Eurasian Journal of Social Sciences, 9(2), 2021, 98-122
DOI: 10.15604/ejss.2021.09.02.004

EURASIAN JOURNAL OF SOCIAL SCIENCES

www.eurasianpublications.com

IDENTIFYING BEHAVIORAL CONSTRUCTS IN RELATION TO USER CYBERSECURITY BEHAVIOR

Thulani Mashiane
Corresponding Author: University of South Africa, South Africa
Email: 63383993@mylife.unisa.ac.za

Elmarie Kritzinger
University of South Africa, South Africa
Email: kritze@unisa.ac.za

Received: May 11, 2021 Accepted: June 24, 2021

Abstract

A behavior such as enabling two factor authentication has a positive impact on a users' information security. It is assumed that given the benefits, users will want to perform this cybersecurity related behavior. However, some users choose not to perform the beneficial security behavior. Varied explanations have been provided as to why users choose to perform or not perform cybersecurity behaviors. The factors that influence users in the decision making of whether to perform or not perform a cybersecurity related behavior are referred to as constructs. This study seeks to combine the results of selected studied, with the aim of identifying prominent user cybersecurity behavior constructs, as well as the relationships between the constructs. The contributions made by the study is the consolidated visualization of behavior constructs that have an influence on user cybersecurity behavior. Furthermore, the study also provides practical applications of the cybersecurity behavior constructs. To achieve the goals of the study, a literature review is used as the study methodology. Data from previous studies is systematically collected, and analyzed. The study makes use of the Theoretical Domains Theory as a tool, which aids in consolidating the different behavior constructs found in cybersecurity literature. The constructs Beliefs about Capabilities, Beliefs about Consequences, Reinforcements, Social Influences, Intentions, Emotions, Social/Professional Role and Identity, Knowledge and Skills are found to have influence on cybersecurity behavior.

Keywords: Cybersecurity, Behavior, Construct, Theoretical Domains Framework

1. Introduction

An Internet user, or simply user, is a person that makes use of the Internet to carry out activities (Addae *et al.* 2019; Radic *et al.* 2020). On an individual level, a user makes use of the Internet for electronic activities such as information gathering, entertainment, education, communication, and performing transactions (Reglitz, 2020; Skovhoj, 2020). On an organizational level, the Internet is used for activities such as to carry out transactions, meetings and data storage (de Boer *et al.* 2019). On a national level, some countries' critical assets such as electricity infrastructure, medical infrastructure, and financial systems rely on the Internet to operate (Abbadi, 2011;

McDonald, 2017). Given the importance of the Internet, securing the Internet has become a priority for governments, organizations, and individuals.

Cybersecurity is the term used to refer to the protection of computer systems, hardware and software, and networks from theft or damage (Herrmann and Pridöhl, 2020). To implement cybersecurity, governance instruments such as policies, standards, and guidelines provide information to be used when designing, implementing, or using the Internet (de Boer *et al.* 2019; Ying and Zonghua, 2020). To ensure cybersecurity, the appropriate technology, both hardware and software, has to be in place. Furthermore, users are a key requirement to ensure cybersecurity (Herrmann and Pridöhl, 2020), because users are the ones that ensure that the appropriate technology, policies and standards are in place and are used as expected. The researchers such as Kuppusamy *et al.* (2020), Safa *et al*. (2015) and Michie *et al.* (2008) highlight that user behaviors are key in the maintenance of cybersecurity (Kuppusamy *et al.* 2020; Michie *et al.* 2008; Safa *et al.* 2015). The actions taken by users to ensure cybersecurity can be restated as user cybersecurity behaviors. The understanding of user behavior in the cybersecurity domain has not yet reached the maturity of the understanding of technology and governance.

The contribution of this paper is towards the understanding of user cybersecurity behavior by identifying and visualizing the relationship between behavior constructs and cybersecurity behavior. The findings of the study are aimed at contributing to the design of cybersecurity user behavior intervention initiates. By knowing how the identified behavior constructs impact cybersecurity behavior, the designer of the cybersecurity user behavior intervention initiates has the opportunity to incorporate behavior change strategies which focus on the specific user behavior constructs.

The paper is presented as follows: the second section of the paper presents the background to the study. With the Background section, descriptions to cybersecurity behavior environments, cybersecurity behavior categories, cybersecurity behavior constructs and the Theoretical Domains Framework are presented. The third section of the paper presents a description of the methodology followed in the study. The fourth section presents the results of the study, which is, the relationship between cybersecurity behavior categories and cybersecurity behavior constructs. The fifth section of the study presents a discussion on how the results of the study can be practically implemented. Finally, the sixth section concludes the study.

2. Background

Cybercrime victims' increasing number has led researchers to study other methods of changing user behavior (Bada *et al*. 2019; Briggs *et al.* 2017; Furnell *et al.* 2018; Gangire *et al.* 2019; Jansen and van Schaik, 2019; Shah and Agarwal, 2020; Skinner *et al.* 2018). Traditional intervention strategies, such as Cybersecurity Awareness (CSA) campaigns, have proven to be ineffective. Bada *et al.* (2019) concluded from an evaluation of why CSA campaigns fail to change users' behavior that this is generally because existing cybersecurity interventions are not addressing the challenge of changing users' behavior. Cybersecurity intervention initiatives are primarily knowledge-based (Bada *et al.* 2019). CSA campaigns equip users with cybersecurity information, however, the knowledge is not enough to change behavior. The authors of Bada *et al.* (2019) suggest that to achieve a positive change in users' cybersecurity behaviors, the behavior change problem should be addressed (Bada *et al.* 2019).

2.1. User cybersecurity behavior

A user's cybersecurity behavior includes actions for maintaining or compromising cybersecurity. Based on Stanton *et al.* (2005), user cybersecurity behavior is shaped by a user's intentions, knowledge and environment (Stanton *et al.* 2005).

User intentions, in the current context, refer to a user's purpose for performing the cybersecurity behavior. A user's intentions can lie on a scale between benevolent and malicious. Additionally, a user's environment provides external influence to a user's intentions. For instance, environments that are inductive to performing cybersecurity behaviors encourage users to do so (Stanton *et al.* 2005).

Certain users have the knowledge and skills necessary to perform cybersecurity behaviors that enhance the protection of Internet resources. These users understand the need to maintain cybersecurity. Users may also use the Internet to carry out malicious intent, such as destroying systems or stealing money from individuals, organizations, or governments (Hadlington, 2017; Liggett, 2020; Sabillon *et al.* 2016; Weber *et al.* 2020). An average Internet user can also cause harm unknowingly through unintentional insecure behaviors. A common example of such behavior is the sharing of private information with strangers. Oversharing on the Internet can have devastating consequences (Gratian *et al.* 2018).

While some users may not be aware of the risks associated with online behavior, there exist users that are aware and continue to engage in risky activities despite knowing the consequences. (Bada *et al.* 2019; Herbert *et al.* 2020). Users' motivations for their behavior are not completely understood (Bada *et al.* 2019; Shah and Agarwal, 2020; Van Bavel *et al.* 2020; Wshah *et al.* 2020). Without understanding the influences of user cybersecurity behavior, it is a challenge for cybersecurity professionals to design intervention initiatives.

2.2. Cybersecurity behavior environment and cybersecurity behavior categories

Before identifying cybersecurity behavior constructs, it is imperative to define the cybersecurity behavior being affected by the construct. Cybersecurity behaviors can be divided into two categories, specifically Work behavior and Home behavior. Work and Home are examples of cybersecurity behavior environments. Cybersecurity behavior is influenced by the environment. For instance, it is possible for a user to be targeted more effectively by social engineering attacks when they are at home rather than at work.

In this section, we examine cybersecurity behavior in the work and home environment. Since cybersecurity behaviors are numerous, categorizing the cybersecurity behaviors is an effective way of conducting research on cybersecurity behaviors. Users' cybersecurity behaviors are further classified into behavior categories within the environments (Guo, 2013; Mashiane and Kritzinger, 2019; Stanton *et al.* 2005). By categorizing behaviors, a researcher can focus on a smaller scope of behaviors and group similar behavior together.

2.3. Cybersecurity behavior at work

A user’s cybersecurity behavior is governed by policies, regulations, and cybersecurity controls in the work environment (Beautement *et al.* 2008). Information technology departments or security experts can assist users with adhering to the policy by reminding users to update software, sending out information about new cyber threats, sharing information security best practices, and blocking undesirable applications or websites. In the work environment, users are held accountable for misconduct or not adhering to the organizational policy (Kritzinger and von Solms, 2010; Safa *et al.* 2016).

2.3.1. Cybersecurity behavior categories at work

Six categories of cybersecurity behavior in the work environment were identified by Stanton *et al.* (2005) (Figure 1). The categorization was developed by interviewing 110 stakeholders. During the interview, participants listed good and bad user cyber security behaviors. The behaviors were then assigned categories by ten domain experts. Grouping the behaviors was based on the level of expertise required to perform a behavior, and the intentions to support the organization. The six categories being: Intentional Destruction, Dangerous Tinkering, Aware Assurance, Detrimental Misuse, Naïve Mistakes, and Basic Hygiene (Stanton *et al.* 2005). A two-dimensional plane was used as the visualization tool for the cybersecurity behavior categories. The x-axis plots the intention of the user, which ranges from malicious to benevolent. The y-axis plots the user expertise, which ranges from novice and expert users (Stanton *et al.* 2005). Mashiane and Kritzinger (2019) added Security Compliance as a category that encompassed cybersecurity behaviors performed to comply with organizational security policies (Mashiane and Kritzinger, 2019). Additionally, Mashiane and Kritzinger (2019) divided the y-axis of the graph into four sections labeled: Intentional Malicious, Unintentional Malicious, Unintentional Benevolent and Intentional Benevolent. Mashiane and Kritzinger (2019) introduced this change to make the graph easier to interpret in terms of the intentions of users in terms of cybersecurity behavior (Mashiane and Kritzinger, 2019). Figure 1 illustrates the cybersecurity behaviors of users in the work environment.

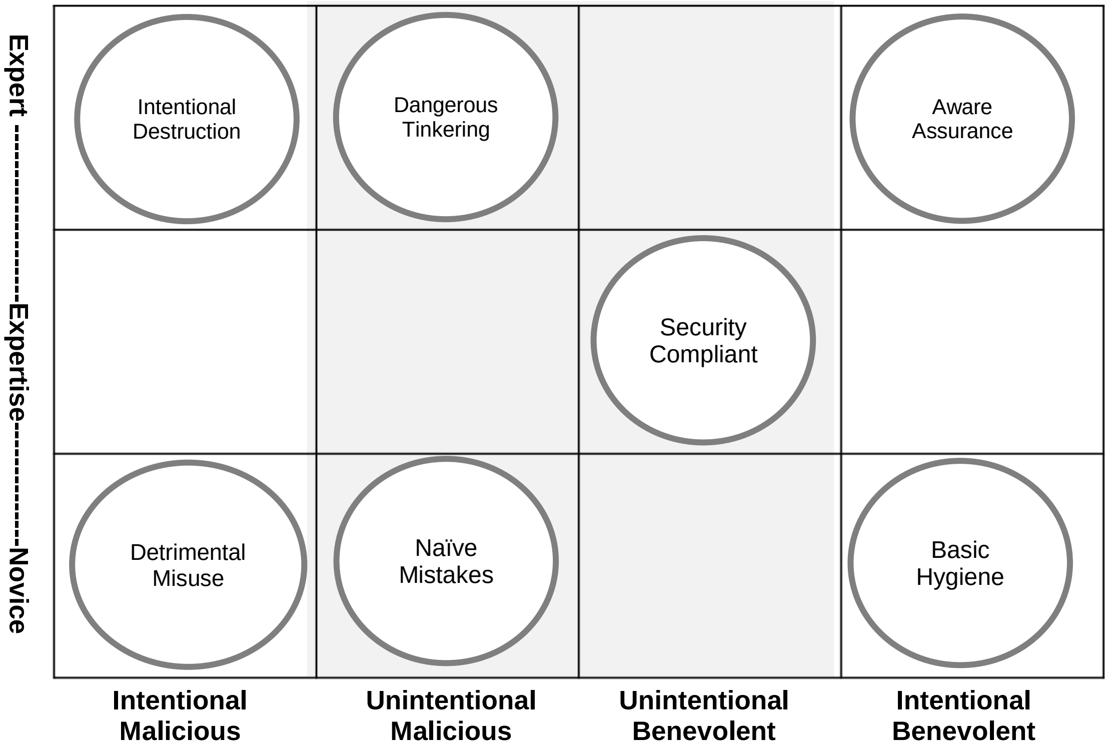


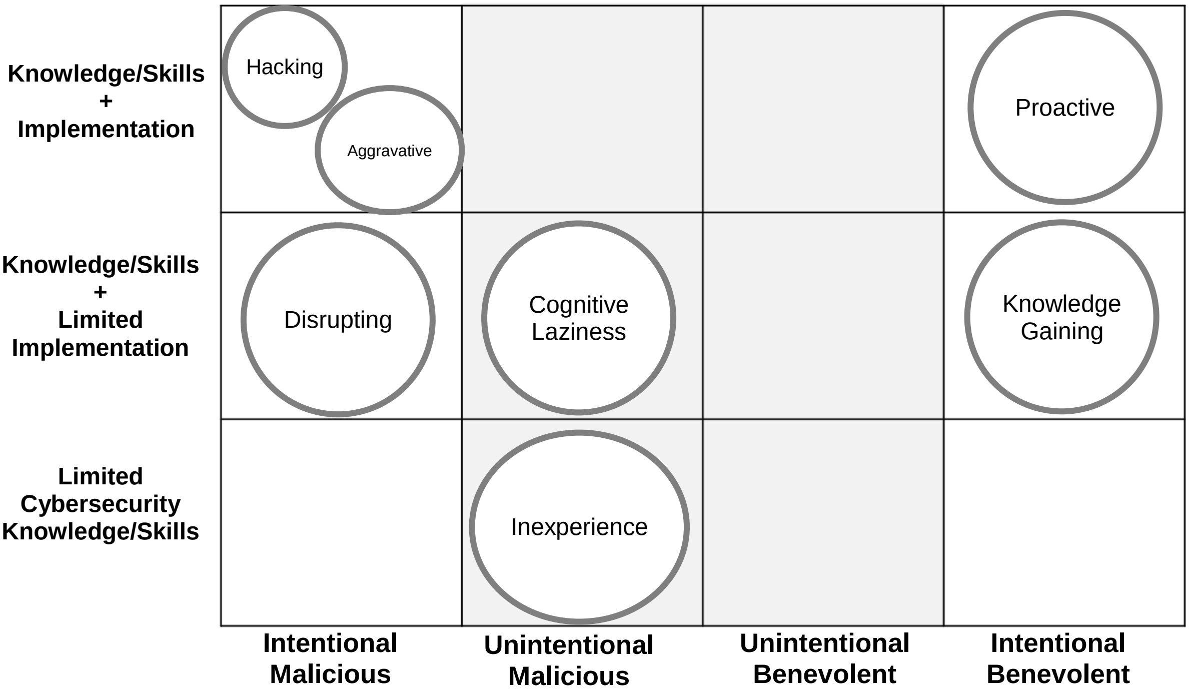
Figure 1. **User cybersecurity in the work environment**
Source: Mashiane and Kritzinger (2019)

2.3.2. Cybersecurity behavior at home

Home users use computers or mobile devices that are connected to the Internet at home as well as individuals of all ages. Users are responsible for ensuring that cybersecurity controls are implemented at home. Cybersecurity controls include both technical measures such as firewall installation and user-centered measures such as creating strong passwords. It is also the choice of the home user to enforce cybersecurity laws. Whether stringent cybersecurity controls are implemented or not is up to the user. Users are in control of their home environment.

Presented in this section are user cybersecurity behaviors in the home environment. Mashiane and Kritzinger (2019) conducted an exercise to extract the behavior of users in the cybersecurity context from literature (Mashiane and Kritzinger, 2019). The x-axis of Figure 2 is labeled with the intention labels shown in Figure 1. The y-axis has been updated to reflect home user cybersecurity behavior. Rather than having knowledge or skills of cybersecurity, demonstrating knowledge application in the home environment is a more appropriate means of measuring user knowledge (Anderson and Agarwal, 2010; Mashiane and Kritzinger, 2019; Ruiz *et al.* 2017; Simonet and Teufel, 2019; Talib *et al*. 2010). In order to include these labels on the y-axis, the following labels were added: None or Limited Knowledge and Skills, Knowledge and Skills with No Application, and Knowledge and Skills with Application.

Figure 2 shows an analysis of behavior categories. Eight categories are depicted on the graph. Hacking, Aggravative, Disrupting, Unconcerned, Inexperience, Cognitive Laziness, Convenience, Proactive, Aware and Knowledge Graining.



	Intentional Malicious	Unintentional Malicious	Unintentional Benevolent	Intentional Benevolent
Knowledge/Skills + Implementation	Hacking Aggravative			Proactive
Knowledge/Skills + Limited Implementation	Disrupting	Cognitive Laziness		Knowledge Gaining
Limited Cybersecurity Knowledge/Skills		Inexperience		

Figure 2. Home Users' Cybersecurity Behavior Categories
Source: Mashiane and Kritzinger (2019)

2.4. Behavioral constructs

While knowledge, intentions, and environment are useful to define user behavior, there exist additional behavioral factors or behavioral constructs that are associated with cybersecurity behaviors among users (Alqahtani and Kavakli-Thorne, 2020; de Kok *et al.* 2020; Hadlington, 2018). Behavioral constructs are defined according to psychology in this study. It can therefore be said that behavioral constructs are factors that are not directly observable or measurably accurate, but can be observed in the resulting behavior (Hadlington, 2021; Kelly, 2020). For instance, users' attitudes toward cybersecurity have been associated with their behavior. While attitude cannot be directly observed or measured, a user’s attitude towards cybersecurity has been shown to have an influence on a user’s performance of cybersecurity behaviors (de Kok *et al.* 2020).

Through the use of recent empirical studies that have evaluated the psychological influences on user behavior in cybersecurity, this study attempts to gain a new understanding of cybersecurity behavior. Having a common terminological framework is essential for combining the results of different studies. Through the Theoretical Domains Framework, a terminology like this is made possible.

2.5. Theoretical Domains Framework (TDF)

Behavior change is a key component of the Theoretical Domains Framework. Research done by Psychologists, health service researchers, and health psychologists led to the development of the framework, which brings together existing behavioral theories. As the use of the framework matured, so did its adoption in different disciplines (Atkins *et al.* 2017; Cane *et al.* 2012; Phillips *et al.* 2015; Wshah *et al.* 2020).

Theoretical Domains Framework was created to meet the challenge of selecting a theory in the development of behavior change interventions. Creating behavior change interventions became challenging due to the large number of behavioral theories available to healthcare professionals. There is a need for standardization in intervention design. For results to be comparable, behavior theories have to be selected and applied consistently. Furthermore, different intervention designs and inconsistent language used when describing intervention techniques made it difficult to trace successful interventions (Atkins *et al.* 2017; Cane *et al.* 2012; Phillips *et al.* 2015).

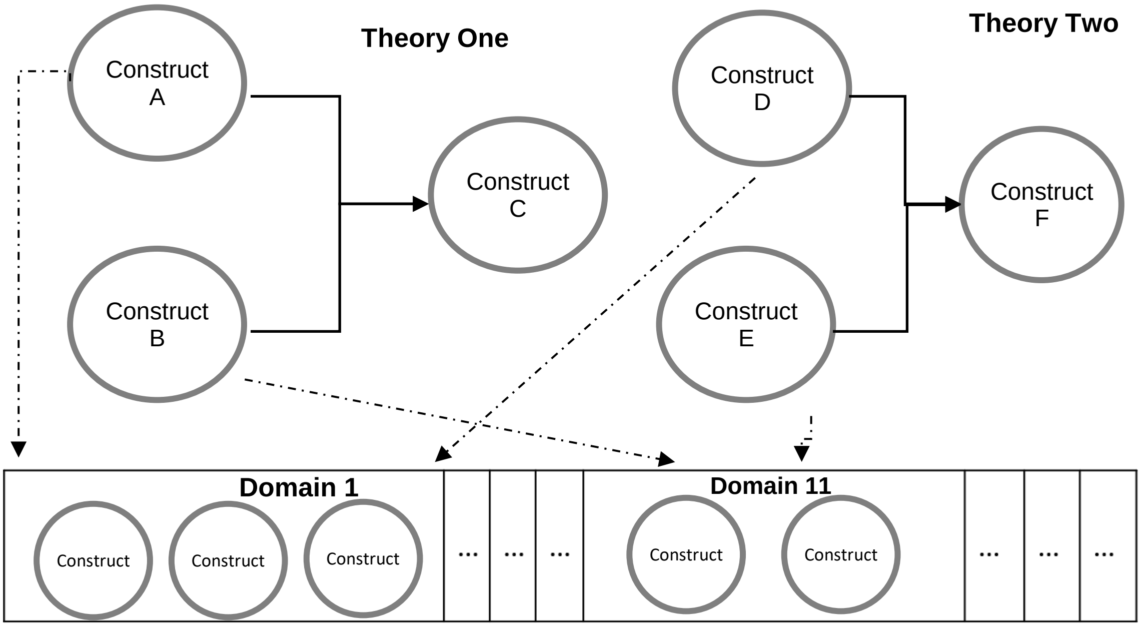


Figure 3. Illustration of the Concept of the TDF
Source: Cane *et al.* (2012)

Following a rigorous process, behavioral theories were identified, constructs were extracted, and finally domains were grouped. Figure 3 illustrates the idea of how theoretical domains are defined. In order to validate the identification of domains, backward validation was applied, in which pilot interview questions based on theoretical domains were sent out for evaluation.

A total of 112 constructs were contained in twelve domains of the resulting framework. Cane *et el.* (2012) refined the framework and produced the latest version which has fourteen domains, grouping eighty-four constructs. The domains in the latest version of the Theoretical Domains Framework are: Knowledge, Skills, Emotions, Memory and Attention and Decision Processes, Behavioral Regulation, Social Or Professional Role and Identity, Beliefs about Capabilities, Optimism, Beliefs about Consequences, Intentions, Goals, and Reinforcement (Cane *et al.* 2012).

3. Methodology

To achieve the study's objectives, a systematic literature review was conducted. According to Okoli and Schabram (2010), a Systematic Literature Review is a method that clearly identifies, evaluates, and synthesizes previously completed and recorded work produced by researchers, scholars, and practitioners (Okoli and Schabram, 2010). The systematic literature review is driven by a clear research question, which guides the collection of literature, the extraction of data, and ultimately the analysis of the data. A Systematic Literature Review results in new knowledge or a new perspective on existing knowledge (Boell and Cecez-Kecmanovic, 2015; Ghosh and Guchhait, 2020; Kuppusamy *et al.* 2020; Xiao and Watson, 2019).

The Systematic Literature Review is held to the same standards as other scientific methodologies. The results of a Systematic Literature Review must be repeatable, reliable, and valid. The Systematic Literature Review is conducted according to steps outlined by the researcher.

Several guidelines are available on how to conduct a Systematic Literature Review. A quality literature review follows a four-phase process, including planning, literature selection, data extraction, and writing the review (Alexander, 2020; Boell and Cecez-Kecmanovic, 2015; Keele, 2007; Okoli, 2015; Okoli and Schabram, 2010; Xiao and Watson, 2019). Okoli and Schabram’s (2010) guidelines were created for the research on information systems, so the research follows those guidelines.

Numerous studies have examined cybersecurity behavior change from the perspective of different psychological theories. To date, no study has separated the theories into their constructs and compared the results collectively. It was found appropriate to perform a Systematic Literature Review to compare cybersecurity behavior and behavior constructs. Systematic Literature Reviews are conducted in order to identify cybersecurity behavioral constructs. To identify cybersecurity behavioral constructs, the protocol followed in the study is detailed in the remaining sections of the methodology.

The search terms "cyber", "security", "psychology", "behavior", "theory" and "cybersecurity" were initially entered into Google Scholar. We scanned the abstracts of the publications that mentioned a behavioral theory. We documented these theories in preparation for the next phase of our search. Then, we searched Google Scholar and Research Gate using the list of behavior theories presented in Step 1 and the terms "cybersecurity" or "cyber security". A date filter was applied to Google Scholar so that searches only returned publications from 1999 up to 2019.

According to the practical screening criteria, participants must meet the following requirements: There is an English version of the publication, and the publication was published between 1999 and 2019.

For quality appraisal, the following inclusion criteria were used: An empirical study, the study uses a questionnaire/survey for data collection. A hypothesis test is conducted in this study.One of the null hypotheses has to quantify the relationship between the construct and the construct's "intention to behave" or its actual behavior. Study-validated constructs or previously validated constructs were used in the study. Equal weight was given to each of the inclusion criteria. Articles had to comply with all the criteria in order to be considered.

During the study, data was extracted as follows: For each study, extract following demographic data was collected: Author Name, Article Title, Year of publication, Study Design, Context of Study (Home or Work), Psychology Theories, Cybersecurity Behavior, Sample Size, and Gender of participants. By taking into account psychology theories and author-defined theories, we extract constructs used in selected studies. The extracted data is documented on a spreadsheet using Microsoft Excel, 2016, 32-bit software.

The refined Theoretical Domains Framework (Cane *et al.* 2012; Cane *et al.* 2015) was used for the study. The constructs of the Theoretical Domains Framework were placed on the spreadsheet. Definitions for each construct were extracted from previous literature by looking at both the provided definition as well as the associated question in the provided questionnaires (Cane *et al.* 2012; Cane *et al.* 2015). Finally, each construct taken from the qualifying literature was mapped onto the Theoretical Domains Framework based on the definition of that construct provided by the author. The write-up of the Systematic Literature Review is presented in this study.

4. Relationship between cybersecurity behavior categories and behavior constructs

This section presents the results of the Systematic Literature Review. The behavior constructs found in the literature have been mapped to the Theoretical Domains Framework. This section presents the relationship between cybersecurity behavior categories (presented in Section 3) and the behavior constructs.

In Figure 4, you will find the key to interpreting the next set of diagrams. An arrow with a solid line indicates a positive relationship between constructs, in other words construct A is positively correlated with construct B. Negative relationships are represented by dotted lines, thus Construct A has a negative/reduced relationship with Construct B. The colour of the line indicates whether or not the relationship has been found to be significant in a study. Statistically significant relationships are indicated by green lines, while relationships that are not significant are indicated by red lines.

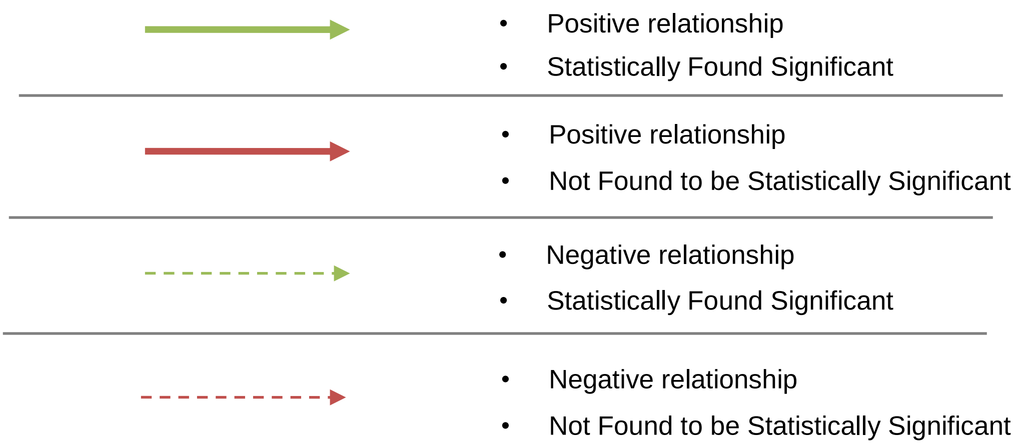

• Positive relationship
• Statistically Found Significant
• Positive relationship
• Not Found to be Statistically Significant
• Negative relationship
• Statistically Found Significant
• Negative relationship
• Not Found to be Statistically Significant

Figure 4. Relationship Key

4.1. Cybersecurity behavior categories and constructs: work environment

This section outlines the results of our study regarding cybersecurity behavior in the work environment.

4.1.1. Intentional malicious behavior

This section presents the constructs and the cybersecurity behaviors under intentional malicious behavior.

4.1.1.1. Detrimental misuse and theoretical domains framework behavior constructs

Choi *et al.* (2013) was the only one that focused on Detrimental Misuse behavior (Choi *et al.* 2013). Detrimental Misuse is evaluated through Skills Development, Self-Efficacy, Organizational Culture/Climate, Skills, Stability of Intentions, Knowledge, and Action Planning (Figure 5).

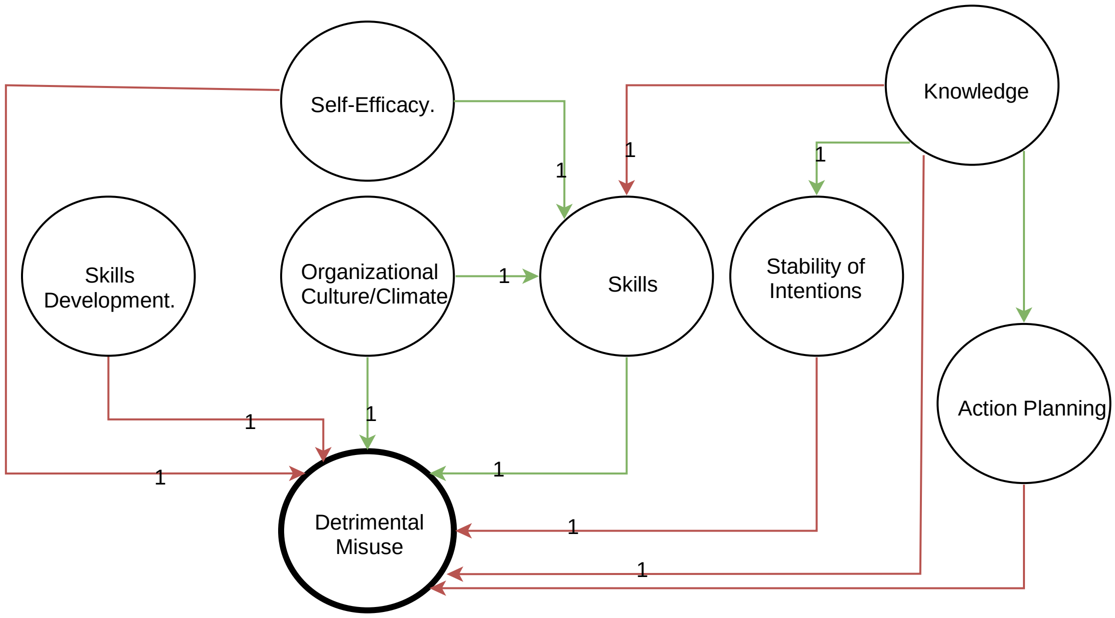


Figure 5. Detrimental misuse and behavior constructs

The constructs Organizational Culture/Climate and Skills were found to be statistically significant in reducing Detrimental Misuse. The study by Choi *et al.* (2013), is aligned with the finding of other researchers (Bada *et al.* 2019), which is, a cybersecurity culture positively impacts user cybersecurity behavior.

Based on Self-Efficacy, Skills Development, Stability of Intentions, Knowledge, and Action Planning, it was not statistically significant that Detrimental Misuse had reduced.

4.1.2. Unintentional malicious behavior

This section presents the constructs and the cybersecurity behaviors under the unintentional malicious behavior.

4.1.2.1. Dangerous tinkering and theoretical domains framework behavior constructs

Ifinedo (2017) is the only study that looked at Dangerous Tinkering. The evaluated constructs are Perceived Behavioral Control and Knowledge of Condition/Scientific Rational. There was statistical significance between Perceived Behavioral Control and Dangerous Tinkering, particularly low Perceived Behavioral Control (Figure 6).

Statistically significant reductions in Dangerous Tinkering were found when Factor and Condition were taken into account, however Knowledge of Condition and Scientific Rationale was not found to be significant reductions in Dangerous Tinkering**.**

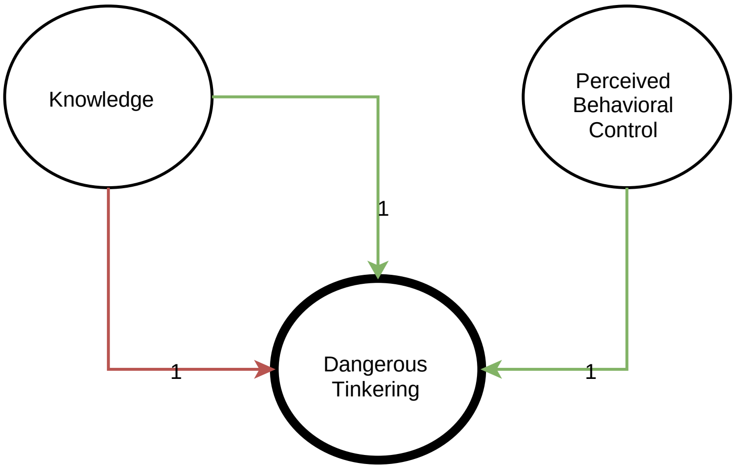


Figure 6. Dangerous tinkering behavior and behavior constructs

4.1.2.2. Naïve mistakes and theoretical domains framework behavior constructs

A comparison of two studies examined Naïve Mistakes (Cashin and Ifinedo, 2014; Ifinedo, 2014). Outcome Expectancies, Modeling, Self-Monitoring, Stages of Change Model, Self-Efficacy, and Leadership (Figure 7) were the constructs evaluated.

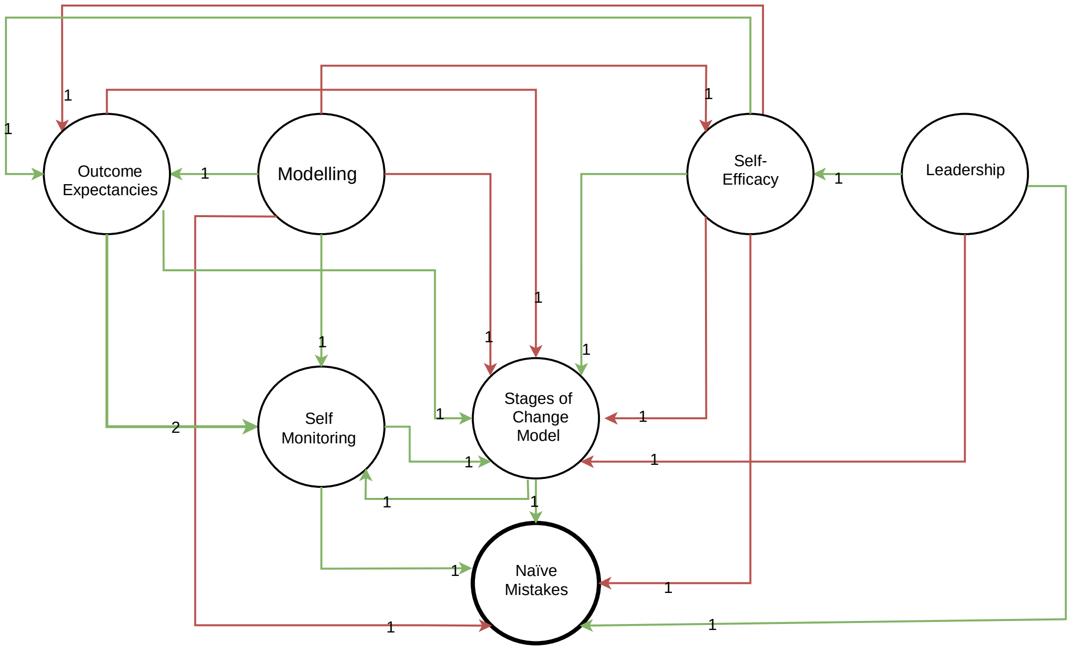


Figure 7. Naïve mistakes and behavior constructs

Statistically significant reductions of Information Security Careless behavior were found to be linked to Leadership and Self-monitoring. Leadership is defined as the management and executive structure of the company supporting benevolent cybersecurity practices. Self-Monitoring means that employees or users have the responsibility of monitoring themselves while performing cybersecurity related behaviors.

It is noteworthy that Outcome Expectancies were found to be a significant contributor to increasing self-monitoring in this context. Outcome Expectancies, in this context, refer to whether the user expects there to be a worthwhile outcome of performing the cybersecurity behavior. Hence, if users believe what they are doing is worthwhile, there is a greater likelihood of them self-monitoring, which in turn will lead to fewer naive mistakes in the work environment.

4.1.3. Unintentional benevolent behavior

This section presents the constructs and cybersecurity behaviors under unintentional benevolent behavior.

4.1.3.1. Security compliant behavior

Nine studies focused on Security Compliant Behavior (Herath and Rao, 2009; Ifinedo, 2014; Johnston and Warkentin, 2010; Koohang *et al.* 2019; Li *et al.* 2014; Ofori *et al.* 2020; Siponen *et al.* 2014; Siponen *et al.* 2007; Vance *et al.* 2012). The evaluated constructs are Leadership, Procedural Knowledge, Knowledge Probability\Vulnerability of the Threat, Self-efficacy, Beliefs (under Beliefs about Capabilities), Consequents (under Beliefs about Consequences), Breaking Habit, Rewards, Outcome Expectancies, Social Norm, Consequents (under Reinforcement), Stages of Change Model, Cues to Action, Organizational Culture/Climate, Positive/Negative Affect, Susceptibility of the Threat, Subjective Norm, Sanctions, Barriers and Facilitators, Incentives, Group Identity, Punishment, and Certainty of Detection (Figure 8).

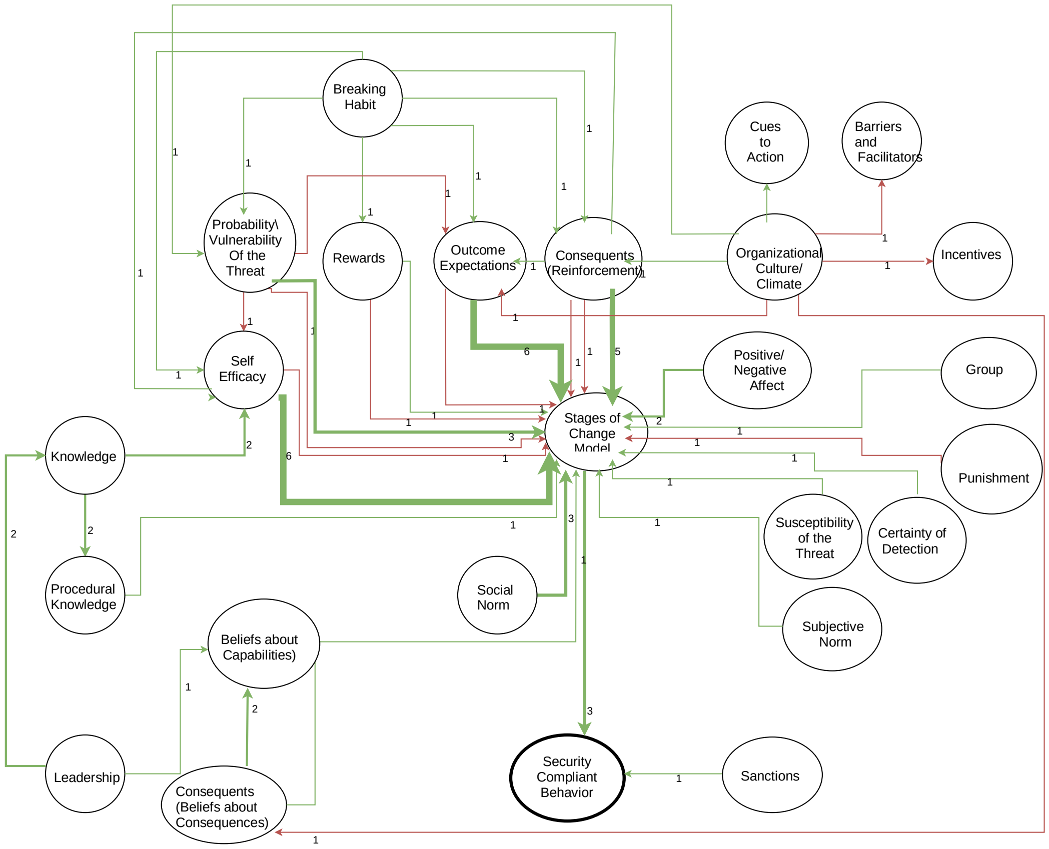

Breaking Habit
Cues to Action
Barriers and Facilitators
Probability\ Vulnerability Of the Threat
Rewards
Outcome Expectations
Consequents (Reinforcement)
Organizational Culture/ Climate
Incentives
Self Efficacy
Positive/ Negative Affect
Group
Knowledge
Stages of Change Model
Punishment
Susceptibility of the Threat
Certainty of Detection
Procedural Knowledge
Social Norm
Subjective Norm
Beliefs about Capabilities)
Leadership
Consequents (Beliefs about Consequences)
Security Compliant Behavior
Sanctions

Figure 8. Security compliant behavior and behaviour constructs

The constructs Self-efficacy, Outcome Expectancies, Consequences (under Reinforcement) and Social Norms had more than two studies that statically prove the relationship with Stages of Change Model. In this context, the Stages of Change construct refers to the intention of a user to perform Security Compliant Behavior. Ajzen (2011) stated that intentions to perform a behavior are secondary to the actual behavior. According to Ajzen (2011), users should have a strong intention (Stages of Change Model) to perform a behavior, there is a benevolent chance that the user will perform the behavior (Ajzen, 2011).

4.1.4. Intentional benevolent behavior

This section presents the constructs and the cybersecurity behaviors under the intentional benevolent behavior.

4.1.4.1. Basic hygiene and behavior constructs

Two studies focused on Basic Hygiene behavior (Addae *et al.* 2019; Hong and Furnell, 2019). The evaluated constructs are Characteristics of Outcome Expectancies, Resources/Material Resources, Anxiety, Beliefs (Beliefs about Consequences), Positive/Negative Affect, Competence, Probability\Vulnerability of the Threat, Self-efficacy, Identity (Optimism), Stages of Change Model, Reinforcement, Organizational Commitment, Social Support, Social Pressure, Group Identity, Perceived Behavior Control, Beliefs (Beliefs about Capabilities), and Ability (Figure 9).

Beliefs (Beliefs about Capabilities), Social Support and Stages of Change Model were not found to be significant in increasing cybersecurity Basic Hygiene behavior. Beliefs (Beliefs about Capabilities) are the user's belief of the usefulness of performing the cybersecurity Basic Hygiene behavior. Social Support refers to the reassurance that there will be sufficient support and assistance should it be required when performing the behavior.

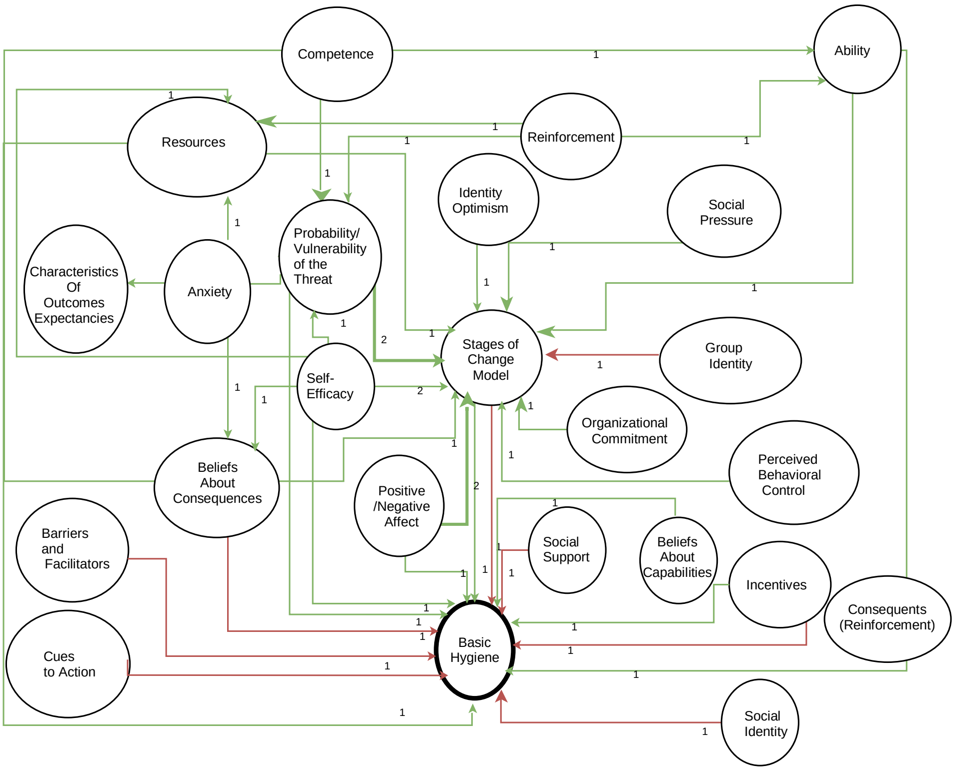

Competence
Ability
Resources
Reinforcement
Identity Optimism
Social Pressure
Probability/ Vulnerability of the Threat
Characteristics Of Outcomes Expectancies
Anxiety
Stages of Change Model
Group Identity
Self-Efficacy
Organizational Commitment
Perceived Behavioral Control
Beliefs About Consequences
Positive /Negative Affect
Barriers and Facilitators
Social Support
Beliefs About Capabilities
Incentives
Consequents (Reinforcement)
Cues to Action
Basic Hygiene
Social Identity

Figure 9. Basic hygiene and behavior constructs

4.1.4.2. Aware Assurance and Behavior Constructs

Two studies focused on Aware Assurance (Flores *et al.* 2014; Safa *et al.* 2015). The evaluated constructs are Skills Development, Group Conformity, Beliefs (under about Capabilities), Barriers and facilitators, Knowledge, Positive/Negative Affect, Self-efficacy, Perceived Behavior Control, Cues to Action, Social Support, Reinforcement, Social Pressure, Organizational Culture/Climate, Social Identity, Identity (under Optimism) Group Identity, Stages of Change Model, and Organizational Commitment.

A negative relationship was hypothesized between of Stages of Change construct and Detrimental Misuse. The relationship was found to be statistically significant (Figure 10). Knowledge of Condition/Scientific Rationale is the only construct that was found to be statistically significant to increase detrimental misuse. Skills Development was hypothesized to reduce detrimental misuse behavior. This relationship was not found to be statistically significant. Self-efficacy was hypothesized to reduce detrimental misuse behavior. This relationship was not found to be statistically significant. Self-efficacy was also hypothesized to increase Skills. Knowledge was evaluated to have a positive relationship with Stages of Change Model, Stability of Intentions and Skills. The relationship between Skills and Knowledge was not found to be statistically significant, the relationship between Stages of Change Model and Stability of Intentions was found to be statistically significant.

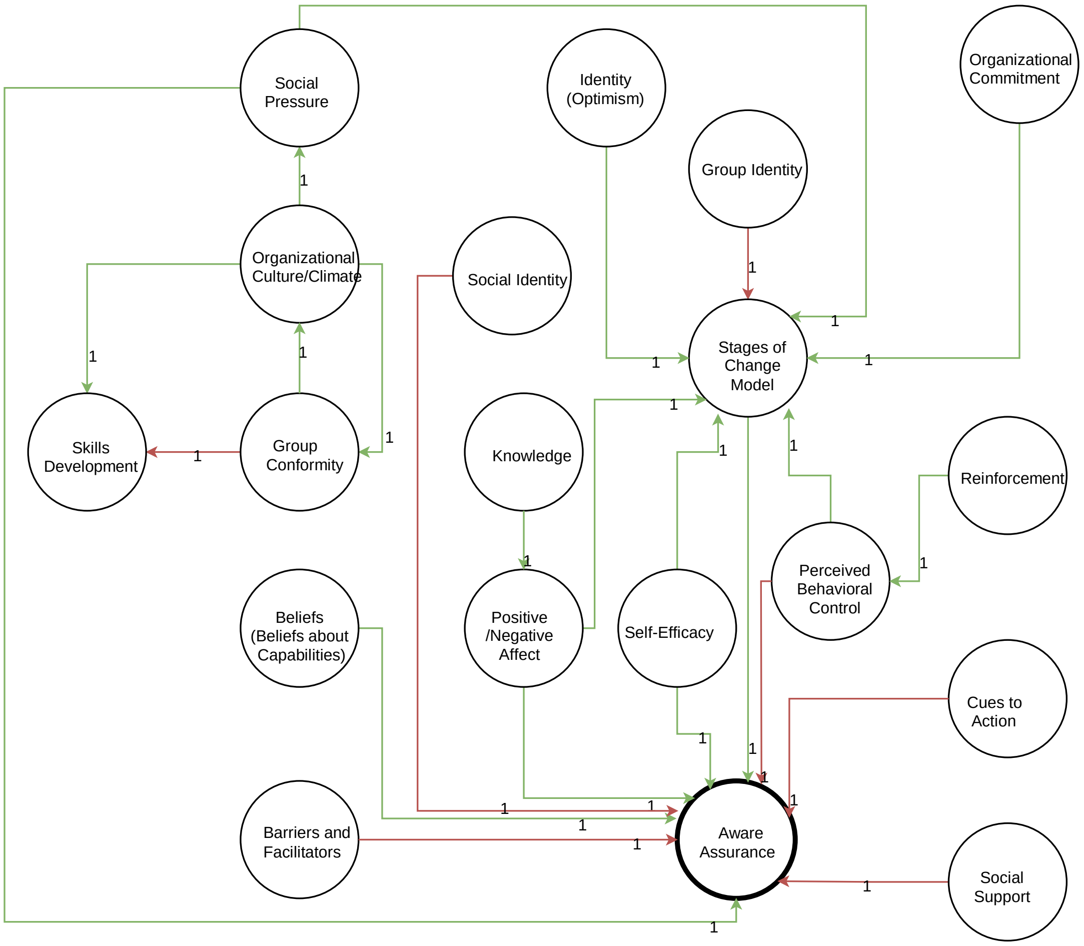


Figure 10. Aware Assurance and Behavior Constructs

4.2. Cybersecurity behavior categories and constructs: home environment

This section presents the results of the results for cybersecurity behavior in the home environment.

4.2.1. Intentional malicious behavior

This section presents the constructs and cybersecurity behaviors under intentional malicious behavior.

4.2.1.1. Disrupting Behavior and Behavior Constructs

Only one study focused on Disrupting Behavior (Xiao and Wong, 2013). The evaluated constructs were Cues to Action, Knowledge of the Environment and Social Norms. All evaluated constructs were found to be statically significant in contributing towards Disrupting Behavior (Depicted in **Error! Reference source not found.**1).

Cues to Action is a construct that has been added to the Theoretical Domains Framework for this study. Cues to Action refers to triggers that motivate users into performing an action. In this context, Xiao and Wong (2013) used the example of 'the craving for attention' as a cue to action.

Knowledge of the environment refers to the knowledge of the circumstances in which to perform Disrupting Behavior. Therefore, the results imply that users that perform Disrupting behavior perceive the Internet environment as a suitable place to carry out Disrupting Behavior.

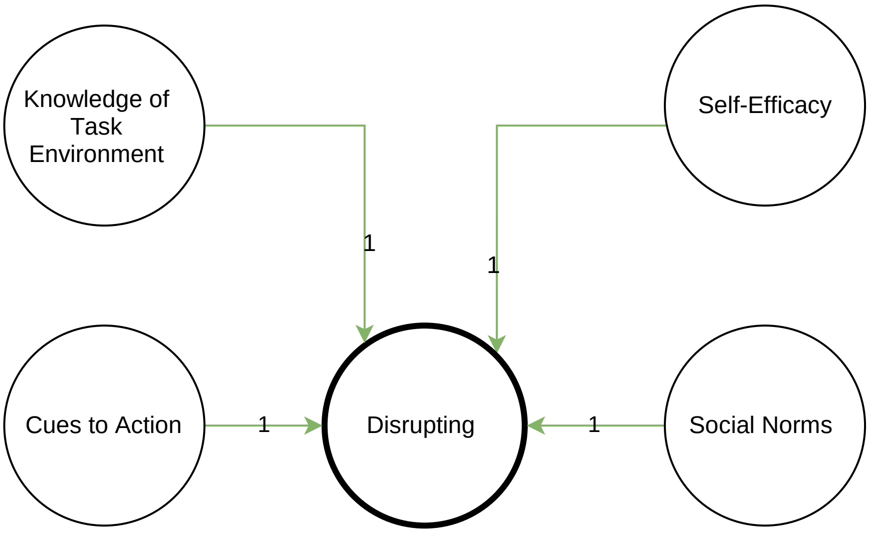


Figure 11. Disrupting and Behavior Constructs

4.2.2. Unintentional Malicious Behavior

This section presents the constructs and cybersecurity behaviors under unintentional malicious behavior.

4.2.2.1. Cognitive laziness and behavior constructs

Two studies focused on Cognitive Laziness (Milne *et al.* 2009; Verkijika, 2018). The evaluated constructs are Consequents (under Reinforcement), Self-efficacy, Knowledge, Skills, Cues to

Action, Fear, Anticipated Regret, Susceptibility to the Threat and Outcome Expectancies (Figure 12).

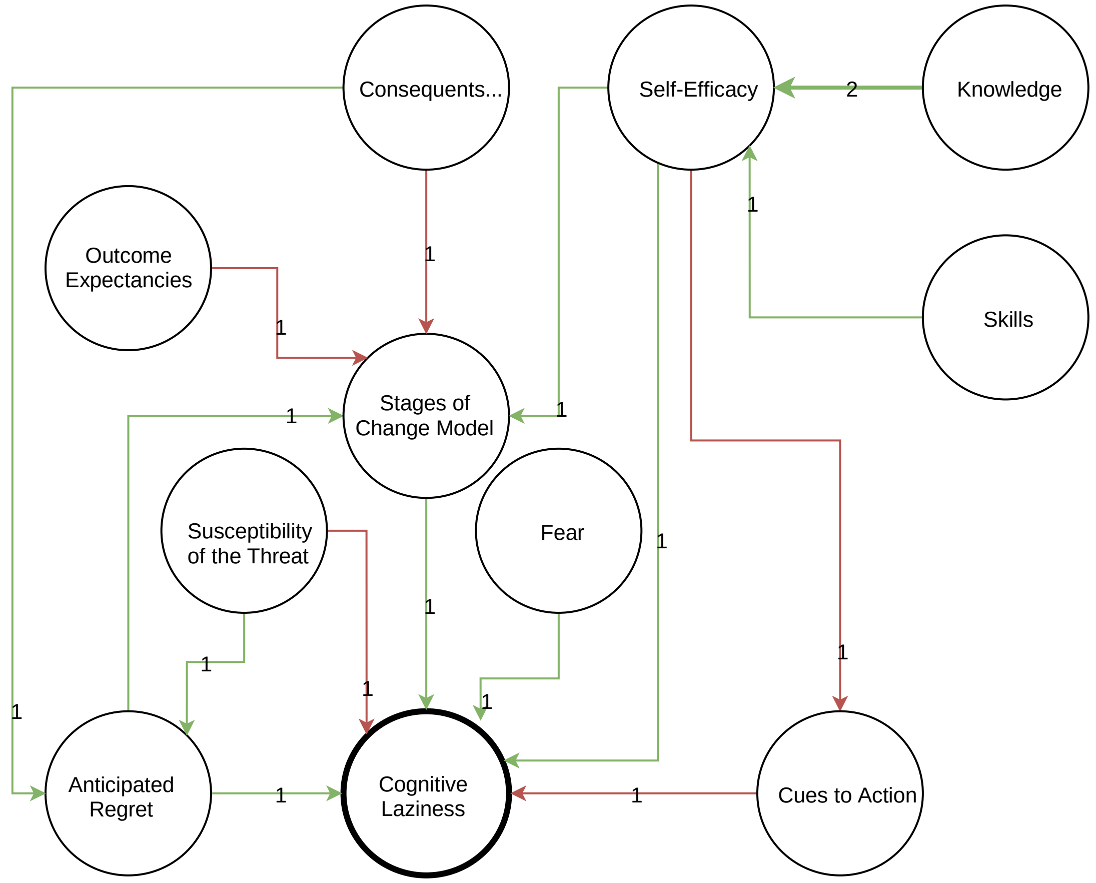


Figure 12. Cognitive Laziness and Behavior Constructs

4.2.2.2. Inexperience and behavior constructs

Two studies focused on cybersecurity behavior associated with Inexperience (Vishwanath *et al.* 2018). The evaluated constructs are Probability\Vulnerability of the Threat, Attention Control, Consequences (under the Reinforcement domain), Decision Making, Perceived Behavioral Control, Breaking Habit, Fear and Self-efficacy (**Error! Reference source not found.**3).

Self-Efficacy, Decision Making, and Perceived Behavioral Control were found to be statically significant in reducing inexperienced behavior. Decision Making, in this context, refers to remembering and making the decision about cybersecurity.

Attention Control and Consequences (under the Reinforcement domain) were found to be statically significant in increasing inexperienced behavior. Attention Control in Vishwanath *et al.* (2018) particularly refers to deficient amount of Attention Control. Consequences (under the Reinforcement domain) refer to the cost of not performing a behavior. In this context, it refers to the costs of not performing cybersecurity behavior.

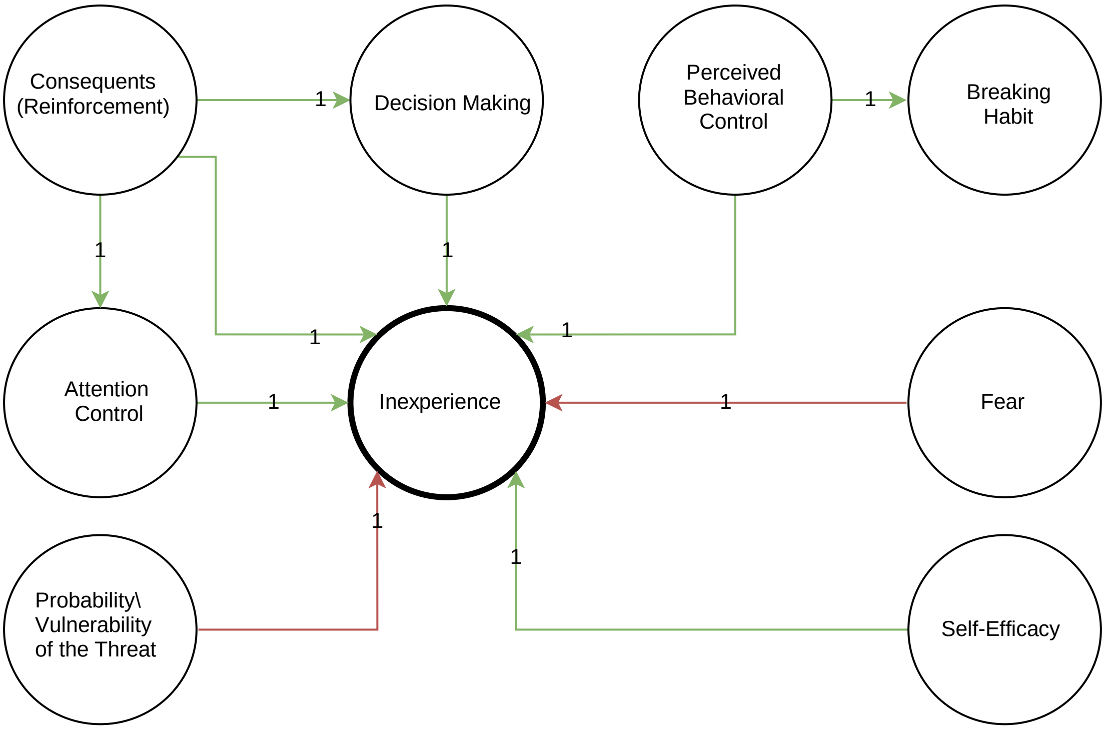

Consequents (Reinforcement)
Decision Making
Perceived Behavioral Control
Breaking Habit
Attention Control
Inexperience
Fear
Probability\ Vulnerability of the Threat
Self-Efficacy
1
1
1
1
1
1
1
1
1
1
1

Figure 13. Inexperience and behavior construct

4.2.3. Intentional benevolent behavior

This section presents the constructs and cybersecurity behaviors under intentional benevolent behavior.

4.2.3.1. Knowledge gaining and behavior constructs

One study focused on Knowledge Gaining Behavior (Hanus and Wu, 2016). The evaluated constructs are Consequents (under the Beliefs domain), Knowledge of the condition and Scientific Rational, Consequents (under the reinforcement domain), Probability/Vulnerability of the Threat, Outcome Expectations, Skills, Self-efficacy and Consequents (under the Beliefs domain) (Figure 14).

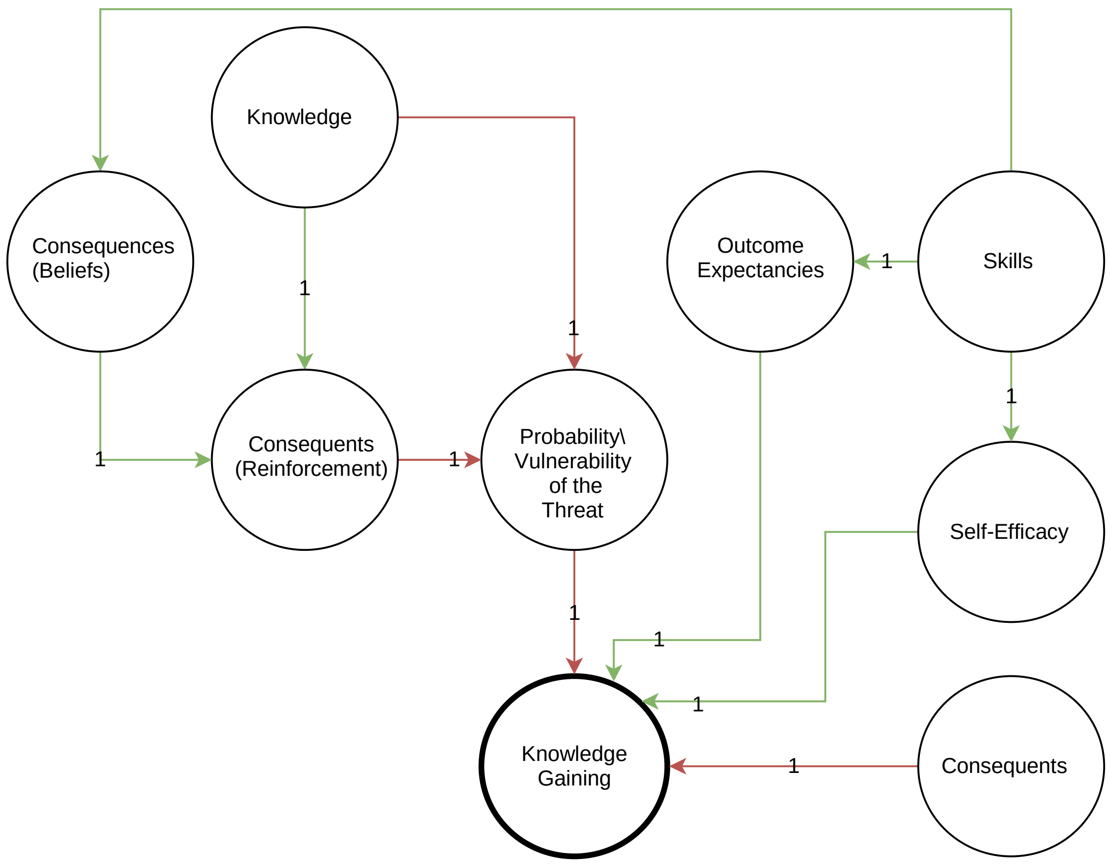


Figure 14. Knowledge gaining and behavior constructs

4.2.3.2. Proactive and behavior constructs

Eight studies focused on Proactive cybersecurity behavior (Anderson and Agarwal, 2010; Arachchilage and Love, 2014; Burns and Roberts, 2013; Chai *et al*. 2006; Chenoweth *et al.* 2009; Jansen and van Schaik, 2019; Milne *et al.* 2009; Tsai *et al.* 2016). The evaluated constructs are Goal Priority, Positive/Negative Affects, Knowledge, Knowledge of Condition/Scientific Rationale, Anxiety, Self-efficacy, Susceptibility of the Threat, Fear, Identity, Cues to Action Knowledge of Task Environment Perceived Competence, Consequents (under beliefs) Probability/Vulnerability of Threat, Braking Habit, Stages of Change Model, Pessimism, Beliefs, Knowledge of Environment, Skills, Outcomes Expectations, Group Identity, Psychological Ownership, Consequents (under Reinforcement), Social Pressure, and Social Pressure (Figure 15).

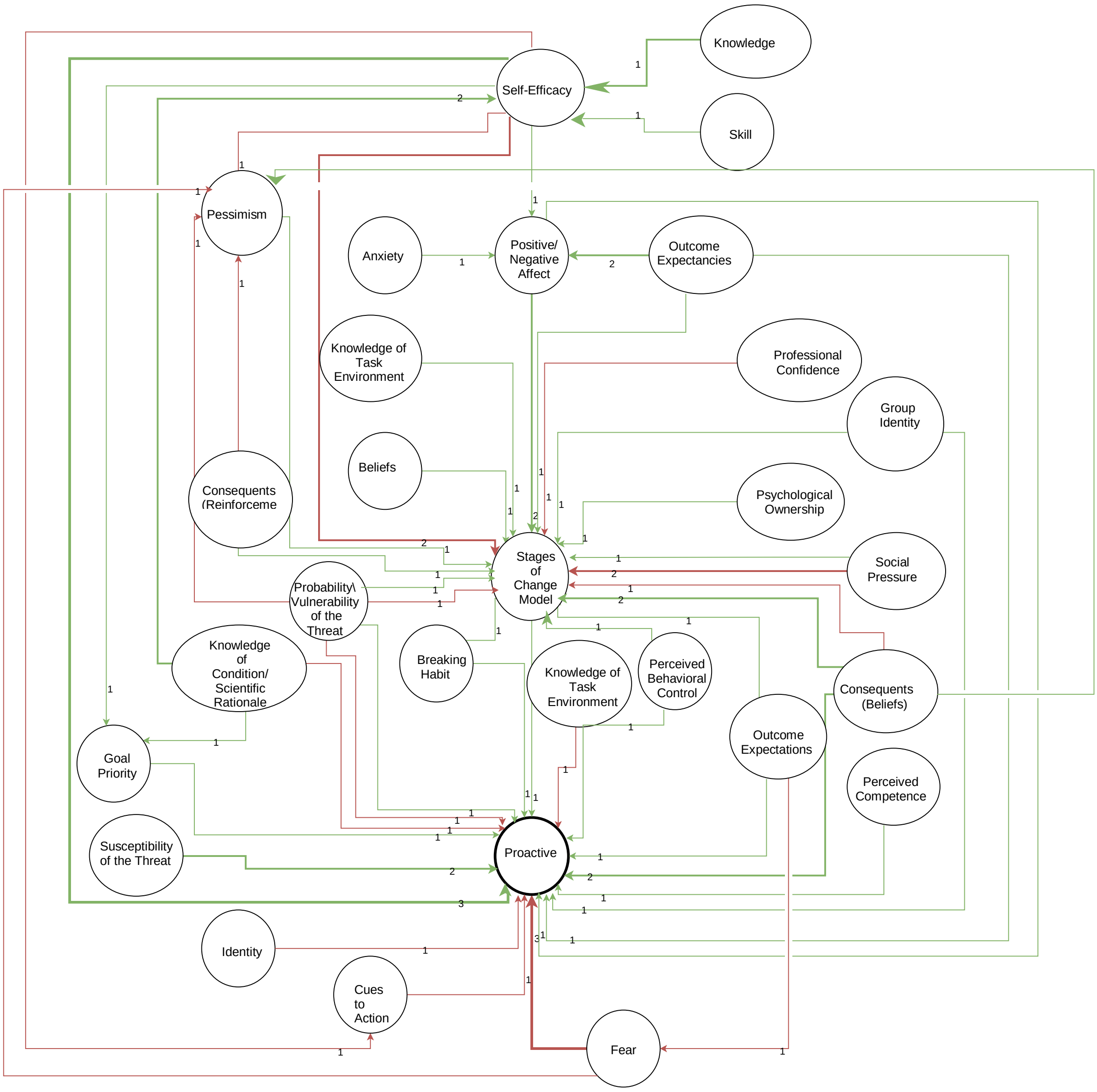


Figure 14. Proactive and behavior constructs

4.3. Discussion: Cybersecurity behavior categories and behavior constructs

This discussion will elaborate on the findings of Section 4.1 and Section 4.2.

4.3.1. The work environment

Cybersecurity has traditionally been seen as a knowledge gap issue (Bada *et al.* 2019). The focus of cybersecurity training is to increase awareness and knowledge in order to decrease malicious cybersecurity behavior (Corradini, 2020; Legárd, 2020; Simonet and Teufel, 2019). According to the results of the previous section (Section 4.1), technological-based measures such as training, discipline, self-monitoring, and leadership could enhance the ability of organizational culture and climate to decrease malicious cyber behavior. This study suggests that if users understand what cybersecurity includes, as well as the outcomes of cybersecurity related behavior, they are more likely to decrease malicious cybersecurity behavior in a work setting. Organizational leaders should foster a culture that discourages malicious cybersecurity behavior.

The constructs that were found to promote benevolent cybersecurity behaviors within an organization were Self-efficacy, Outcome Expectations, Consequences (under Reinforcement), Probability/Vulnerability of Threats, Social Norm, Organizational Culture, Social Pressure, Positive/Negative Affect, and Organizational Commitment. As part of the work environment, the institution has direct control over its culture and commitment and is able to put in place interventions that promote active cyber security behavior.

4.3.2. The home environment

Among the constructs that discourage malicious cyber behavior at home are Self-Efficacy, Decision Making, and Perceived Behavioral Control. Malicious cybersecurity behavior is influenced by Knowledge of the environment, Self-efficacy, Social Norms, Cue-to-Action, Fear, and Anticipated Regret.

When creating cybersecurity behavior intervention initiatives, constructs such as Outcome Expectations, Self-efficacy, Susceptibility to the Threat, Goal, Priority Breaking Habit, and Perceived Behavioral Control can be included.

5. Practical implications of study

In the following section, we discuss the gaps in current research which this study addresses. A comprehensive overview of the results is presented by combining the results, giving a cybersecurity intervention designer a better understanding of the domain. The contribution is presented in the form of a Model of Cybersecurity Behavior Constructs (MCSBC).

Given that the initiative designer is responsible for designing a cybersecurity behavior program for employees that is intended to raise the employee compliance levels with the organization's data security policy, they will select the Security Compliant Behavior category. Figure 16 presenting the results of the research focused on behavior constructs and cybersecurity compliance behavior will open (Depicted in Figure 8). From Figure 8, it is easy to identify that Self-efficacy, Outcome Expectations and Consequents (Reinforcement) are the top constructs which have been found to have a positive significant relationship with the Stages of Change Model (According to the Stages of Change Model, users' intentions are measured at five stages: preparation, contemplation, action, and maintenance. In the context of cybersecurity, the Stages of Change Model reflects how a user intends to behave regarding cybersecurity.). The designer can investigate how to incorporate components in the program that are aimed at 1) increasing employees' Self-efficacy, 2) communicating clearly the Outcome Expectations of complying and not complying to the information security policy and finally 3) the designer should highlight the consequences of not complying to the information security policy i.e. Consequents (Reinforcement).

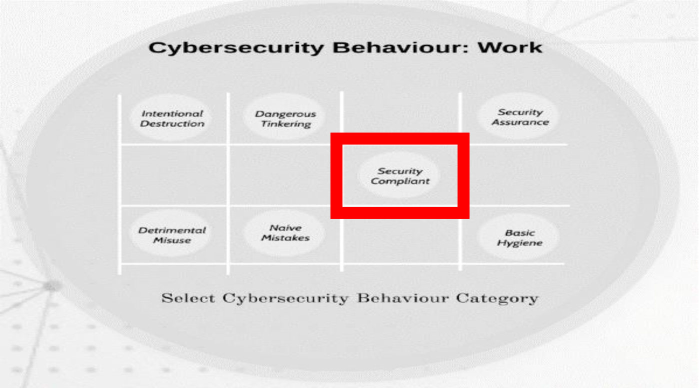


Figure 15. Cybersecurity behavior taxonomy: work

The above example scenario gives an example of how the designers of cybersecurity behavior change initiatives can utilize the knowledge gained from studies in the field to their advantage. Previously, the designer would have to conduct a preliminary study to determine how to best influence employees. Model of Cybersecurity Behavior Constructs provides the designer with a convenient manner of accessing the consolidated information.

6. Conclusion

Systematic Literature Review was presented in the study. First, the study presents literature reviews focused on user cybersecurity behavior. An overview of user cybersecurity behavior in the home and workplace is presented. Each of the environments is accompanied by cybersecurity behavior categories.

The study presented the methodology used to conduct the study. We extracted cybersecurity behavior constructs from the selected literature and mapped them onto the Theoretical Domains Framework during this exercise. As a means of synthesizing the constructs found in the literature, we used Theoretical Domains Framework. An analysis of the relationship between the behavior constructs and each cybersecurity behavior category was presented in the final section.

This study aims to identify the relationship between user cybersecurity behavior categories and user cybersecurity behavior constructs. Study results suggest that in the process of developing a cybersecurity behavior initiative, constructs such as organizational culture/climate, skills, self-monitoring, leadership, outcomes expectations, and knowledge should be considered. The constructs that were found to promote benevolent cybersecurity behaviors in an organization include Self-efficacy, Outcomes expectations, Consequents (under Reinforcement), Probability/Vulnerability of Threat, Social Norm, Organizational Culture, Social Pressure, Positive/Negative Affect and Organizational Commitment.

In the home environment, Self-efficacy, Decision Making, and Perceived Behavioral Control are constructs that discourage malicious cyber activity. The constructs that increase malicious cybersecurity behavior in the home environment include Knowledge of the environment, Self-efficacy, Social Norms, Cue-to-Action, Fear, and Anticipated Regret. When encouraging benevolent cyber behavior in the home environment, constructs like Outcome Expectations, Self-efficacy, Susceptibility to the Threat, Goals, Priority Breaking Habits, and Perceived Behavioral Control can be utilized.

The major contribution of this paper is to detect and explaining the risk eliminating effect that is inherent in inter-temporal transfer of worked hours in working time accounts. Based on a stochastic dominance model of probability mass shift, we were able to show that working time accounts establish a mutual insurance device between employers and employees. For employees, coverage by a working time accounts system provides both, insurance of disposable income and private unemployment insurance. For firms, such a system provides smoothing of labor cost. Moreover, working time accounts improve the quality of present and future employment relations, supporting sustainable enterprises and availability of human capital. In Germany, working time accounts are well disseminated and sophisticated institutional arrangements between the social partners are pretty standard.

The key contribution of this paper helped to close the jobs miracle research gap that has become evident since the global financial and economic crisis, where we revisited the labor market miracle from a disposable income perspective. Interestingly, the appropriate access point to *disclosing the sustaining jobs miracle* is exactly the *sustaining disposable income at work property* that is implemented by working time accounts by construction. Given the revisiting access to the German labor market miracle, the rather unprecedented development of employment and disposable income in Germany prior to, during and in the aftermath of the world crisis has become clear and also fairly predictable.

We conclude with the interpretation that the fact that inter-temporal transfer of worked hours has been enacted beforehand crisis - i.e., the profound experience of working time accounts as a mutual insurance device in Germany’s industrial and workplace relations system - crucially contributed as context factor to the success of the employment stabilizing and even job generating effect during the Great Recession and its aftermath. Thus, employment and income stabilizing over the business cycle through mutual insurance in working time accounts points to an institution that might be promising for other economies and labor markets as well, in particular under conditions of growing scarcity of qualified labor.

The following limitations must be considered when interpreting the presented results. Literature samples are small. The Model of Cybersecurity Behavior Constructs contains some behavior categories for which only one study exists.

Analyses based on Models of Cybersecurity Behavior Constructs have not been empirically evaluated. In addition to its reliability, the model is based on data found in published literature. In this study, there were no statistical strategies developed to combine the results since each study used a different statistical approach to analyze its results.

A limitation of this study is that, as with any literature review, bias and subjectivity were present in selecting literature. As the research within the domain of user cybersecurity behavior continues to grow, so will the literature to provide a comprehensive review of these studies. It is suggested that future studies conduct a meta-analysis literature review. Statistical information from a meta-analysis will complement the overview literature review, strengthening its conclusions.

References

Abbadi, I. M., 2011. *Toward trustworthy clouds' internet scale critical infrastructure.* Paper presented at the International Conference on Information Security Practice and Experience. https://doi.org/10.1007/978-3-642-21031-0_6

Addae, J. H., Sun, X., Towey, D., and Radenkovic, M., 2019. Exploring user behavioral data for adaptive cybersecurity. *User Modeling and User-Adapted Interaction, 29*(3), pp. 701-750. https://doi.org/10.1007/s11257-019-09236-5

Ajzen, I., 2011. *The theory of planned behaviour: Reactions and reflections.* New York: Taylor & Francis. https://doi.org/10.1080/08870446.2011.613995

Alexander, P. A., 2020. Methodological guidance paper: The art and science of quality systematic reviews. *Review of Educational Research, 90*(1), pp. 6-23. https://doi.org/10.3102/0034654319854352

Alqahtani, H., and Kavakli-Thorne, M., 2020. *Exploring Factors Affecting User's Cybersecurity Behaviour by Using Mobile Augmented Reality App (CybAR).* Paper presented at the Proceedings of the 2020 12th International Conference on Computer and Automation Engineering. https://doi.org/10.1145/3384613.3384629

Anderson, C. L., and Agarwal, R., 2010. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS quarterly, 34*(3), pp. 613-643. https://doi.org/10.2307/25750694

Arachchilage, N. A. G., and Love, S., 2014. Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, pp. 304-312. https://doi.org/10.1016/j.chb.2014.05.046

Atkins, L., Francis, J., Islam, R., O'Connor, D., Patey, A., Ivers, N., Foy, R., Duncan, E. M., Colquhoun, H., Grimshaw, J. M., Lawton, R., and Michie, S., 2017. A guide to using the Theoretical Domains Framework of behaviour change to investigate implementation problems. *Implementation science, 12*(1), 77. https://doi.org/10.1186/s13012-017-0605-9

Bada, M., Sasse, A. M., and Nurse, J. R., 2019. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Beautement, A., Sasse, M. A., and Wonham, M., 2008. *The compliance budget: managing security behaviour in organisations.* Paper presented at the Proceedings of the 2008 New Security Paradigms Workshop. https://doi.org/10.1145/1595676.1595684

Boell, S. K., and Cecez-Kecmanovic, D., 2015. On being 'systematic'in literature reviews. In: L. P. Willcocks, C., Sauer, and M. C., Lacity, 2015. *Formulating research methods for* *information systems*. London: Palgrave Macmillan. pp. 48-78. https://doi.org/10.1057/9781137509888_3

Briggs, P., Jeske, D., and Coventry, L., 2017. Behavior change interventions for cybersecurity *Behavior change research and theory*. Elsevier. pp. 115-136. https://doi.org/10.1016/B978-0-12-802690-8.00004-9

Burns, S., and Roberts, L., 2013. Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety, 15*(1), pp. 48-64. https://doi.org/10.1057/cpcs.2012.13

Cane, J., O'Connor, D., and Michie, S., 2012. Validation of the theoretical domains framework for use in behaviour change and implementation research. *Implementation Science, 7*(1), 37. https://doi.org/10.1186/1748-5908-7-37

Cane, J., Richardson, M., Johnston, M., Ladha, R., and Michie, S., 2015. From lists of behaviour change techniques (BCT s) to structured hierarchies: Comparison of two methods of developing a hierarchy of BCT s. *British Journal of Health Psychology, 20*(1), pp. 130-150. https://doi.org/10.1111/bjhp.12102

Cashin, J., and Ifinedo, P., 2014. Using social cognitive theory to understand employees' counterproductive computer security behaviors (CCSB): A pilot study.

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., and Upadhyaya, S., 2006. Role of Perceived Importance of Information Security: An Exploratory Study of Middle School Children's Information Security Behavior. *Issues in Informing Science & Information Technology, 3*. https://doi.org/10.28945/2956

Chenoweth, T., Minch, R., and Gattiker, T., 2009. *Application of protection motivation theory to adoption of protective technologies.* Paper presented at the 2009 42nd Hawaii International Conference on System Sciences.

Choi, M., Levy, Y., and Hovav, A., 2013. *The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse.* Paper presented at the Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC–Workshop on Information Security and Privacy (WISP).

Corradini, I., 2020. Developing Cybersecurity Awareness *Building a Cybersecurity Culture in Organizations* (pp. 101-113): Springer. https://doi.org/10.1007/978-3-030-43999-6_6

de Boer, P. S., van Deursen, A. J., and van Rompay, T. J., 2019. Accepting the Internet-of-Things in our homes: The role of user skills. *Telematics and informatics, 36*, pp. 147-156.

de Kok, L. C., Oosting, D., and Spruit, M., 2020. The influence of knowledge and attitude on intention to adopt cybersecure behaviour. *Information & Security, 46*(3), pp. 251-266. https://doi.org/10.11610/isij.4618

Flores, W. R., Antonsen, E., and Ekstedt, M., 2014. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security, 43*, pp. 90-110. https://doi.org/10.1016/j.cose.2014.03.004

Furnell, S., Esmael, R., Yang, W., and Li, N., 2018. Enhancing security behaviour by supporting the user. *Computers & Security, 75*, pp. 1-9. https://doi.org/10.1016/j.cose.2018.01.016

Gangire, Y., Da Veiga, A., and Herselman, M., 2019. *A conceptual model of information security compliant behaviour based on the self-determination theory.* Paper presented at the 2019 Conference on Information Communications Technology and Society (ICTAS). https://doi.org/10.1109/ICTAS.2019.8703629

Ghosh, S., and Guchhait, S., K., 2020. Literature review and research methodology. In: S., Ghosh, and S., K., Guchhait, 2020. *Laterites of the Bengal Basin.* Springer. pp. 17-31. https://doi.org/10.1007/978-3-030-22937-5_2

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., and Ginther, A., 2018. Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, pp. 345-358. https://doi.org/10.1016/j.cose.2017.11.015

Guo, K. H., 2013. Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security, 32*, pp. 242-251. https://doi.org/10.1016/j.cose.2012.10.003

Hadlington, L., 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hadlington, L., 2018. Employees Attitudes towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom. https://doi.org/10.4018/978-1-7998-7705-9.ch087

Hadlington, L., 2021. The "human factor" in cybersecurity: Exploring the accidental insider *Research Anthology on Artificial Intelligence Applications in Security* (pp. 1960-1977): IGI Global.

Hanus, B., and Wu, Y. A., 2016. Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information systems management, 33*(1), pp. 2-16. https://doi.org/10.1080/10580530.2015.1117842

Herath, T., and Rao, H. R., 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), pp. 154-165. https://doi.org/10.1016/j.dss.2009.02.005

Herbert, F., Schmidbauer-Wolf, G. M., and Reuter, C., 2020. *Differences in IT Security Behavior and Knowledge of Private Users in Germany.* Paper presented at the Proceedings of the International Conference on Wirtschaftsinformatik (WI). https://doi.org/10.30844/wi_2020_v3-herbert

Herrmann, D., and Pridöhl, H., 2020. Basic concepts and models of cybersecurity. In: M. Christen, B., Gordijn, and M., Loi, 2020. *The Ethics of cybersecurity.* Cham: Springer. pp. 11-44. https://doi.org/10.1007/978-3-030-29053-5_2

Hong, Y., and Furnell, S., 2019. *Organizational formalization and employee information security behavioral intentions based on an extended TPB model.* Paper presented at the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). https://doi.org/10.1109/CyberSecPODS.2019.8885405

Ifinedo, P., 2014. *Social Cognitive Determinants of non-Malicious, counterproductive Computer Security Behaviors (Ccsb): an Empirical Analysis.* Paper presented at the MCIS. https://doi.org/10.1109/ICASTECH.2014.7068109

Ifinedo, P., 2017. *Effects of Organization Insiders' Self-Control and Relevant Knowledge on Participation in Information Systems Security Deviant Behavior: [Best Paper Nominee].* Paper presented at the Proceedings of the 2017 ACM SIGMIS Conference on Computers and People Research. https://doi.org/10.1145/3084381.3084384

Jansen, J., and van Schaik, P., 2019. The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies, 123*, pp. 40-55. https://doi.org/10.1016/j.ijhcs.2018.10.004

Johnston, A. C., and Warkentin, M., 2010. Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, pp. 549-566. https://doi.org/10.2307/25750691

Keele, S., 2007. Guidelines for performing systematic literature reviews in software engineering: Technical report, Ver. 2.3 EBSE Technical Report. EBSE.

Kelly, G., 2020. *The psychology of personal constructs.* Oxfordshire: Routledge. https://doi.org/10.4324/9780203359037

Koohang, A., Anderson, J., Nord, J. H., and Paliszkiewicz, J., 2019. Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems,* 118(6), pp. 1209-1228.

Kritzinger, E., and von Solms, S. H., 2010. Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security, 29*(8), pp. 840-847. https://doi.org/10.1016/j.cose.2010.08.001

Kuppusamy, P., Samy, G. N., Maarop, N., Magalingam, P., Kamaruddin, N., Shanmugam, B., and Perumal, S., 2020. *Systematic Literature Review of Information Security Compliance Behaviour Theories.* Paper presented at the Journal of Physics: Conference Series. https://doi.org/10.1088/1742-6596/1551/1/012005

Legárd, I., 2020. Building an effective information security awareness program. *Central and Eastern European eDem and eGov Days, 338*, pp. 189-200. https://doi.org/10.24989/ocg.338.15

Li, L., He, W., Xu, L., Ivan, A., Anwar, M., and Yuan, X., 2014. *Does explicit information security policy affect employees' cyber security behavior? A pilot study.* Paper presented at the 2014 Enterprise Systems Conference. https://doi.org/10.1109/ES.2014.66

Liggett, R. L., 2020. *The Effects of Information Security on Business Continuity: Case Study.* University of Phoenix.

Mashiane, T., and Kritzinger, E., 2019. *Cybersecurity Behaviour: A Conceptual Taxonomy.* Paper presented at the International Conference on Information Security Theory and Practice, Cham. https://doi.org/10.1007/978-3-030-20074-9_11

McDonald, J. D., 2017. *Electric power substations engineering*: CRC press. https://doi.org/10.1201/b12061

Michie, S., Johnston, M., Francis, J., Hardeman, W., and Eccles, M., 2008. From theory to intervention: mapping theoretically derived behavioural determinants to behaviour change techniques. *Applied psychology, 57*(4), pp. 660-680. https://doi.org/10.1111/j.1464-0597.2008.00341.x

Milne, G. R., Labrecque, L. I., & Cromer, C., 2009. Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs, 43*(3), pp. 449-473. https://doi.org/10.1111/j.1745-6606.2009.01148.x

Ofori, K. S., Anyigba, H., Ampong, G. O. A., Omoregie, O. K., Nyamadi, M., and Fianu, E., 2020. Factors Influencing Information Security Policy Compliance Behavior *Modern Theories and Practices for Cyber Ethics and Security Compliance*: IGI Global. pp. 152-171. https://doi.org/10.4018/978-1-7998-3149-5.ch010

Okoli, C., 2015. A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems*, 37. https://doi.org/10.17705/1CAIS.03743

Okoli, C., and Schabram, K., 2010. *A guide to conducting a systematic literature review of information systems research.* Sprouts working papers on information systems. https://doi.org/10.2139/ssrn.1954824

Phillips, C. J., Marshall, A. P., Chaves, N. J., Jankelowitz, S. K., Lin, I. B., Loy, C. T., Rees, G., Sakzewski, L., Thomas, S., To, T.-P., Wilkinson, S. A., Michie, S., 2015. Experiences of using the Theoretical Domains Framework across diverse clinical environments: a qualitative study. *Journal of multidisciplinary healthcare, 8*, pp. 139-146. https://doi.org/10.2147/JMDH.S78458

Radic, A., Ariza-Montes, A., Hernández-Perlines, F., and Giorgi, G., 2020. Connected at sea: The influence of the internet and online communication on the well-being and life satisfaction of cruise ship employees. *International journal of environmental research and public health, 17*(8), 2840. https://doi.org/10.3390/ijerph17082840

Reglitz, M., 2020. The human right to free internet access. *Journal of Applied Philosophy, 37*(2), pp. 314-331. https://doi.org/10.1111/japp.12395

Ruiz, R., Winter, R., and Amatte, F., 2017. The leakage of passwords from home banking sites: A threat to global cyber security? *Journal of Payments Strategy & Systems, 11*(2), pp. 174-186.

Sabillon, R., Cano, J., Cavaller Reyes, V., and Serra Ruiz, J., 2016. Cybercrime and cybercriminals: a comprehensive study. *International Journal of Computer Networks and Communications Security, 2016, 4(6),* pp. 165-176.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., and Herawan, T., 2015. Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, pp. 65-78. https://doi.org/10.1016/j.cose.2015.05.012

Safa, N. S., Von Solms, R., and Furnell, S., 2016. Information security policy compliance model in organizations. *Computers & Security, 56*, pp. 70-82. https://doi.org/10.1016/j.cose.2015.10.006

Shah, P., and Agarwal, A., 2020. Cybersecurity behaviour of smartphone users in India: an empirical analysis. *Information & Computer Security, 28(2)*. https://doi.org/10.1108/ICS-04-2019-0041

Simonet, J., and Teufel, S., 2019. *The Influence of Organizational, Social and Personal Factors on Cybersecurity Awareness and Behavior of Home Computer Users.* Paper presented at the IFIP International Conference on ICT Systems Security and Privacy Protection. https://doi.org/10.1007/978-3-030-22312-0_14

Siponen, M., Mahmood, M. A., and Pahnila, S., 2014. Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), pp. 217-224. https://doi.org/10.1016/j.im.2013.08.006

Siponen, M., Pahnila, S., & Mahmood, A. (2007). *Employees' adherence to information security policies: an empirical study.* Paper presented at the IFIP International Information Security Conference. https://doi.org/10.1007/978-0-387-72367-9_12

Skinner, T., Taylor, J., Dale, J., and McAlaney, J., 2018. *The development of intervention e-learning materials and implementation techniques for cyber-security behaviour change*.

Skovhoj, F. H. Z., 2020. *"I cannot go through a day without the internet": exploring the dynamics of everyday uses of the internaet in China.* University of Copenhagen,[Faculty of Humanities].

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J., 2005. Analysis of end user security behaviors. *computers & security, 24*(2), pp. 124-133. https://doi.org/10.1016/j.cose.2004.07.001

Talib, S., Clarke, N. L., and Furnell, S. M., 2010. *An analysis of information security awareness within home and work environments.* Paper presented at the 2010 International Conference on Availability, Reliability and Security. https://doi.org/10.1109/ARES.2010.27

Tsai, H.-y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., and Cotten, S. R., 2016. Understanding online safety behaviors: A protection motivation theory perspective. *computers & security, 59*, pp. 138-150. https://doi.org/10.1016/j.cose.2016.02.009

Van Bavel, J. J., Baicker, K., Boggio, P. S., Capraro, V., Cichocka, A., Cikara, M., Crockett, M. J., Crum, A. J., Douglas, K. M., Druckman, J. N., Drury, J., Dube, O., Ellemers, N., Finkel, E. J., Fowler, J. H., Gelfand, M., Han, S., Haslam, S. A., Jetten, J., ... Willer, R., 2020. Using social and behavioural science to support COVID-19 pandemic response. *Nature Human Behaviour*, 4(5), pp. 460-471. https://doi.org/10.31234/osf.io/y38m9

Vance, A., Siponen, M., and Pahnila, S., 2012. Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management, 49*(3-4), pp. 190-198. https://doi.org/10.1016/j.im.2012.04.002

Verkijika, S. F., 2018. Understanding smartphone security behaviors: an extension of the protection motivation theory with anticipated regret. *Computers & Security, 77*, pp. 860-870. https://doi.org/10.1016/j.cose.2018.03.008

Vishwanath, A., Harrison, B., and Ng, Y. J., 2018. Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research, 45*(8), pp. 1146-1166. https://doi.org/10.1177/0093650215627483

Weber, K., Schütz, A. E., Fertig, T., and Müller, N. H., 2020. *Exploiting the Human Factor: Social Engineering Attacks on Cryptocurrency Users.* Paper presented at the International Conference on Human-Computer Interaction. https://doi.org/10.1007/978-3-030-50506-6_45

Wshah, A., Selzler, A.-M., Hill, K., Brooks, D., and Goldstein, R., 2020. Determinants of Sedentary Behaviour in Individuals with COPD: A Qualitative Exploration Guided by the Theoretical Domains Framework. *COPD: Journal of Chronic Obstructive Pulmonary Disease*, 1-9. https://doi.org/10.1080/15412555.2019.1708883

Xiao, B., and Wong, Y. M., 2013. Cyber-bullying among university students: An empirical investigation from the social cognitive perspective. *International Journal of Business and Information, 8*(1), pp. 34-69.

Xiao, Y., and Watson, M., 2019. Guidance on conducting a systematic literature review. *Journal of Planning Education and Research, 39*(1), pp. 93-112. https://doi.org/10.1177/0739456X17723971

Ying, G., and Zonghua, L., 2020. *The Characteristics and Value of Internet Use in the Elderly.* Paper presented at the 2020 4th International Seminar on Education, Management and Social Sciences (ISEMSS 2020). https://doi.org/10.2991/assehr.k.200826.001