views on cyber motivational factors. In comparison to PMT variables as a whole, the results suggest that SDT as a whole is a stronger predictor of the behavioural intention to engage in safe cyber behaviour. This means that fear-driven factors are a weaker predictor of behavioural intention than factors that align more closely with healthcare employees' self-concept and internal values. Adding response performance motivation to both theories decreased the strength of the prediction and influenced the significance negatively. Despite that, response performance motivation had a remarkable effect and is regarded as the most effective variable for behavioural intention compared to PMT and SDT variables. Perceived competence and response efficacy were also perceived as impactful variables. Regarding the impact of the SDT variables on the PMT variables, perceived competence had the strongest effect on self-efficacy.

Introduction

Healthcare organisations have been digitising their operations for a long time, thereby making the transition from analogue data (paper-based patient records) to digital data (digital form of patient records) through the use of technology (Tilson et al., 2010; Mihailescu & Mihailescu, 2018). Digitisation has improved the quality and efficiency of healthcare and made it more accessible to a larger number of people (Boer, 2019). Most of the work of healthcare employees today consists of storing information, processing, transferring, and analysing data (Gupta et al., 2015). As a consequence of this digitisation, healthcare organisations have been acknowledged as information-based industries (Martínez-Caro et al., 2018). Consider retrieving and sending patient information to their online dossiers, ordering medicine prescriptions, and using electronic devices that provide data used by employees. In 2020, the healthcare sector accounted for 30% of all data worldwide. The increase in healthcare data is accompanied by more cyber security threats (Hoffman, 2020), resulting in healthcare organisations being the most targeted sectors by cyber criminals (Argaw et al., 2020). Organisations' systems may contain vulnerabilities that can be exploited, damaging functions such as hardware, software, networks, operating systems, and medical devices (Aljuraid & Justinia, 2022). This data is significantly more valuable for cybercriminals to sell on the black market than in other sectors (Luna et al., 2016). This is due to sensitive data such as names, citizen service numbers, dates of birth, addresses, and credit card details (Bhuyan et al., 2020). These attacks harm the privacy of all persons connected to healthcare, from health workers providing care to the security of the organisations, their finances, and their reputation (Kamerer & McDermott, 2020; Le Bris & Al Asri, 2016).

With the threat of cyber attackers, healthcare organisations constantly try to develop and improve themselves by taking preventive measures to avoid becoming victims. They use advanced technology such as authorisation, authentication, and privacy measures such as encryption and much more (McDermott et al., 2019). Despite those advanced measures, the human mistakes made by employees can cause security breaches (Kahanda et al., 2023). Those mistakes are primarily the result of insufficient knowledge and education on how to deal with cybersecurity (Wanyonyi et al., 2017). Cyber attackers are aware that the weakest links are mainly the employees of an organisation (Heartfield & Loukas, 2018).

Social engineering is a psychological manipulation technique that lures individuals to perform malicious actions to retrieve data by misusing their inattention or trust (Thornburgh, 2004). Cyberhackers use these techniques to gain confidential and sensitive information about healthcare organisations (Schaab et al., 2017). According to Z-CERT (2023), phishing, a tactic

in which hackers impersonate real persons to try to collect sensitive data via email, is the most common attack within healthcare organisations. Cialdini (2007), Gragg (2003), and Stajano and Wilson (2011) established principles that influence individuals to perform malicious actions. These principles are based on liking, 'similarity & deception', 'commitment, reciprocation & consistency', and distraction (Ferreira et al., 2015).

To prevent cyber-attacks, healthcare institutions should offer training to prepare their employees (Argaw et al., 2020). These trainings should focus on improving employees' understanding and enhancing their efficacy to prevent themselves from cyber-attacks (Bhuyan et al., 2020). Effective communication of policy/training to all relevant employees is essential for creating a productive learning environment and promoting a secure organisational culture (Siponen, 2000). These policies or training can quickly be seen as an obstacle which keeps people away from their work. This can make people less engaged in learning about and adhering to best practices in security procedures and processes (Bada et al., 2019). This phenomenon is also described as 'security fatigue' (Nobles, 2022). Hogan (2005) indicates that the main drivers of a person's behaviour are recognised as understanding, skills, and knowledge of cyber security as well as one's perception, attitude, and beliefs. Motivation and personal ability are the two most influential ones (Bada et al., 2019). Furthermore, discovering the discrepancy between what people say and what they do is an important factor. To establish new habits, individuals must renew their existing thought patterns.

Many studies have examined the PMT and SDT independently, both within and beyond the healthcare sector, to identify the motivational drivers of cybersecurity (Raj Sreenath et al., 2014; Osawaru, 2024; Feraru & Bacali, 2024). Menard et al. (2017) were the first to combine the protection motivation theory (PMT) and the self-determination theory (SDT) into one integrated model in the field of cybersecurity. The PMT is used to assess their perceptions of threats and their belief in their ability to deal with those threats, which gives insight into their motivation to protect themselves. The SDT gives insight into motivational factors, explaining why people are more likely to engage and sustain protective behaviours when this aligns with their values. The second one who did research on this topic was Yang et al. (2020), with a replication study. The studies' main focus was to gain an understanding of how to most effectively motivate users into performing secure behaviour, which gave them insight into effectively implementing secure countermeasures that contribute to an overall safer computing environment.

This study aims to expand this approach into a different scope by translating the theories into the healthcare sector and targeting healthcare employees. To the best of this researcher's

knowledge, the combination of healthcare focusing on safe cyber behaviour and the two combined theories has never been studied. Healthcare is an interesting sector to focus on because its professional code consists of core values and professional obligations of protecting and ensuring the quality and safety of healthcare (Verpleegkundige & Verzorgende Nederland, n.d.). The combination of these ethical and professional standards is distinct from those in other sectors, which adds to its uniqueness. Each sector has its own interests, which also shape its motivational factors. Alshmemri et al. (2017) and Healy (2016) state that the highest intrinsic motivation of healthcare employees is to care for patients. This, for example, differs from those in the construction industry, where the intrinsic motivation may lie in creating structures. The text below explains both theories independently, addresses their differences, details the variable response performance motivation, and relates their relevance to the healthcare sector.

Protection motivation theory (PMT)

Rogers was the first person to develop the PMT (Prentice-Dunn & Rogers, 1997). The theory was originally designed to give insights into how people react to communications about health threats that evoke fear (Sutton, 2001). Rogers (1975) stated that when a threatening situation occurs, threat and coping lead to protective motivation, which involves adopting behaviours that prevent individuals from harm. The theory examines five elements: threat severity and vulnerability under the threat appraisal, self-efficacy, response efficacy, and response cost under the coping appraisal. This cognitive process influences how individuals respond to the perceived threat (Boss et al., 2015).

In assessing threats, threat severity is seen as the seriousness of the consequences of a threat. Threat vulnerability can be defined as a person's sensitivity to a threat (McLeod et al., 2015). A person assesses whether the threat is sufficiently harmful, likely, and worth taking protective measures against (Norman et al., 2015; Li et al., 2022). If the threat rating is higher than the benefit of ignoring the threat, the person is more likely to choose to adopt protective behaviour (Howell, 2021).

The coping appraisal consists of three factors. Firstly, self-efficacy is the belief that the recommended action can successfully be performed (Mou et al., 2017). Second, response efficacy is the belief that the recommended actions can effectively reduce the threat (Sutton, 2001). Lastly, response cost is the expenses associated with the recommended behaviour (Prentice-Dunn et al., 2009). Adaptive actions will be taken when people perceive that the actions can be performed, effectively reducing the threat and the costs are low (Norman et al., 2015).

Numerous studies have linked the theory to information security awareness (Menard et al., 2017; Mehraj et al., 2021; Mou et al., 2022). They confirm that information security behaviour is explained by the PMT. Furthermore, they provide valuable insights into the intention of why employees are more likely to engage in safe cyber behaviour, emphasising extrinsic motivation. This information gives healthcare organisations a greater understanding of where to concentrate efforts on developing suitable new cybersecurity tools and motivating employees to behave in a safe cyber way (Towbin, 2019). The text below establishes the connection between PMT variables and the healthcare sector.

The perceived severity of cyber-attacks could cause healthcare employees to fear that their personal or client information has been exposed and that hackers are going to use it for the wrong purposes. Or that their work device on work is hacked and that they could lose their job for letting this hack happen (Li et al., 2022; Ophoff & Lakay, 2019). According to Hughes (2016), when healthcare employees have a better understanding of these consequences, it can help to improve organisational security behaviour. This effect is confirmed by a study by Martens et al. (2019). Proactive and cautious behaviour can also occur when there is an increased perception of disease severity (Moyo et al., 2022). It is thus suggested that perception of severity positively affects the healthcare employees' behavioural intention to perform safe cyber behaviour.

Both Giwah et al. (2019) and Holmes and Ophoff (2019) showed that perceived vulnerability significantly affected protective motivation towards information security behaviour. In healthcare settings, it can be explained as an employee's feeling that their work device on work is very likely to be hacked. The feeling that hackers want sensitive information what is on their work devices increases protective motivation (Osawaru, 2024). Highly vulnerable information healthcare employees perceive about themselves makes them even more aware of their workplace safety compared to people who do not have it (Shi et al., 2025). During the COVID-19 pandemic, this perceived vulnerability prompted healthcare employees to take protective actions (Makhanova & Shepherd, 2020). Therefore, it is expected that when healthcare employees perceive a high level of vulnerability, it positively affects behavioural intention to perform safe cyber behaviour.

Self-efficacy in a healthcare setting refers to healthcare employees' belief that they can protect their work devices on work against hackers. An increase in this belief is accompanied by trust and confidence to perform that behaviour. Earlier studies indicate that the belief in capability positively affects taking protective actions in cyber security (Crossler & Bélanger, 2014; Hooper & Blunt, 2020). This is in line with the findings of Shorey and Lopez (2021),

where the self-efficacy of healthcare employees had a significant effect on behaviour. Thus, based on this, self-efficacy likely positively affects behavioural intention to perform safe cyber behaviour.

Response efficacy in the healthcare setting is the employees' subjective point of view on the extent to which safe security behaviours will reduce security threats on their devices in their organisation (Raj Sreenath et al., 2024). Both Tsai et al. (2016) and Giwah et al. (2019) established a relationship between response efficacy and the user's protective motivation for information security behaviour. Healthcare employees utilise evidence-based methods as they demonstrate the most beneficial outcomes for patients (Connor et al., 2023). This underscores the importance of effectiveness when something proves successful. The expectation is that response efficacy positively affects the behavioural intention to perform safe cyber behaviour.

The response cost is the disadvantage that healthcare employees perceive associated with performing safe cybersecurity behaviour on their devices in their organisation (Haag et al., 2021). A lack of time or effort may be a disadvantage they experience (Ophoff & Lakay, 2019). Individuals make a considered decision not to adopt cyber security measures if the cost exceeds the benefit (Crossler & Bélanger, 2014). The study of Shahbaznezhad et al. (2021) confirms this negative relation. According to the Centraal Bureau voor de Statestiek (2022), more than 50% of Dutch healthcare workers perceive the workload to be high. Every extra bit of work can be seen as a burden, including cybersecurity measures. Based on this literature, it is assumed that perceived cost has a negative effect on behavioural intention to perform safe cyber behaviour.

Self-determination theory (SDT)

As illustrated in the PMT, the measured variables provide extrinsic motivation, as external drivers provoke them. The SDT covers intrinsic and extrinsic motivation (Legault, 2020; Patel & Alismail, 2024). According to Deci (2017), intrinsic motivation is an autonomous form of motivation. It arises from interests and goals that internally drive individuals, which aligns with their self-concept (Bandhu et al., 2024). It thus points to activities for which the motivation is rooted in the behaviour itself (Deci, 2017). The SDT insinuates that there are three basic psychological needs that people should have to experience continuous growth, integrity, and well-being (Ryan & Deci, 2024). The basic needs are autonomy, relatedness and competence (Romero-Masters, 2023; Ryan, 2017). Autonomy can be explained by the ownership of one's actions (Ryan & Deci, 2020). Relatedness explains the urge of a person's feelings and support of connection with others, things, or tasks (Alahmari, 2021). For competence, a person should have the feeling of ability and effectiveness in performing a task

(Alahmari, 2021). The SDT also consist of extrinsic motivation, which stems from external factors (Bandhu et al., 2024). It suggests that many behaviours initially stem from extrinsic motivation. This motivation may develop over time into intrinsic motivation as individuals internalise it and align it more closely with their self-concept (Deci et al., 2017; Ryan & Deci, 2020). The text below establishes the connection between SDT variables and the healthcare sector.

The studies by Kam et al. (2020) and Francis et al. (2024) utilise the SDT alongside cybersecurity practices to explain the motivational factors driving cybersecurity learning. They demonstrated that intrinsic motivation increases among individuals and that targeted interventions enhance engagement and retention in cybersecurity education. Additionally, numerous studies utilising the SDT emphasise the importance of internal factors in education (Alonso et al., 2023; Diwakar et al., 2023).

Perceived autonomy in the setting of cybersecurity can be seen as a healthcare employee's perception of a sense of control over their own actions to perform safe cyber behaviour on their work device in their organisation. Several studies found that when employees were in the lead to choose their training program, motivation was increased (Kam et al., 2022; Baldwin et al., 1991). Abraham and Chengalur-Smith (2019) indicated in their study that information security training had positively been influenced by perceived learning autonomy. For healthcare workers, the autonomy to make choices enhances employee well-being and boosts job satisfaction (Cicolini et al., 2014). Therefore, the assumption is that perceived autonomy has a positive effect on behavioural intention to perform safe cyber behaviour.

Relatedness is seen as a healthcare employee's sense of connection and collaboration regarding their actions to perform safe cyber behaviour on their work device within their organisation. According to Kam et al. (2022), when employees have a sense of connection and collaboration during training, it will enhance their motivation. In Babenko's (2018) study on healthcare employees' well-being, perceived relatedness was found to score the highest. It is expected that the relatedness of healthcare employees positively affects the intention to perform safe cyber behaviour.

The last one, competence, is described as the healthcare employee's perception of their ability and effectiveness in performing safe cyber behaviour on their work device in their organisation. Employees should have the sense that they can grow and succeed and perceive the ability to gain cybersecurity knowledge (Ryan & Deci, 2020; Kam et al., 2022). Roca and Gagné (2008) confirm this in their study by demonstrating that perceived competence is an

intrinsic motivator. For healthcare employees, this also increases motivation and enhances the quality of daily work (Ortega-Lapiedra et al., 2023). Based on those studies, a prediction is made that healthcare employees' perception of their ability and effectiveness positively affects behavioural intention to perform safe cyber behaviour.

Response performance motivation

The PMT and the SDT both concentrate on variables that enhance motivation; however, they do not directly measure it. Menard et al. (2017) included the variable "response performance motivation" in the Integrated Model. They positioned it as a variable for comparison to determine whether the addition to the theories has an effect. This variable distinguishes itself from the other variables in the PMT and the SDT because it measures motivation as a variable rather than as a component that provides motivation. It encompasses intrinsic motivation within the model, as it directly measures the inner drive that activates healthcare workers to engage in safe cyber behaviour without any necessary influencing factors. Cybersecurity is not a profession that most healthcare employees have graduated from, nor is it one that they hold dear. Perspectives on this matter will differ among employees. According to social psychology, when cybersecurity behaviour is integrated into the self-concept of a healthcare employee, intrinsic motivation fosters the performance of that behaviour (Forsyth, 2019). This occurs even in the absence of any external variable that enhances motivation. Therefore, it is assumed that healthcare employees' perceived response performance motivation positively influences their behavioural intention to engage in safe cyber behaviour.

Protection motivation theory, in combination with the self-determination theory

Integrating the PMT and the SDT into one model has a benefit. The PMT influences the intention to perform safe cyber behaviour based on the threat appraisal (the perceived severity and vulnerability) and the coping appraisal (the perceived self-efficacy, response efficacy, and response cost). These appraisals directly trigger a person's behavioural intention, leading to motivation (Norman et al., 2015). The SDT is a good addition to get a more complete picture of the motivational drivers. Internalised motivation guides people's behaviour and helps them understand why they maintain it. Their behaviour is in line with their own values and beliefs (self-concept of a person) (Deci et al., 2017). So, getting insight into the effect of the SDT on the PMT provides a comprehensive understanding of how internal motivation, effective for the long term, shapes external motivation, which increases immediate actions.

The combination of the two theories will give insight into five different ways that impact employee motivation: perceived relatedness and each individual threat appraisal (threat severity

and threat susceptibility), perceived competence and self-efficacy, perceived autonomy and response efficacy, and perceived autonomy and response cost.

First is perceived relatedness and each individual threat appraisal (threat severity and susceptibility). Perceived relatedness is the emotional connection between healthcare employees and the behaviour of performing safe cyber behaviour on their work devices in their organisation. The emotional bond with that behaviour increases if it is similar to a person's self-concept. The more attached people are to that behaviour, the more they will care about it and are likely to protect it (Nisbet & Zelenski, 2024). When the employees perceive the threat as very serious, acknowledge the consequences and perceive their selves as likely targets, their self-concept is in danger (Dulaney, 2021). Therefore, the assumption is that when healthcare employees have an increased relatedness with the behaviour of performing safe cyber behaviour, this will have a positive effect on threat severity and threat susceptibility.

Perceived competence and self-efficacy are closely aligned. Perceived competence focuses on whether the self-concept is in line with the belief healthcare employees have in their ability to perform safe cyber behaviour on their work devices in their organisation. With self-efficacy, the emphasis is on individuals' ability to successfully adopt safe cyber behaviours on their work devices within their organisation (Rodgers et al., 2014). When the behaviour to perform safe cyber behaviour is in line with a healthcare employee's values, they will rely on and will be more supportive towards that behaviour. This supportive attitude will increase the ability to perform safe cyber behaviour successfully. So, the expectation is that an increased perceived level of competence of healthcare employees has a positive effect on their self-efficacy.

Previous research by Wall et al. (2013) about security behaviour indicates that autonomy has a positive influence on the perception of response efficacy and that psychological reactance has a negative effect. According to the psychological reactance theory of Brehm (1966), when the freedom of people is threatened or taken away, people want to restore their freedom because they experience psychological reactance. A choice is based on someone's perception that it fits them the best and what they are most confident about (Tiemeijer, 2010). Therefore, when healthcare employees do not have the feeling that they have the freedom to choose what kind of safe cyber behaviour they can perform, they will be reluctant and choose for themselves what is the most effective option. The expectation is that when employees experience more freedom to choose, the belief in the effectiveness of performing cyber-safe behaviour also increases. The relationship between perceived autonomy and response cost is also affected by the level of freedom employees are given to choose how to perform safe cyber behaviour. If they choose to

perform in a way that is more in line with their self-concept, they choose an option that is most beneficial to them and requires less effort to perform. Therefore, when healthcare employees experience more autonomy in their choices to perform safe cyber behaviour, the experienced cost will decrease.

The present study

This current research focuses on the integrated model of SDT and PMT for security appeal perception to investigate how these theories influence healthcare employees' intention to perform safe cyber behaviour. By emphasising the ongoing impact of cyberattacks within healthcare organisations, gaining insights into the psychological motivators behind the intention to engage in safe behaviour is crucial to prevent these organisations from becoming victims. The study targets healthcare employees connected to the Regional Acute Care Consultation (ROAZ). This Dutch platform connects healthcare organisations within the borders of Euregio and aims to collaborate to optimise acute care, particularly during long-term crises. The research question of this study is: How do the protection motivation theory and the self-determination theory influence healthcare employees' intention to perform safe cyber behaviour? This is examined using the hypotheses in Table 1. The integrated model of PMT and SDT for security appeal perception provides an overview of how the variables of PMT, SDT, and the variable response performance motivation are interconnected and influence behavioural intention, as illustrated in Figure 1.

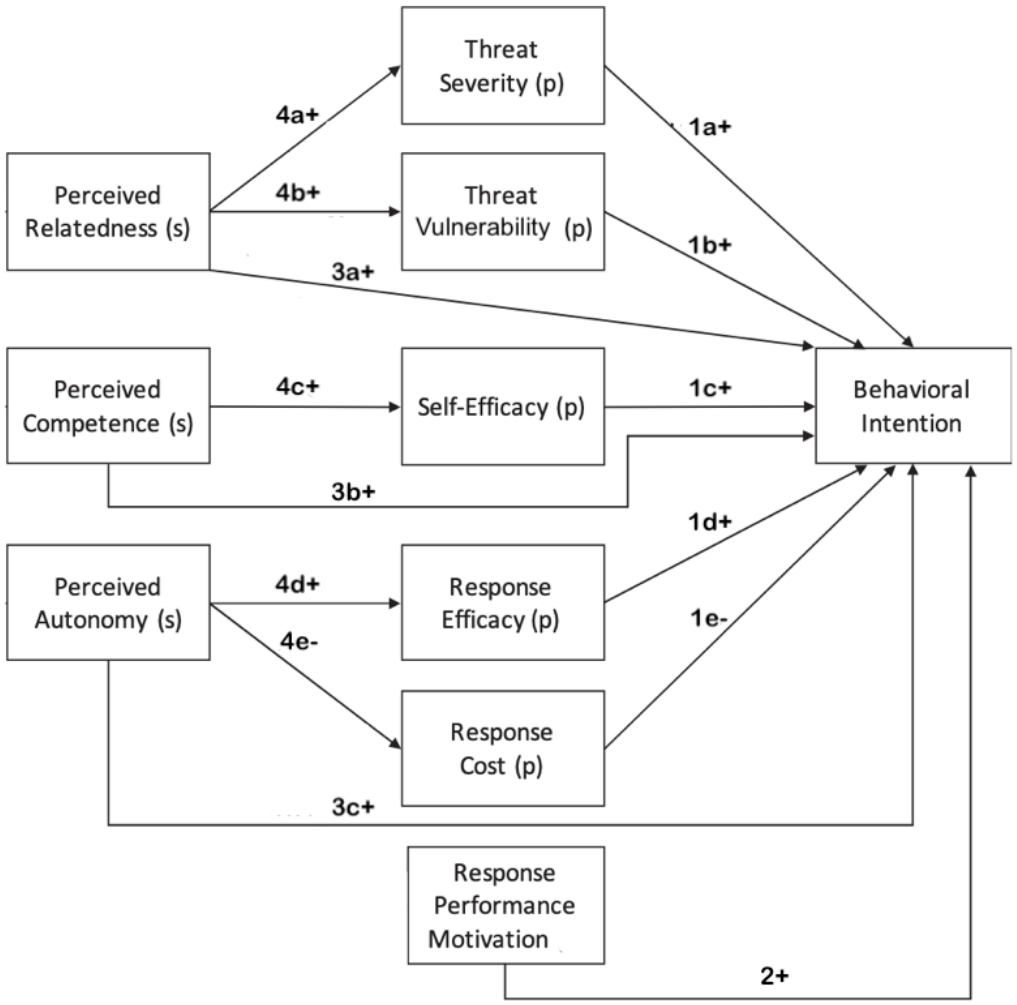
Table 1

Hypotheses present study

Hypothesis	Description
Hypothesis 1a	An increase in the perceived severity of cyber-attacks for employees in the healthcare sector has a positive effect on behavioural intention to perform safe cyber behaviour.
Hypothesis 1b	An increase in perceived vulnerability of cyber-attacks for employees in the healthcare sector has a positive effect on behavioural intention to perform safe cyber behaviour.
Hypothesis 1c	An increase in self-efficacy for employees in the healthcare sector has a positive effect on behavioural intention to perform safe cyber behaviour.
Hypothesis 1d	An increase in response efficacy for employees in the healthcare sector has a positive effect on behavioural intention to perform safe cyber behaviour.
Hypothesis 1e	An increase in response cost for employees in the healthcare sector has a negative effect on behavioural intention to perform safe cyber behaviour.
Hypothesis 2	An increase in response performance motivation for employees in the healthcare sector has a positive effect on performing safe cyber behaviour.
Hypothesis 3a	An increase in relatedness for employees in the healthcare sector has a positive effect on behavioural intention to perform safe cyber behaviour.
Hypothesis 3b	An increase in competence for employees in the healthcare sector has a positive effect on behavioural intention to perform safe cyber behaviour.
Hypothesis 3c	An increase in autonomy for employees in the healthcare sector has a positive effect on behavioural intention to perform safe cyber behaviour.
Hypothesis 4a	An increase in the relatedness of employees in the healthcare sector has a positive effect on threat severity perceptions.
Hypothesis 4b	An increase in the relatedness of employees in the healthcare sector has a positive effect on threat vulnerability perceptions.
Hypothesis 4c	An increase in the perceived competence of employees in the healthcare sector has a positive effect on self-efficacy.
Hypothesis 4d	An increase in the perceived autonomy of employees in the healthcare sector has a positive effect on response efficacy.
Hypothesis 4e	An increase in the perceived autonomy of employees in the healthcare sector has a negative effect on response costs.

Figure 1

The integrated model of SDT and PMT for cybersecurity appeal perception.



(p) is native to the PMT, (s) is native to the SDT, + is referring to a positive relation, – is referring to a negative relation

Methods

Participants and design

Participants who filled in the questionnaire were employees working for healthcare organisations connected to the Regional Acute Care Consultation (ROAZ). Two hundred sixty-one employees started the questionnaire, and 30 of them were directly excluded due to no responses to the general questions and items to measure the first variables of interest (threat severity). To be included in the analysis, an employee had to complete every item that measures a variable. If not, the employee was excluded from that variable, resulting in varying sample sizes across variables. In total, 231 employees completed all items of the first variable (threat severity). The sample includes 74 men, 156 women and one person who did not want to say it, with an overall average age of 50 years (*SD*= 12). Hospital employees constituted 53.9% of the sample, 12.3% were employees from VVT institutions, Medical Specialist Care and Mental Healthcare (GGZ) both scored 9%, and the remaining 15.8% came from different healthcare organisations connected to the ROAZ. Employees who completed all items of all variables totalled 189. Participant collection was through a direct approach to ROAZ member organisations, using convenience sampling to collect a large enough sample (Nikolopoulou, 2022).

The material used to collect data was by means of a cross-sectional design (Connelly, 2016). The questionnaire was divided into three parts: informed consent, general demographic questions and specific items to measure the variables of interest (see Appendix A).

Materials

The questionnaire consisted of 46 items, including 27 items based on the PMT, nine for response performance motivation, one for behavioural intention, and nine for the SDT. The PMT focused on the following variables: threat severity, threat susceptibility, self-efficacy, response efficacy, and response cost. The SDT focused on the variable's perceived relatedness, perceived competence, and perceived autonomy. All items were derived from validated behavioural security studies to guarantee the validity and reliability of the items used to measure the variables. These have been translated into Dutch at the B1 level, meaning the language is accessible to all healthcare employees due to its simplicity and clarity, regardless of their education or language proficiency level. Table 2 gives an overview of the variables, including the mean, standard deviation, Cronbach alpha and the N-valid responses.

Protection motivation theory variables

The variables, threat severity, threat susceptibility, self-efficacy, response efficacy, and response cost, were derived from a study by Thompson et al. (2017). To make the questions

more consistent with this current study, the items were renamed from home computers and mobile devices to work devices within the healthcare organisation. For example, one item of threat severity stated: A hack on my work devices within my organisation would be a big problem for me. The items to measure the variables consisted of statements that participants rate using a five-point Likert scale, ranked from 1 (*totally disagree*) to 5 (*totally agree*) (Nemoto & Beglar, 2014). George and Mallery (2019) and Tananuvat et al. (2022) state that the internal reliability of a Cronbach's alpha greater than 0.7 is acceptable. Threat severity, self-efficacy, response efficacy, and response cost met this standard (see Table 2). Conversely, threat vulnerability was lacking; however, with a Cronbach alpha of 0.69, it is still considered acceptable (George & Mallery, 2019).

Response performance motivation variable

The items used to measure the variable response performance motivation were derived from the study of Menard et al. (2017). They used 16 items to measure response performance motivation to install password manager software. To make the questions consistent with this current questionnaire, 'use of install password manager software' was changed to 'use of security measures on my work devices within my organisation'. Example item that was used: I choose to use security measures on my work devices within my organisation because… I think that this activity is interesting. Because of the high workload and limited time for healthcare employees, this research removed seven items to make it shorter. Therefore, the last four forward-score items and the last three reversed-scored items were removed. The remaining nine items were measured using a slider scale ranging from 1 (*extremely unlikely*) to 5 (*extremely likely*) (Betella & Verschure, 2016). Despite the seven removed items, the variable still had a Cronbach's alpha of 0.64.

Behavioural intention variable

The item used to measure behavioural intention was derived from the study of Menard et al. (2017). The meaning of behavioural intention was similar to that of this research, making it convenient for this study to use this item. One of the 16 items was used to measure the behavioural intention of the healthcare employees. The same adjustment was made, and the same measure scale was used as in the variable response performance motivation. The selected item that was used: I think this activity is good for me.

Self-determination theory variables

The items of SDT variables were derived from the studies conducted by Kam et al. (2022) and Kam (2020). For perceived relatedness, the questions were adjusted for greater consistency with this study, replacing 'training programme' with 'security measures on my

work devices within my organisation that protect them from cybercrime. An example item stated: I feel emotionally committed to preventing cybercrime by taking security measures on my work devices within my organisation. For perceived competence and perceived autonomy, the questionnaire items were adapted to shift the focus to security measures on my work devices within my organisation that protect them from cybercrime. An example item of perceived competence stated: I feel I am getting better at protecting work devices within my organisation from cybercrime through security measures. All items were assessed using statements that participants rate on a five-point Likert scale, from 1 (totally disagree) to 5 (totally agree) (Nemoto & Beglar, 2014). All three Cronbach's alpha values were considered acceptable, with perceived relatedness receiving the highest score (George & Mallery, 2019).

Table 2

Descriptive Statistics of Scales

	M	***SD***	**α**	**N-valid responses**
Behavioural intention	3.50	1.30		194
Threat severity	4.35	0.70	0.89	231
Threat vulnerability	3.40	0.61	0.69	220
Self-efficacy	3.39	0.74	0.87	213
Response efficacy	3.92	0.54	0.75	206
Response cost	2.32	0.75	0.88	201
Response performance motivation	3.01	0.65	0.64	194
Perceived relatedness	3.07	1.04	0.87	192
Perceived competence	3.59	0.67	0.76	189
Perceived autonomy	3.40	0.68	0.72	189

Procedure

The link to the online questionnaire was sent to all the cyber and communication managers of the organisation connected to the ROAZ. These managers then distributed the questionnaire directly or through a newsletter to the healthcare employees. The questionnaire was anonymously processed, so the researcher could not identify personal information.

When participants opened the link, a short introduction was presented with the study's purpose and focus, after which they could consent to participate. Then, the participants encountered some demographic questions, including gender, age, working location, whether they had ever been a victim of cybercrime, and whether the organisation provided enough cyber

prevention tools. The next part covered the 46 items to measure the variables of the PMT, response performance motivation, behavioural intention and the variables of the SDT. Lastly, the participants were thanked for their participation, and the option for debriefing information was provided. The estimated duration to complete the questionnaire was 12 minutes.

Analyse

The analyses were conducted using the statistical software R version 4.4.2. A power analysis was used to determine the minimal sample size needed to detect an effect (Erdfelder et al., 1996). According to the power analysis, the minimal sample size is 97 participants for a study with 10 variables. This research had a minimum of 189 participants for each variable, which gives a reliable indication that the sample size can detect an effect. The level of power was 0.97 for a medium effect size ($f^2 = 0.15$) with an alpha level of 0.05 and 10 predictors.

Bivariate correlations between all variables with Pearson correlations were examined (see Table 3). This presents the strength and direction of a linear relationship (Lee Rodgers & Nicewander, 1988). Afterwards, multiple linear regressions were performed. First, the variables of the PMT (threat severity, threat vulnerability, self-efficacy and response cost), response performance motivation and the variables of the SDT (perceived relatedness, competence and autonomy) are tested against the behavioural intention to perform safe cyber behaviour (H1a-f, H2 and H3a-c). Secondly, PMT variables were tested against SDT variables (H4a-e). Next to that, linear regression with all PMT variables and all SDT variables was tested as a whole towards behavioural intention. Another linear regression, incorporating response performance motivation, was conducted to assess this effect.

Results

Analyses of protection motivation theory and self-determination theory

Table 3 explains the Pearson correlation between the variables, the threat and coping appraisals of the PMT, response performance motivation and the perceived relatedness, perceived competence and perceived autonomy of the SDT. The variable response cost negatively correlates to all the other variables. All remaining variables show positive correlations with each other. The variables of the SDT have, on average, higher correlations with each other than the variables of the PMT. The correlation varies between 0.45 and 0.59, which was considered moderate, according to Dancey (2007).

Table 3

Pearson Correlation Between Variables

	BI	**TS** (p)	**TV** (p)	**SE** (p)	**RE** (p)	**RC** (p)	**RPM**	**PR** (s)	**PC** (s)
TS (p)	.16*								
TV (p)	.16*	.24***							
SE (p)	.18*	.28***	.04						
RE (p)	.25***	.21**	.09	.39***					
RC (p)	-.24***	-.20**	-.12	-.31***	-.22**				
RPM	.53***	.28***	.31***	.25***	.24***	-.44***			
PR (s)	.22**	.20**	.20**	.16*	.13	-.24***	.49***		
PC (s)	.40***	.25***	.19**	.34***	.31***	-.14	.49***	.55***	
PA (s)	.30***	.16*	-.02	.46***	.32***	-.21**	.37***	.45***	.59***

**p <0.05, **p <0.01, ***p <0.001*

BI= Behavioural Intention, TS= Threat Severity, TV= Threat Vulnerability, SE= Self-efficacy, RE= Response Efficacy, RC= Response Cost, RPM= Response Performance Motivation, PR= Perceived Relatedness, PC= Perceived Competence, PA= Perceived Autonomy, *(p) = native to the PMT, (s) = native to the SDT*

Regression model

The linear, multiple regressions between the variables examined in this study are shown in Table 4. The variables of the PMT (threat severity (H1a), threat vulnerability (H1b), self-efficacy (H1c), response efficacy (H1d), response cost (H1e)), response performance motivation (H2) and the SDT (perceived relatedness (H3a), perceived competence (H3b), perceived autonomy (H3c)) had significant outcomes to behavioural intention. All variables had positive relationships except for the response cost, which was negatively related to

behavioural intention. The strongest relationship was among the variable response performance motivation, followed by perceived competence and response efficacy. The weakest relation was found by perceived relatedness, and the rest had in-between scores.

All outcomes were also significant for the SDT to the PMT variables in H4 (a - e). One negative relation was found between perceived autonomy and response cost, and the rest of the relations between the variables were positive. With perceived competence and self-efficacy, the strongest link is found, the weakest being between perceived relatedness and threat vulnerability. The rest scored in between.

Table 4

Linear, Multiple Regressions for PMT and SDT variables.

H	From	To	β	*SE*	*t*	ηp²
1a	Threat severity	Behavioural intention	.31*	.14	2.21	.02
1b	Threat vulnerability	Behavioural intention	.37*	.16	2.31	.03
1c	Self-efficacy	Behavioural intention	.32*	.13	2.53	.03
1d	Response efficacy	Behavioural intention	.61***	.17	3.60	.06
1e	Response cost	Behavioural intention	-.42***	.12	-3.45	.06
2	Response performance motivation	Behavioural intention	.89***	.12	8.70	.29
3a	Perceived relatedness	Behavioural intention	.27**	.09	3.12	.05
3b	Perceived competence	Behavioural intention	.78***	.13	6.04	.16
3c	Perceived autonomy	Behavioural intention	.56***	.13	4.29	.14
4a	Perceived relatedness	Threat severity	.12**	.04	2.89	.04
4b	Perceived relatedness	Threat vulnerability	.11**	.04	2.76	.04
4c	Perceived competence	Self-efficacy	.37***	.74	4.95	.12
4d	Perceived autonomy	Response efficacy	.25***	.05	4.64	.10
4e	Perceived autonomy	Response cost	-.23**	.08	-3.00	.05

**p <0.05, **p <0.01, ***p <0.001*

Using a linear regression model, the differences between the two theories towards behavioural intention, with and without response performance motivation, are established. The SDT, including the variables perceived relatedness, competence, and autonomy (β = .63, *SE* = .14, *t* = 4.47, *p* = .14e-04), was significant and had a stronger impact on behavioural intention to perform safe cyber behaviour compared to the PMT which was established as not significant,

including the variables threat severity, threat vulnerability, self-efficacy, response efficacy, and response cost (β = .46, *SE* = .47, *t* = 1.49, *p* = .14). Including the variable response performance motivation had an effect on the theories. The SDT (β = .14, *SE* = .15, *t* = .96, *p* = .34) and the PMT (β = .34, *SE* = .29, *t* = 1.20, *p* = .23) both had a decreased effect and were established as not significant.

Discussion

The increasing digitalisation of healthcare organisations is accompanied by new threats that they must protect against (Boer, 2019; Hoffman, 2020). A lack of skills and human error make healthcare employees the weakest link for cyber attackers to retrieve sensitive information (Kahanda et al., 2023; Wanyonyi et al., 2017). The focus should be on understanding employee behaviour and what encourages them to counter these attacks.

This study examines information on the motivational factors of healthcare employees by integrating two motivational theories and the variable response performance motivation into one model. The model consists of the PMT variables, including threat severity, threat vulnerability, self-efficacy, response efficacy, and response cost; the variable response performance motivation; and the SDT variables, including perceived relatedness, perceived competence, and perceived autonomy, all leading to the intention for behavioural change among healthcare employees within the borders of Euregio. All variables in the integrated model are significant, suggesting that it is unlikely that the results occurred by chance. Response performance motivation had the strongest effect on behavioural intention, followed by perceived competence. The weakest outcome is attributed to perceived relatedness. In general, the SDT had more effect on behavioural intention than the PMT, which was insignificant. This means that fear-driven factors are a weaker predictor of behavioural intention than factors that align more closely with healthcare employees' self-concept and internal values. Adding response performance motivation to the theories decreased the effect. Regarding the impact of SDT variables on PMT variables, perceived competence has the strongest effect on self-efficacy, while the lowest effect is observed between perceived relatedness and threat vulnerability.

In the following sections, findings related to PMT variables will be discussed in the first part, followed in the second part by the findings related to SDT variables. Lastly, the differences between the two theories are discussed, attention is given to the variable response performance motivation, as well as the findings of the SDT towards the PMT variables.

Protection motivation theory

In the scoping review by Almansoori et al. (2023) on the frontiers of cybersecurity, self-efficacy is the most influential factor, followed by perceived severity, with response efficacy in third place. This finding contrasts with current research, which shows that response efficacy has the highest effect on behavioural intention compared to all other PMT variables. This suggests that healthcare employees value the effectiveness of a particular behaviour over their own confidence in their abilities to perform it. This aligns with the desire of employees to help

patients in the most effective manner to facilitate their recovery (Verpleegkundige & Verzorgende Nederland, n.d.). This may indicate that healthcare employees only perform safe cyber behaviour if it is proven to be effective.

The lowest effect came from perceived severity, which contrasts with the findings of the meta-analysis by Haag et al. (2021), where this variable had the second-highest effect. This could imply that healthcare employees perceive threats differently than those in other sectors. They deal daily with stressful situations and life-threatening emergencies (Heath et al., 2020). Experiencing such circumstances allows them to process and prioritise threats more effectively compared to other sectors where these kinds of situations do not occur.

This research indicated that coping appraisals are more effective regarding behavioural intention than threat appraisals, which contradicts the findings of Floyd's (2000) study. While threat appraisals enhance individuals' attention, they do not directly lead to managing the threat. Healthcare employees possess a problem-solving attitude towards fear (Arango-Martinez et al., 2024). This could suggest that the mindset of healthcare employees is primarily centred on taking action to tackle this challenge, driven by helping patients.

Self-determination theory

In the integrative review of Dombestein et al. (2020), autonomy was the most effective variable for caregivers' well-being. Orsini et al. (2015) indicate that including autonomy is most effective in teaching healthcare employees. In contrast, this study has other outcomes, namely that perceived competence is the most influential variable compared to perceived relatedness and autonomy. This may be because healthcare employees' ability to help directly impacts patients' recovery. If they feel confident in their actions, accompanied by minor anxiety, it positively influences their clinical performance (Yu et al., 2021). Despite the high level of perceived competence, it is still possible that under certain time pressure, which is common in healthcare organisations, employees can make inappropriate decisions (Groom et al., 2014; Lyle, 2009).

Perceived autonomy was placed with the second highest effect on behavioural intention. Freedom to choose what suits best stimulates the well-being of the employee and increases job satisfaction (Cicolini et al., 2014). It is likely that many healthcare workers all have to perform broadly the same work according to established protocols, but each completes it in their own way. By putting your own spin on it, working methods come closer to the sense of self. According to Hagger and Protogerou (2020), autonomously motivated healthcare employees are more likely to engage in these behaviours and persist in them.

Kam et al.'s (2022) study of organisational cybersecurity training relatedness is also defined as a variable that indicates the sense of connection with a particular behaviour. In their study, perceived relatedness had the most effect on behavioural intention, which is the opposite of this study's findings. This could imply that healthcare employees have different perceptions of relatedness. They may see cybersecurity as something that does not directly impact patients' wellness, making it less important. If they perceive it this way, it lies further away from their sense of self, which does not stimulate motivation. Not being motivated leads to not performing the behaviour (Gagné, 2014).

Difference between protection motivation theory and self-determination theory

In this study, the SDT had a stronger effect on behavioural intention than the PMT, which was considered not significant. The results of this study correspond with those of Menard et al. (2017) and Yang et al. (2020). This could imply that people, in general, are more sensitive to changing their behaviour when the motivation comes from internal satisfaction and matches personal and professional values. For healthcare workers, this can be explained by their identity, which mainly consists of helping and protecting others. According to Peethambaran and Naim (2023), work enjoyment can be interpreted as becoming part of one's identity. So, the intrinsic motivator factor of healthcare employees to help and protect patients outweighs the extrinsic motivator factor, which is based on avoiding risks. The population of healthcare employees, in combination with cyber-safe behaviour, influences the PMT significance. Healthcare employees' main focus is taking care of patients and helping them recover, so cybersecurity coping and threats feel further away from them. They may find it hard to see how patients could be affected by those attacks, or they may not consider it their duty to counter these dangers.

In the studies of Menard et al. (2017) and Yang et al. (2020), the response performance motivation variable had a higher effect than PMT and SDT variables. This aligns with the findings of this study, suggesting that if healthcare employees' self-concept is in line with safe cyber behaviour, it increases motivation to perform that behaviour (Forsyth, 2019). According to Hoeve et al. (2014), the self-concept of a person is strongly linked to the professional self-concept. The activities of healthcare workers are mainly providing care and protecting patients. This includes countering cyber-attacks where patients' personal data is leaked (Yeng et al., 2019), making safe cyber behaviour a part of one's professional self-concept and bringing it closer to healthcare employees' self-identity. This will increase the intrinsic motivation to protect themselves against cyber-attacks. Despite this high effect, adding response performance motivation to both the SDT and the PMT influenced the significance. Both theories were established as not significant, with response performance motivation included. This could be

explained by the high effect of response performance motivation, which could have overshadowed the other variables.

The individual variables of the SDT towards the individual variables of the PMT show that perceived competence had the strongest effect on self-efficacy. This indicates that when the self-concept aligns with safe cyber behaviour, healthcare employees are more likely to perceive trust in their ability to perform that behaviour. In the research of Yang et al. (2020), this effect between the variables came in second-highest, which is comparable to this study. Conversely, Menard et al. (2017) showed that the effect of these variables was very weak, even the lowest effect compared to other variables. The strong effect found in this study may be because perceived competence is a core component of self-efficacy. According to Bandura (1997), confidence in capability stimulates the ability to perform.

The lowest effect of the whole integrated model was between perceived relatedness and threat vulnerability, indicating that a sense of connection to cyber-safe behaviour does not have a big impact on the extent to which healthcare workers perceive their work devices within their organisations as potential targets of cybersecurity threats. This effect was lower compared to the studies of Menard et al. (2017) and Yang et al. (2020), who both indicated average effect sizes. It is plausible that if healthcare employees do not feel connected to safe cyber behaviour, they are also less likely to engage in staying informed about actual developments, thereby missing information about potential threats in cyber security.

Strengths and limitation

This research's primary strength is that it addresses the gap in the literature on the combined PMT and the SDT concerning healthcare employees. A lot of studies did research on the PMT or the SDT in combination with cyber security. Menard et al. (2017) and Yang et al. (2020) were the only ones who integrated these theories into one model based on information security targeting general organisations. This research covers the gap by specifying the target group of healthcare organisations' employees. To the knowledge of the researcher of this study, no other research combined the PMT and the SDT to get more insight into how these theories influence healthcare employees' behavioural intention to perform safe cyber behaviour.

The second strength of this study was that all participants were actual healthcare employees who were still working. This ensured that the data presented a realistic picture of how individuals behave and think in practice. Therefore, this research is suitable for providing appropriate recommendations to healthcare organisations affiliated with the ROAZ. However, this also had some limitations. The distribution of healthcare workers from various organisations was not equal. The study would have a stronger foundation if all healthcare

organisations had nearly equal numbers of employees participating. This would provide a more comprehensive and representative overview of the opinions of particular organisations. Nevertheless, several organisations participated and provided input, offering a wide diversity of responses and a representative picture of the motivational factors affecting employees' behavioural intentions in healthcare organisations.

A second limitation of this research is that it focused on measuring behavioural intention rather than actual behaviour. Behavioural intention is not completely coherent with how actual behaviour manifests itself (Wiedemann et al., 2009). Sheeran et al. (2005) termed this the intention-behaviour gap. External factors such as time pressure or workload could interfere, leading to different behaviour than intended (Moghavvemi et al., 2015). Nonetheless, the results are based on the real experiences of healthcare employees and could be applicable in real-life practices if all circumstances are favourable.

The final limitation concerns the measurement of behavioural intention. This study used for the variable behavioural intention one of the 16 items of response performance motivation. This was an oversight on the researcher's part. Subsequent studies should utilise a variable that serves as a more precise item that measures behavioural intention and place it in a separate paragraph to focus people's attention even more on this variable. Now, it did not measure behavioural intention directly but rather indirectly by reflecting employees' personal subjective feelings about how beneficial it is for them to engage in safe cyber behaviour. Nevertheless, the researcher has made every effort to rectify this issue. There is a slight difference in outcome when comparing the mean and standard deviation of the variable behavioural intention in the study by Menard et al. (2017), but the difference is negligible.

Future research

To build on the findings of this study, future research should translate the most effective outcomes into an intervention that can be experienced and test whether these are effective in day-to-day life. Prior to designing an intervention, it is essential to first investigate which types of interventions are most effective for healthcare employees. Additionally, ethical considerations must be carefully addressed, as the research involves human participants (Dupuis & Renaud, 2021). The PMT is a theory that is partly based on fear appraisals. Triggering anxiety in people can increase feelings of fear and tension; people with mental illnesses or at a particular age are more prone to this (Hyman & Tansey, 1990).

Future studies should focus on contextual factors that could influence the behaviour of healthcare employees. In the healthcare sector, contextual factors are particularly sensitive and could affect various study outcomes (Coles et al., 2020). Relevant factors may include high

workload, type of department, task prioritisation, ethical considerations, and ethnic background. To address this gap, it would be helpful to conduct observational studies to record actual behaviour and observe how external factors influence it would be beneficial.

Conclusion

Nowadays, cyber-attacks are unavoidable in healthcare organisations. Due to the vast amount of sensitive data they possess, cyber attackers consider them attractive targets. As a result, healthcare organisations experience more cyberattacks compared to other sectors. Countering these attacks by using advanced technology is not enough; the focus should be on understanding employee behaviour and what is encouraging them to counter these attacks. This research combined two academic theories, the PMT and the SDT, and added the variable response performance motivation into real-world practices for healthcare organisations. It gave insight into motivational factors of the intentions that healthcare employees have to behave cyber-safe behaviour.

The findings indicate that, compared with PMT variables as a whole, SDT as a whole more strongly predicted behavioural intention to engage in safe cyber behaviour. This means that fear-driven factors are a weaker predictor of behavioural intention than factors that align more closely with healthcare employees' self-concept and internal values. Adding response performance motivation to both theories decreased the strength of the prediction and influenced the significance negatively. Despite that, the variable response performance motivation had an outstanding effect and is considered the most effective variable for behavioural intention. Perceived competence and response efficacy were also perceived as impactful variables. Regarding the impact of the individual SDT variables on the individual PMT variables, perceived competence had the strongest effect on self-efficacy.

References

Abraham, S., & Chengalur-Smith, I. (2019). Evaluating the effectiveness of learner controlled information security training. *Computers & Security*, *87*, 101586.

Alahmari, S. (2021). *A model for describing and encouraging cyber security knowledge sharing to enhance awareness* (Doctoral dissertation, University of Glasgow).

Aljuraid, R., & Justinia, T. (2022). Classification of challenges and threats in healthcare cybersecurity: a systematic review. *Advances in Informatics, Management and Technology in Healthcare*, 362–365.

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behaviour: A systematic review of studies and theories. *Applied Sciences, 13*(9), 5700.

Alonso, R. K., Vélez, A., & Martínez-Monteagudo, M. C. (2023). Interventions for the Development of Intrinsic Motivation in University Online Education: Systematic Review—Enhancing the 4th Sustainable Development Goal. *Sustainability*, *15*(13), 98

Alshmemri, M., Shahwan-Akl, L., & Maude, P. (2017). Herzberg's two-factor theory. *Life Science Journal*, *14*(5), 12-16.

Arango-Martinez, G., Sarmiento, L. B., Forero, I. C., Carreno, L. C., & Cadena-Camargo, Y. (2024). Fear of the unknown: Experience of frontline healthcare workers with coping strategies used to face the COVID 19 pandemic. *PLOS Global Public Health*, *4*(8), e0003373.

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., et al. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making, 20*(1). https://doi.org/10.1186/s12911-020-01161-7

Babenko, O. (2018). Professional well-being of practicing physicians: The roles of autonomy, competence, and relatedness. *Healthcare, 6*(1), 12. https://doi.org/10.3390/healthcare6010012

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv*. https://doi.org/10.48550/arXiv.1901.02672

Baldwin, T. T., Magjuka, R. J., & Loher, B. T. (1991). The perils of participation: Effects of choice of training on trainee motivation and learning. *Personnel psychology*, *44*(1), 51–65.

Bandhu, D., Mohan, M. M., Nittala, N. A. P., Jadhav, P., Bhadauria, A., & Saxena, K. K. (2024). Theories of motivation: A comprehensive analysis of human behaviour drivers. *Acta Psychologica*, *244*, 104177.

Bandura, A. (1997). *Self-efficacy: The exercise of control.* W. H. Freeman.

Betella, A., & Verschure, P. F. (2016). The affective slider: A digital self-assessment scale for the measurement of human emotions. *PloS one*, *11*(2), e0148037.

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., ... & Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of Medical Systems*, *44*, 1–9.

Boer, F. (2019). Healthcare innovation—Experiences from the Netherlands. *Vestnik of Saint Petersburg University. Medicine, 14*(3), 245–254.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS quarterly*, 39(4), 837–864.

Brehm, J. W. (1966). *A theory of psychological reactance.* Oxford, England: Academic Press.

Centraal Bureau voor de Statistiek (CBS). (2022, November 16). *Helft zorgwerknemers vindt werkdruk te hoog.* Retrieved from https://www.cbs.nl/nl-nl/nieuws/2022/46/helft-zorgwerknemers-vindt-werkdruk-te-hoog

Cialdini, R. B. (2007). *Influence: The psychology of persuasion* (Vol. 55, p. 339). New York: Collins.

Cicolini, G., Comparcini, D., & Simonetti, V. (2014). Workplace empowerment and nurses' job satisfaction: a systematic literature review. *Journal of Nursing Management*, *22*(7), 855–871.

Coles, E., Anderson, J., Maxwell, M., Harris, F. M., Gray, N. M., Milner, G., & MacGillivray, S. (2020). The influence of contextual factors on healthcare quality improvement initiatives: a realist review. *Systematic reviews*, *9*, 1–22.

Connelly, L. M. (2016). Cross-sectional survey research. *Medsurg Nursing*, *25*(5).

Connor, L., Dean, J., McNett, M., Tydings, D. M., Shrout, A., Gorsuch, P. F., Hole, A., Moore, L., Brown, R., Melnyk, B. M., & Gallagher-Ford, L. (2023). Evidence-based practice improves patient outcomes and healthcare system return on investment: Findings from a scoping review. *Worldviews on evidence-based nursing*, *20*(1), 6–15. https://doi.org/10.1111/wvn.12621

Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *45*(4), 51–71.

Dancey, C. P. (2007). *Statistics without maths for psychology* (4th ed.). Prentice Hall.

Deci, E. L., Olafsen, A. H., & Ryan, R. M. (2017). Self-determination theory in work organizations: The state of a science. *Annual Review of Organizational Psychology and Organizational Behavior, 4*(1), 19–43. https://doi.org/10.1146/annurev-orgpsych-032516-113108.

Diwakar, S., Kolil, V. K., Francis, S. P., & Achuthan, K. (2023). Intrinsic and extrinsic motivation among students for laboratory courses-Assessing the impact of virtual laboratories. *Computers & Education*, *198*, 104758.

Dombestein, H., Norheim, A., & Lunde Husebø, A. M. (2020). Understanding informal caregivers' motivation from the perspective of self-determination theory: An integrative review. *Scandinavian Journal of Caring Sciences, 34*(2), 267–279.

Dulaney, E. S. (2021). *True self in threat resilience: Using essentialist self-views to neutralize personal morality threats.*

Dupuis, M., & Renaud, K. (2021). Scoping the ethical principles of cybersecurity fear appeals. *Ethics and Information Technology*, *23*(3), 265–284.

Erdfelder, E., Faul, F., & Buchner, A. (1996). GPOWER: A general power analysis program. *Behavior research methods, instruments, & computers*, *28*, 1–11

Feraru, I., & Bacali, L. (2024). Explore the intersection of Self-Determination Theory and cybersecurity education-A literature review. *International Journal of Advanced Statistics and IT&C for Economics and Life Sciences*, *14*(1).

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. In *Human Aspects of Information Security, Privacy, and Trust: Third International Conference, HAS 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015. Proceedings 3* (pp. 36-47). Springer International Publishing.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Forsyth, D. R. (2019). *Group dynamics* (7th ed.). Belmont, CA: Wadsworth Cengage Learning.

Francis, S. P., Kolil, V. K., Pavithran, V., Ray, I., & Achuthan, K. (2024). Exploring gender dynamics in cybersecurity education: a self-determination theory and social cognitive theory perspective. *Computers & Security*, *144*, 103968.

Gagné, M. (Ed.). (2014). *The Oxford handbook of work engagement, motivation, and self-determination theory*. Oxford University Press, USA.

George, D., & Mallery, P. (2019). *IBM SPSS Statistics 26 step by step*. Routledge. https://doi.org/10.4324/9780429056765

Giwah, A. D., Wang, L., Levy, Y., & Hur, I. (2019). Empirical assessment of mobile device users' information security behaviour towards data breach: Leveraging protection motivation theory. *Journal of Intellectual Capital, 21*(2), 215–233.

Gragg, D. (2003). A multi-level defense against social engineering. *SANS Reading Room*, *13*, 1-21.

Groom, J. A., Henderson, D., & Sittner, B. J. (2014). NLN/Jeffries simulation framework state of the science project: Simulation design characteristics. *Clinical Simulation in Nursing, 10*(7), 337–344.

Gupta, A., Patel, V. L., & Greenes, R. A. (Eds.). (2015). *Advances in Healthcare informatics and Analytics* (Vol. 19). Springer.

Haag, S., Siponen, M., & Liu, F. (2021). Protection motivation theory in information systems security research: A review of the past and a road map for the future. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 52*(2), 2567.

Hagger, M. S., & Protogerou, C. (2020). Self-determination theory and autonomy support to change healthcare behavior. *The Wiley handbook of healthcare treatment engagement: Theory, research, and clinical practice*, 141–158.

Healy, K. (2016). A theory of human motivation by Abraham H. Maslow (1942). *The British Journal of Psychiatry*, *208*(4), 313-313.

Heartfield, R., & Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers & Security*, 76, 101–127.

Heath, C., Sommerfield, A., & von Ungern-Sternberg, B. S. (2020). Resilience strategies to manage psychological distress among healthcare workers during the COVID-19 pandemic: a narrative review. *Anaesthesia*, *75*(10), 1364–1371.

Hoeve, Y. T., Jansen, G., & Roodbol, P. (2014). The nursing profession: Public image, self-concept and professional identity. A discussion paper. *Journal of advanced nursing*, *70*(2), 295–309.

Hoffman, S. A. E. (2020). Cybersecurity threats in healthcare organizations: exposing vulnerabilities in the healthcare information infrastructure. *World Libraries, 24*(1).

Hogan, J. (2005). *Motivation. In J. J. Bolhuis (Ed.), The behaviour of animals: Mechanisms, function and evolution* (pp. 41–70). Blackwell Publishing.

Holmes, M., & Ophoff, J. (2019). Online security behaviour: Factors influencing intention to adopt two-factor authentication. In *Proceedings of the 14th International Conference on Cyber Warfare and Security, ICCWS 2019* (pp. 123–132). Academic Conferences International Limited.

Hooper, V., & Blunt, C. (2020). Factors influencing the information security behaviour of IT employees. *Behaviour & Information Technology, 39*(8), 862–874.

Howell, C. J. (2021). *Self-protection in cyberspace: Assessing the processual relationship between thoughtfully reflective decision making, protection motivation theory, cyber hygiene, and victimization*. University of South Florida.

Hughes, A. (2016). *Student information security behaviors and attitudes at a private liberal arts university in the Southeastern United States* (Doctoral dissertation, Northcentral University). ProQuest Dissertations & Theses Global.

Hyman, M. R., & Tansey, R. (1990). The ethics of psychoactive ads. *Journal of Business Ethics*, *9*, 105–114.

Kahanda, G., Rider, S., & Mukhopadhyay, S. (2023). Impact versus frequency on cybersecurity breach trends in the business and medical industry to identify human error. In *International Conference on Global Security, Safety, and Sustainability* (pp. 77–96). Cham: Springer Nature Switzerland.

Kam, H. J., Menard, P., Ormond, D., & Crossler, R. E. (2020). Cultivating cybersecurity learning: An integration of self-determination and flow. *Computers & Security, 96*, 101875.

Kam, H. J., Ormond, D. K., Menard, P., & Crossler, R. E. (2022). That's interesting: An examination of interest theory and self-determination in organisational cybersecurity training. *Information Systems Journal, 32*(4), 888–926.

Kamerer, J. L., & McDermott, D. (2020). Cybersecurity: Nurses on the front line of prevention and education. *Journal of Nursing Regulation*, 10(4), 48–53.

Le Bris, A., & El Asri, W. (2016). State of cybersecurity & cyber threats in healthcare organizations. *ESSEC Business School*, 12.

Lee Rodgers, J., & Nicewander, W. A. (1988). Thirteen ways to look at the correlation coefficient. *The American Statistician, 42*(1), 59–66. https://doi.org/10.1080/00031305.1988.10475524

Legault, L. (2020). Self-determination theory. In *Encyclopedia of personality and individual differences* (pp. 4694–4702). Springer International Publishing.

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behaviour. *Computers in Human Behavior Reports*, 5, 100165.

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Health Care, 24*(1), 1–9.

Lyle, K. E. (2009). *Teachers' perceptions of their technology education curricula* (Doctoral dissertation). Immaculata College.

Makhanova, A., & Shepherd, M. A. (2020). Behavioral immune system linked to responses to the threat of COVID-19. *Personality and Individual Differences*, *167*, 110221.

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior, 92*, 139–150. https://doi.org/10.1016/j.chb.2018.11.002

Martínez-Caro, E., Cegarra-Navarro, J. G., García-Pérez, A., & Fait, M. (2018). Healthcare service evolution towards the Internet of Things: An end-user perspective. *Technological Forecasting and Social Change*, 136, 268-276.

McDermott, D. S., Kamerer, J. L., & Birk, A. T. (2019). Electronic health records: A literature review of cyber threats and security measures. *International Journal of Cyber Research and Education (IJCRE)*, 1(2), 42–49.

McLeod, L. J., Hine, D. W., Please, P. M., & Driver, A. B. (2015). Applying behavioural theories to invasive animal management: Towards an integrated framework. *Journal of Environmental Management, 161,* 63–71.

Mehraj, H., Jayadevappa, D., Haleem, S. L. A., Parveen, R., Madduri, A., Ayyagari, M. R., & Dhabliya, D. (2021). Protection motivation theory using multi-factor authentication for providing security over social networking sites. *Pattern Recognition Letters*, *152*, 218-224.

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of*

Management Information Systems, 34(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

Mihailescu, M., & Mihailescu, D. (2018). The emergence of digitalisation in the context of health care.

Moghavvemi, S., Salleh, N. A. M., Sulaiman, A., & Abessi, M. (2015). Effect of external factors on intention–behaviour gap. *Behaviour & Information Technology, 34*(12), 1171–1185. https://doi.org/10.1080/0144929X.2015.1055801

Mou, J., Cohen, J. F., Bhattacherjee, A., & Kim, J. (2022). A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach. *Journal of the Association for Information Systems*, *23*(1), 196-236.

Mou, J., Cohen, J., & Kim, J. (2017). A meta-analytic structural equation modeling test of protection motivation theory in information security literature.

Moyo, N., Bhappu, A. D., Bhebhe, M., & Ncube, F. (2022). Perceived risk of COVID-19 and employee decision-making: How psychological distress during the pandemic increases negative performance outcomes among healthcare workers. *International Journal of Environmental Research and Public Health*, *19*(11), 6762.

Nemoto, T., & Beglar, D. (2014, November). Likert-scale questionnaires. In *JALT 2013 conference proceedings* (Vol. 108, No. 1, pp. 1–6).

Nikolopoulou, K. (2022, October 20). *What Is Convenience Sampling? | Definition & Examples.* Scribbr. Retrieved December 03, 2022, from https://www.scribbr.com/methodology/convenience-sampling/

Nisbet, E. K., & Zelenski, J. M. (2024). Nature relatedness and subjective well-being. In *Encyclopedia of quality of life and well-being research* (pp. 4602–4610). Springer International Publishing.

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA–Journal of Business and Public Administration, 13*(1), 49–72.

Norman, P., Boer, H., Seydel, E. R., & Mullan, B. (2015). Protection motivation theory. In R. P. C. M. & R. G. J. (Eds.), *Predicting and changing health behaviour: Research and practice with social cognition models* (3rd ed., pp. 70–106). Open University Press.

Ophoff, J., & Lakay, M. (2019). Mitigating the ransomware threat: a protection motivation theory approach. In *Information Security: 17th International Conference, ISSA 2018, Pretoria, South Africa, August 15–16, 2018, Revised Selected Papers 17* (pp. 163-175). Springer International Publishing.

Orsini, C., Evans, P., & Jerez, O. (2015). How to encourage intrinsic motivation in the clinical teaching environment?: A systematic review from the self-determination theory. *Journal of Educational Evaluation for Health Professions, 12*(1), 1–8. https://doi.org/10.3352/jeehp.2015.12.8

Ortega-Lapiedra, R., Barrado-Narvión, M. J., & Bernués-Oliván, J. (2023). Acquisition of competencies of nurses: improving the performance of the healthcare system. *International journal of environmental research and public health*, *20*(5), 4510.

Osawaru, G. (2024). *Electronic health record data breaches in US healthcare industry: A quantitative study using the Protection Motivation Theory (PMT) to mitigate data breaches* (Doctoral dissertation, University of the Cumberlands).

Patel, D., & Alismail, A. (2024). Relationship between cognitive load theory, intrinsic motivation and emotions in healthcare professions education: a perspective on the missing link. *Advances in Medical Education and Practice*, 57–62.

Peethambaran, M., & Naim, M. F. (2023). Connecting the dots: linking empowering leadership, employee work passion, and flourishing-at-work. *Industrial and Commercial Training*, *55*(4), 544–557

Prentice-Dunn, S., & Rogers, R. W. (1997). Protection motivation theory.

Prentice-Dunn, S., McMath, B., & Cramer, R. (2009). Protection motivation theory and stages of change in sun protective behaviour. *Journal of Health Psychology, 14*(2), 297–305.

Raj Sreenath, S. S., Hewitt, B., & Sreenath, S. (2024). Understanding security behaviour among healthcare professionals by comparing results from technology threat avoidance theory and protection motivation theory. *Behaviour & Information Technology*, 1-16.

Roca, J. C., & Gagné, M. (2008). Understanding e-learning continuance intention in the workplace: A self-determination theory perspective. *Computers in human behavior*, *24*(4), 1585–1604.

Rodgers, W. M., Markland, D., Selzler, A. M., Murray, T. C., & Wilson, P. M. (2014). Distinguishing perceived competence and self-efficacy: An example from exercise. *Research quarterly for exercise and sport*, *85*(4), 527–539.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology, 91*(1), 93–114.

Romero-Masters, P. M. (2023). *A Qualitative Study of Self-Determination Theory in Cybersecurity Using Autonomy Framing*. The University of Wisconsin-Madison.

Ryan, R. M. (2017). *Self-determination theory: Basic psychological needs in motivation, development, and wellness*. Guilford Press.

Ryan, R. M., & Deci, E. L. (2020). Intrinsic and extrinsic motivation from a self-determination theory perspective: Definitions, theory, practices, and future directions. *Contemporary educational psychology*, *61*, 101860.

Ryan, R. M., & Deci, E. L. (2024). Self-determination theory. In *Encyclopedia of quality of life and well-being research* (pp. 6229-6235). Cham: Springer International Publishing.

Schaab, P., Beckers, K., & Pape, S. (2017). Social engineering defence mechanisms and counteracting training strategies. *Information & Computer Security*, *25*(2), 206–222.

Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2021). Employees' behaviour in phishing attacks: what individual, organizational, and technological factors matter?. *Journal of Computer Information Systems, 61*(6), 539–550.

Sheeran, P., Webb, T. L., & Gollwitzer, P. M. (2005). The interplay between goal intentions and implementation intentions. *Personality and Social Psychology Bulletin, 31*(1), 87–98. https://doi.org/ 10.1177/0146167204271308

Shi, J., Cook, A. S., van Vugt, M., & Bakker, A. B. (2025). Do individual differences in perceived vulnerability to disease shape employees' work engagement?. *Personality and Individual Differences*, *232*, 112863.

Shorey, S., & Lopez, V. (2021). Self-Efficacy in a nursing context. *Health promotion in health care–Vital theories and research*, 145–158.

Siponen, M. T. (2000). "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management and Computer Security, 8*(1), pp. 31–41.

Stajano, F., & Wilson, P. (2011). Understanding scam victims: seven principles for systems security. *Communications of the ACM*, *54*(3), 70-75.

Sutton, S. (2001). Health behaviour: Psychosocial theories. In P. R. H. L. T. & P. L. W. W. (Eds.), *Psychosocial approaches to health and health care* (pp. 117–130). Wiley.

Tananuvat, N., Tansanguan, S., Wongpakaran, N., & Wongpakaran, T. (2022). Role of neuroticism and perceived stress on quality of life among patients with dry eye disease. *Scientific reports*, *12*(1), 7079. https://doi.org/10.1038/s41598-022-11271-z

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behaviour. *Computers & Security*, *70*, 376–391.

Thornburgh, T. (2004, October). Social engineering: the" dark art". In *Proceedings of the 1st annual Conference on Information Security Curriculum Development* (pp. 133-135).

Tiemeijer, W. L. (2010). *Hoe mensen keuzes maken: De psychologie van het beslissen* (p. 132). Amsterdam University Press.

Tilson, D., Lyytinen, K., & Sørensen, C. (2010). Digital infrastructures: The missing IS research agenda. *Information Systems Research, 21*(4), 748–759.

Towbin, R. S. (2019). *A protection motivation theory approach to healthcare cybersecurity: A multiple case study*. Northcentral University.

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security, 59*, 138–150.

Verpleegkundigen & Verzorgenden Nederland (V&VN). (n.d.). *De nationale beroepscode voor verpleegkundigen en verzorgenden.* https://www.venvn.nl/media/042ooa1u/de-nationale-beroepscode-voor-verpleegkundigen-en-verzorgenden.pdf

Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *Journal of Information Privacy and Security*, *9*(4), 52–79.

Wanyonyi, E., Rodrigues, A., Abeka, S. O., & Ogara, S. (2017). Effectiveness of security controls on electronic health records

Wiedemann, A. U., Schüz, B., Sniehotta, F. F., Scholz, U., & Schwarzer, R. (2009). Disentangling the relation between intentions, planning, and behavior: A moderated mediation analysis. *Psychology and Health, 24*(1), 67–79. https://doi.org/10.1080/08870440801958214

Yang, N., Singh, T., & Johnston, A. (2020). A Replication Study of User Motivation in Protecting Information Security using Protection Motivation Theory and Self Determination Theory. *AIS Transactions on Replication Research*, *6*(1), 10.

Yeng, P., Yang, B., & Snekkenes, E. (2019). Observational measures for effective profiling of healthcare staffs' security practices. *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, *2*, 397–404.

Yu, J. H., Chang, H. J., Kim, S. S., Park, J. E., Chung, W. Y., Lee, S. K., … & Jung, Y. J. (2021). Effects of high-fidelity simulation education on medical students' anxiety and confidence. *PloS ONE, 16*(5), e0251078. https://doi.org/10.1371/journal.pone.0251078

Z-CERT. (2023). *Cybersecurity dreigingsbeeld voor de zorg 2023.* Z-CERT. https://z-cert.nl/cybersecurity-dreigingsbeeld-voor-de-zorg-2023/

Appendix

Appendix A: Questionnaire

Dear participant,

This survey is about what motivates you as a healthcare professional to perform your work safely on work devices within your organisation, such as computers and phones. By participating in this survey, you will help us understand the factors that influence this. This could ultimately help make healthcare safer. The research is part of my Master's thesis at the University of Twente for Acute Care Euregio.

Confidentiality and consent

Your participation is entirely voluntary and all data will be treated anonymously and confidentially.
We will only use the data for research purposes and it will not be shared with third parties.
By giving your consent below by clicking: YES, you consent to participate in this study and give permission for your input to be used for research purposes.

Contact

If you have any questions about the study or the questionnaire, please feel free to contact me at crisisbeheersing_euregio@mst.nl.
University of Twente: i.vansintemaartensdijk@utwente.nl

Thank you for your time and participation. Your input is important for the success of this study.

Kind regards,
Koen Jannink
Acute Care Euregio
University of Twente

Consent

I hereby consent to participate in this study.

- Yes
- No

Demographic questions

How do you identify yourself?

- Male
- Female
- Non-binary/third gender
- I'd rather not say

What is your age?

- Younger than 18
- 18 - 24
- 25 - 34
- 35 - 44
- 45 - 54
- 55 - 64
- 65 - 74
- 75 - 84
- 85 or older

How long have you been working for your organisation?

- 0 - 5
- 6 - 10
- 11 - 15
- 16 - 20
- 21 - 25
- 26 - 30
- 30 +

Which sector does your organisation fall under?

- Hospital
- GP care
- Ambulance service
- Medical specialist care
- Nursing and care homes and home care (VVT)
- GGD/ GHOR

- Mental health care (GGD)
- Obstetric care (1st and 2nd line)
- None of the above, but....

Have you ever been scammed over the internet or had your personal details stolen at work?

- Yes
- No
- Would rather not say

I feel well informed by my organisation not to become a victim of cybercrime?

- Likert scale on a 5 point ranging from ‘strongly agree’ to ‘strongly disagree’. We coded the responses as follows; 1 - ‘strongly disagree’, 2 - ‘disagree’, 3 - ‘neutral’, 4 - ‘agree’, 5 - ‘strongly agree’

Instruction page

Clarification of common terms used in this research on the motivating factors that encourage healthcare professionals to engage in cyber-secure behaviour.

Hack: someone who tries to access your computer or phone in a clever or secret way without permission.
Work devices: these are the devices you use for work, such as a laptop, phone or tablet.
Security measures: these are the steps you take to keep your work devices and data secure. For example, consider setting strong passwords, using multi-factor authentication (where you have an extra step besides your password to log in), or sending emails securely via special programmes like Zivver etc.

Once you get to the questions, you can answer them by choosing the answer that best suits your situation. The question can be answered on a Likert scale from 1 (totally disagree) to 5 (totally agree), or with a slider that can be set from 1 (totally disagree) to 5 (totally agree).

Variables

Threat severity

- A security breach on my *device* in my organisation would be a serious problem for me
- Loss of information of my organisation resulting from hacking in would be a serious problem for me
- Having my confidential information on my *device* in my organisation accessed by someone without my consent or knowledge would be a serious problem for me.
- Having someone successfully attack and damage my *device* in my organisation would be very problematic for me
- I view information security attacks on my *device* in my organisation as harmful
- I believe that protecting the information on my *device* in my organisation is important

Likert scale on a 5 point ranging from '*strongly agree'* to '*strongly disagree'*. We coded the responses as follows; 1 – '*strongly disagree*', 2 – '*disagree'*, 3 – '*neutral*', 4 – '*agree*', 5 – '*strongly agree'*

Threat vulnerability

- I could be subject to a serious information security threat in my organisation
- I feel that my *device* in my organisation could be vulnerable to a security threat
- It is likely that my *device* in my organisation will be compromised in the future
- My information and data of the organisation are vulnerable to security breaches
- My organisation could fall victim to a malicious attack if I fail to follow good security practices

Likert scale on a 5 point ranging from '*strongly agree'* to '*strongly disagree'*. We coded the responses as follows; 1 – '*strongly disagree*', 2 – '*disagree'*, 3 – '*neutral*', 4 – '*agree*', 5 – '*strongly agree'*

Self-efficacy

- I feel comfortable taking measures to secure my *device* in my organisation
- Taking the necessary security measures in my organisation is entirely under my control
- I have the resources and the knowledge to take the necessary security measures to prevent my organisation becoming a victim of cybercrime.

- Taking the necessary security measures to protect my organisation from cybercrime is easy
- I can protect my *device* in my organisation by myself
- I can enable security measures on my *device* in my organisation

Likert scale on a 5 point ranging from '*strongly agree'* to '*strongly disagree'*. We coded the responses as follows; 1 – '*strongly disagree*', 2 – '*disagree'*, 3 – '*neutral*', 4 – '*agree*', 5 – '*strongly agree'*

Response efficacy

- Enabling security measures on my *device* in my organisation will prevent security breaches
- Implementing security measures on my *device* in my organisation is an effective way to prevent hackers
- Enabling security measures on my *device* in my organisation will prevent hackers from stealing my identity
- The preventative measures available to stop people from getting confidential personal or financial information of my organisation on my *device* in my organisation are effective

Likert scale on a 5 point ranging from '*strongly agree'* to '*strongly disagree'*. We coded the responses as follows; 1 – '*strongly disagree*', 2 – '*disagree'*, 3 – '*neutral*', 4 – '*agree*', 5 – '*strongly agree'*

Response cost

- Taking security measures to prevent my organisation becoming a victim of cybercrime inconveniences me
- There are too many overheads associated with taking security measures to protect my *device* in my organisation
- Taking security measures to prevent my organisation becoming a victim of cybercrime would require considerable investment of effort
- Implementing security measures on my *device* in my organisation would be time consuming

- The cost of implementing recommended security measures to protect my organisation from cybercrime exceeds the benefits
- The impact of security measures to protect my organisation from cybercrime on my productivity exceeds the benefits

Likert scale on a 5 point ranging from '*strongly agree'* to '*strongly disagree'*. We coded the responses as follows; 1 – '*strongly disagree*', 2 – '*disagree'*, 3 – '*neutral*', 4 – '*agree*', 5 – '*strongly agree'*

Response performance motivation

I choose to use security measures .... (passwords, multi-factor authentication, secure mail (Zivver), awareness campaigns, meetings, e-learning etc.)…because I think that this activity is interesting.

1. …because I think that this activity is fun.
2. …because I feel good when doing this activity.
3. …because I think that this activity is good for me.
4. …because I decided that this activity is beneficial.
5. …because I believe that this activity is important to me.
6. …because it is something that I have to do.
7. …because I don't have any choice.
8. …but I don't see what the activity brings me.
9. …but I am not sure it is a good thing to pursue it.
10. …but personally I don't see any good reasons to do this activity.

- Reversed coding items: 9, 10, 11, 12, 13, 14, 15, 16

Likelihood to install slider scale, 0–5 (0 = Extremely unlikely; 5 = Extremely likely)

Perceived Relatedness

- I feel that I am emotionally invested in cybersecurity prevention behaviours
- I feel a personal connection to behaviour that prevent my organisation becoming a victim of cybercrime.
- I feel attached to behaviour that prevent my organisation from becoming a victim of cybercrime.

Likert scale on a 5 point ranging from '*strongly agree'* to '*strongly disagree'*. We coded the responses as follows; 1 – '*strongly disagree*', 2 – '*disagree'*, 3 – '*neutral*', 4 – '*agree*', 5 – '*strongly agree'*

Perceived competence

- I feel I have been making progress with my cybersecurity prevention behaviour to protect my organisation from becoming victim of cybercrime.
- I feel that I'm doing a good job with my cybersecurity preventive behaviour to protect my organisation from cybercrime
- I feel that I can manage cybersecurity prevention behaviour to protect my organisation from cybercrime.

Likert scale on a 5 point ranging from '*strongly agree'* to '*strongly disagree'*. We coded the responses as follows; 1 – '*strongly disagree*', 2 – '*disagree'*, 3 – '*neutral*', 4 – '*agree*', 5 – '*strongly agree'*

Perceived autonomy

- The behaviour I learned from my organisation to perform cybersecurity prevention behaviour are compatible with my choices and interests
- I feel that what I'm told to learn from my organisation to perform cybersecurity prevention behaviour fits perfectly with what I prefer to learn.
- I feel that I have the opportunity to make choices within my organisation concerning what I learn to perform cybersecurity prevention behaviour

Likert scale on a 5 point ranging from '*strongly agree'* to '*strongly disagree'*. We coded the responses as follows; 1 – '*strongly disagree*', 2 – '*disagree'*, 3 – '*neutral*', 4 – '*agree*', 5 – '*strongly agree'*

Debrief

Purpose of the Study was
This study investigated the impact of factors from Protection Motivation Theory (PMT) and Self-Determination Theory (SDT) on healthcare professionals' cybersecurity-related behaviours. By completing this questionnaire, you helped us understand how different motivational factors influence healthcare professionals to engage in cybersecurity-related behaviours.

What happens and with the data?
The data will only be used for the purposes of this study, it will not be shared with third parties. At the end of the study, a recommendation will be made to your organisation, giving them insight into what factors motivate healthcare professionals to engage in cyber-secure behaviour.

Contact
If you have any questions about the study or the questionnaire, please feel free to contact me at crisisbeheersing_euregio@mst.nl.
University of Twente: i.vansintemaartensdijk@utwente.nl

Ending

Thank you for participating in this survey!

Your input is of great value to my research and contributes to a better understanding of how cybersecurity is perceived and applied within the healthcare sector. With your input, we can work on improvements that will strengthen both the security of sensitive information and the overall working environment.

Again, thank you very much for your time and cooperation!