The Forgotten Model – Validating the Integrated Behavioral Model in Context of Information Security Awareness

Andreas E. Schütz
University of Applied Sciences
Würzburg-Schweinfurt
andreas.schuetz@fhws.de

Tobias Fertig
University of Applied Sciences
Würzburg-Schweinfurt
tobias.fertig@fhws.de

Abstract

The behavior of employees has a strong influence on the information security of a company. Whether humans behave information security compliant depends on a large extent on their information security awareness (ISA). Social psychology provides an understanding about factors that influence awareness and thus gives relevant insights on how to increase an employee's ISA. A promising theory from health psychology is the Integrated Behavioral Model (IBM). To validate the significance of the IBM for ISA, a structured literature review about models that explain ISA has been conducted. The analysis of the found ISA models and their constructs showed that the IBM indeed includes all found factors. Based on the findings, the paper presents an extended model of the IBM within the ISA context with a higher level of detail. The model can be used to analyze individualized ISA and help companies to enhance ISA in a systematic way.

Keywords: Information Security Awareness, ISA, Human Factor, Information Security, Integrated Behavioral Model.

1. Introduction

Society and work has been influenced by increasing digitization for several years. The COVID-19 pandemic has given this digital development a further boost and shifted previously analog activities, such as meetings, into the digital space. As digitization continues to grow, so do the demands on information security. A survey found that, on average, 43 percent of companies surveyed worldwide have experienced a cyber attack in the last twelve month (Hiscox Ltd, 2021). A study in which German small- and medium-sized enterprises (SME) were surveyed produced a similar figure: 45 percent of SME stated that they had been confronted with a cyber attack in the last 12 months that required an active response and intervention (Huaman et al., 2021). Several years ago, companies were able to counter these threats primarily with technical measures, like firewalls. Today, however, attackers are increasingly targeting an easier entry point: the human factor. To manipulate the user instead of trying to gain access to a system by using exploits or brute force attacks is easier for attackers. Recent studies confirm that enterprises are most often hit by attacks targeting the human factor: social engineering attacks, such as phishing, and the distribution of malware or ransomware are prevailing (Huaman et al., 2021; ISACA, 2021). In order to react appropriately to this development, it is becoming more important for enterprises to sensitize their employees for information security. The degree to which an individual is sensitized is also referred to as information security awareness (ISA). Security awareness is the interaction of knowledge and skills, intention, salience, and habits related to an specific information security behavior (Schütz, 2018). The aim of sensitization measures is to encourage employees to behave in a manner that is compliant with information security rules and regulations (Schütz et al., 2020).

Social psychology examines how the behavior of individuals can be influenced (Ajzen, 2020). More specific, health psychology uses behavioral models to explain behaviors related to, for example, physical activity or drug use. A popular model is described by the Theory of Planned Behavior (TPB) (Ajzen, 1991) that evolved from the Theory of Reasoned Action (TRA) (Fishbein & Ajzen, 1975). Behavioral models have been used by researchers from other disciplines as well. For example, the TPB has been used to study

URI: https://hdl.handle.net/10125/103462
978-0-9981331-6-4
(CC BY-NC-ND 4.0)

behaviors related to protecting one's privacy (Ajzen, 2020). Findings from social psychology are therefore also recommended to understanding human behavior with regard to information security (Bosworth & Kabay, 2002). A literature analysis of Lebek et al. (2013) shows that TPB and TRA are the most commonly used models in this context. In 1998 both theories were further developed by Kasprzyk et al. (1998) and after several field studies proposed as extension of the TRA and TPB (Montaño & Kasprzyk, 2008). This so called Integrated Behavioral Model (IBM) includes important constructs that have been explained only marginally in TPB / TRA, such as a person's knowledge and skills. Despite the extensions, however, the model has found little application in the field of ISA. Schütz (2018) has proposed the IBM for interpretation in this research field.

This work aims to methodologically test the suitability of IBM for the research field ISA. This validation qualifies the model for further use in the research field and thus substantiates the scientific findings based on it. The study also helps to interpret the IBM in the context of ISA, as concepts from other theories and models are assigned to the IBM. We use a systematic literature review to identify commonly used research models that explain ISA and information security compliant behavior. Afterwards we analyze whether the IBM includes the constructs used in the models or whether additions are necessary. As a secondary outcome, we document the theories and models of social psychology underlying the models to provide an updated review to the research community.

Section 2 describes the theoretical background of ISA and the IBM. We are specifying the research questions in Section 3 and the research approach in Section 4. Section 5 introduces the used data sources. The results of the review are explained in Section 6 and discussed in Section 7. The last section provides the conclusion.

2. Theoretical Background

ISA addresses the "human factor" and how users can be sensitized to behave in an information security-compliant way. With their compliant behavior, such as not connecting USB devices of unknown sources to their PC, users help increasing the information security within a company. By actively involving users in the information security concept of a company, they become a last line of defense. One commonly accepted method for this involvement are security awareness campaigns. These campaigns aim for motivating users to actually use their theoretical knowledge about information security in practice (Bada et al., 2014) and for convincing them of the importance of their actions.

To explain the mental construct ISA the Integrated Behavioral Model (IBM) (Montaño & Kasprzyk, 2008) shown in Figure 1 is used. The model was already interpreted in the context of ISA (Schütz, 2018). Because of the mental character, only cognitive and affective factors are included in the described understanding of ISA. External factors, such as a company's organization, may influence ISA or information security-compliant behavior, but they are not explicitly part of the ISA. The ISA of a person is the sum of the four factors knowledge and skills ("I know how the behavior is performed"), habit ("I'm used to perform the behavior"), salience ("The performance of the behavior is in my mind"), and behavioral intention ("I want to perform the behavior"). The factors are always observed in connection with a specific behavior, e.g., "I do not open attachments in e-mails from unknown recipients".

The factor behavioral intention is complex and formed by the three mental constructs 'Attitude', 'Perceived Norm' and 'Personal agency' of a person. A person's attitude results from the 'Experiential Attitude' ("What have I experienced while performing the behavior in the past?"), which is influenced by the feelings about a behavior, and the 'Instrumental Attitude' ("What are the consequences of the execution of the behavior?"), which is affected by behavioral beliefs regarding the effects of the behavior. A person's 'Perceived Norm' results from the 'Injunctive Norm' and the 'Descriptive Norm'. The 'Injunctive Norm' reflects the person's normative beliefs about what behavior their social environment expects of the person. The 'Descriptive Norm' describes the normative beliefs of how people in the environment themselves behave. A person's 'Personal Agency' is formed by the 'Perceived control' ("Is the execution of the behavior simple or difficult in view of the circumstances?") and the 'Self-efficacy' ("Do I dare to perform the behavior with my abilities?"). The first is created by the control beliefs and the second by the efficacy beliefs of a person. To influence all of these intentional factor, campaigns to change behaviors need to address a person's feelings and beliefs (Montaño & Kasprzyk, 2008).

In order to convince a user to behave in compliance with information security policies, one or several of the above mentioned factors need to be influenced. But even then, 'Environmental Constraints', such as lack of required technical equipment can prevent the performance of the behavior.

A literature review by Lebek et al. (2013) examined various theories that influence ISA research. In

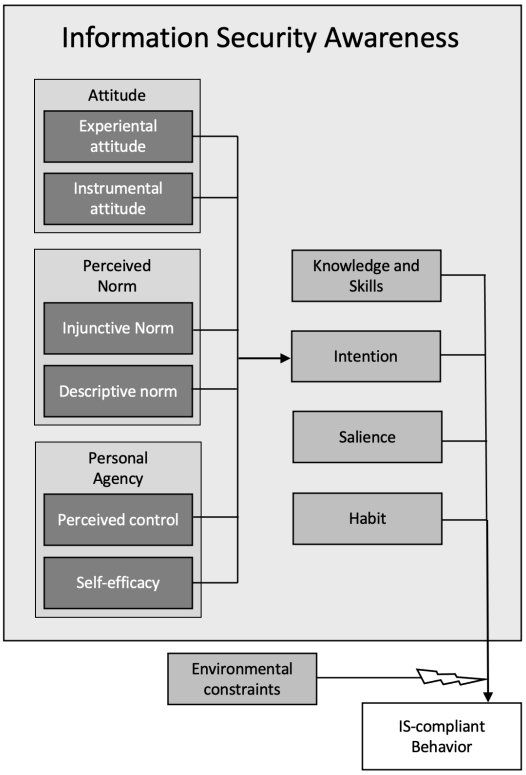

Figure 1. Explanation of ISA based on the IBM of Montaño and Kasprzyk (2008)

113 analyzed publications, 54 different theories were discovered. The most frequently used theories were the Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB), General Deterrence Theory (GDT), Protection Motivation Theory (PMT), and the Technology Acceptance Model (TAM). Based on these models the researchers developed a meta-model. We aim to update these results. Instead of developing a meta-model, however, the understanding of ISA based on the IBM will be validated.

3. Research Approach

The research aims to confirm the completeness of the IBM for application in this research field. The purpose of this review is to identify any missing or complementary constructs that could supplement the explanation of ISA presented in Section 2. It is the aim to affirm the suitability of the IBM for interpretation in the context of ISA. This leads to the following questions:

Q1) Does the understanding of ISA based on the IBM include all important constructs of the research field ISA?

Q2) Can constructs from the research field ISA be used to extend the understanding of ISA based on the IBM?

We analyzed the publications of the ISA research field with a structured literature review. An additional result of the analysis is a collection of models, theories and definitions used in the identified models to explain ISA. The collection may help researchers to develop, refine, or evaluate their own understanding of ISA. This leads to the third research question:

Q3) What are the primary models, theories and definitions used to explain ISA?

A rigorous search process is fundamental for the quality of a literature review (Brocke et al., 2009). We followed the recommendations of Webster and Watson (2002) to ensure that the literature research is valid, reliable and repeatable.

To meet the requirements of Webster and Watson (2002), the research process was started with a keyword search. As relevant data sources, we used scientific databases related to Computer Science. The databases used are listed in Table 1. We used the term 'security awareness' as the main search term, which also covers synonymous terms such as 'information security awareness' or 'IT security awareness'. To get an exact match, we used the quotation mark-operator for the term. We further specified the keyword search and included the closely related keywords 'model', 'factor', 'behavior' and 'influence'. The term 'security awareness' was AND concatenated with any of these four keywords. In addition to the title, the abstract and, if possible, the author-related keywords of the publications in the database were searched.

Only papers in English and only papers published after the year 2000 were included to ensure timeliness of the results. All search results were filtered by manually scanning the titles, abstracts and, if necessary, the full texts of the papers. Only articles were included that described a model that either contained a description of ISA or a procedure to promote ISA.

For each data source, Table 1 shows the respective hits and the publications that were ultimately included. The relevant sources were then manually used in a backward and forward search, which resulted in one additional publication to be included. Duplicates were removed from the numbers of included papers. As a duplicate we understood the repeated appearance of the same publication or the repeated appearance of an identical model, e.g., in another publication of the same author. In the latter case, the original publication of the model was included in the further analysis. We found a total of 41 relevant publications.

Table 1. Results of the Keyword Search

Data Source	Hits	Included	Forw./ Backw.
IEEE Xplore Digital Library	204	11	1
ACM Digital Library	203	3	0
Science Direct	142	10	0
Springer Link	76	8	0
AIS eLibrary	348	8	0

4. Research Results

The 41 found publications were analyzed in detail. Many models did not focus on ISA, but only used ISA in context to explain other issues like corporate culture. These publications were excluded. Other models were excluded, because they interpreted ISA in very specific use cases, e.g., ISA of customers (Bredenkamp et al., 2021), which does not add to a generic understanding of ISA. We also sorted out the aforementioned model by (Schütz, 2018), as this corresponds exactly to the researched understanding of ISA based on the IBM. 19 publications had thus been excluded from the list of results. The remaining 22 publications are listed in Table 2. Table 2 also lists the social psychology theories underlying the models and the author's understanding of ISA. The full names of the abbreviations used for the fundamental theories or models can be seen in Table 3.

As broken down in Table 3, most of the models included were based on models and theories from the field of health psychology. Some publications even built on multiple models and theories. The most popular of these are the already mentioned Theory of Reasoned Action (TRA) / Theory of Planned Behavior (TPB), which also strongly influenced the IBM. 13 publications used it as a basis. Also popular is the Protection Motivation Theory (PMT) (Rogers, 1975), used by ten publications. The Health Belief Model (HBM) was also used five times. Other models and theories used sporadically were the General Deterrence Theory (GDT) from the field of criminology (Straub, 1990), the Knowledge Attitude Behavior Model (KAB), the Technology Acceptance Model (TAM), which is based on the TRA (Davis, 1989), the Behaviourism Theory (BT) from general psychology, and the Technology Threat Avoidance Theory (TTAT), which is based on the PMT. One of the publications did neither use a theory nor model.

In a closer analysis of the ISA models described in the identified publications, we reviewed the factors and constructs presented in the models and their effects. Only factors and constructs not already explicitly included in the IBM were examined. We did not consider factors from a person's environment as they do not represent cognitive and affective factors. Many models include factors from the organization of a company, such as information security policies. These factors influence the ISA of a person with the goal to make them behave information security compliant. However, these interventions do not add to the understanding of ISA as such and are not considered in this research. Therefore, we excluded the following factors: Operant Conditioning, Classical Conditioning, Risk Communication, Information Security Culture and Organizational Factors.

Furthermore, no factors were considered that represent personal characteristics of a person, such as gender or age. These factors cannot be influenced by companies in awareness measures and are therefore not relevant as factors for describing a person's ISA. They provide an explanation of why a person has certain beliefs about a behavior. In this context, however, only the beliefs themselves are interesting. For example, a lazy person might believe that changing a password is too exhausting. This belief, along with other beliefs, influences the person's intention. Only the beliefs and the intention are part of a person's ISA, because only they are directly related to the information security issue. The company may, for example, improve the process of changing a password to lower the barrier to performing the behavior, or use rewards to encourage the "leap" over the hurdle. However, the lazy character trait of the person will not change. For these reasons, the factors Learning Style, Personal Traits and Control Variables were excluded. However, these individual properties are not useless in context of security awareness. They support the selection of suitable measures for a campaign.

The remaining factors were closer analyzed regarding whether they were already included in the IBM or not. We found that all factors and constructs were covered within the IBM. The factors examined often corresponded to a different level of detail and described concepts that are already included in the model as a higher-level term. Some factors also turned out to be synonymous terms for an already existing factor. The collection and assignment of factors are listed in Table 4. In the left column is the collection of factors from the literature review. In the right column are the corresponding factors of the IBM based ISA understanding.

The factors 'IT Expertise' and 'Experience with cyber security practice' are more specific terms for the factor 'Knowledge and Skills'. Since a concrete instantiation of the model is on the level of a single

Table 2. The relevant Publications from the Literature Review.

Authors	Foundations	Definition ISA
Humaidi et al. (2014)	HBM	Influencing a user's attitude and behavior toward greater safety awareness.
Lebek et al. (2013)	TRA, TPB, GDT, PMT, TAM	No definition.
Gundu and Flowerday (2012)	TRA, PMT	Train employees to behave securely in the area of information security. Employees must be aware of the importance of security and the consequences of mistakes.
Moletsane and Tsibolane (2020)	KAB, TPB	No definition.
Gundu and Flowerday (2013)	TRA, BMT, BT	Raising employee awareness and promoting appropriate behavior in the area of information security.
Alohali et al. (2017)	None	Users must be aware of their responsibilities, have the necessary knowledge for their role in information security and know how to protect themselves.
Connolly et al. (2018)	GDT	Encourage employees to behave in a safety-conscious manner.
Hassan and Ismail (2015)	HBM	No definition.
Simonet and Teufel (2019)	TPB, PMT	Provide policies, security training, and create a culture of information security.
Rocha Flores et al. (2014)	TRA, TPB	Awareness of threats to information security, recognizing and responding to fraudulent social engineering techniques used by attackers.
Parsons et al. (2017)	KAB	Understand safe information security behaviors, commit to best practices, and behave accordingly.
Hanus et al. (2018)	TTAT, PMT	Understanding of the importance of information security and the associated responsibility for users, knowledge and understanding of security issues in the organization.
Curry et al. (2018)	TPB, PMT	No definition.
Nasir et al. (2017)	TPB	No definition.
Grassegger and Nedbal (2021)	TRA, TPB	Inform employees about information security risks, explain tasks and responsibilities.
Bélanger et al. (2017)	TPB	General security awareness of a person and awareness about information security policy.
Cox (2012)	TPB, PMT, HBM	Establish policies, procedures, and mandatory user training.
Ng et al. (2009)	HBM	Influencing a user's attitude and behavior toward greater safety awareness.
Anwar et al. (2017)	HBM, PMT	No definition.
Thompson et al. (2017)	PMT, TPB	No definition.
Yoon et al. (2012)	PMT	Awareness of an external threat or peer pressure on information security trigger information security behavior.
Jaeger (2018)	TRA/TPB	An individual's knowledge and understanding of topics related to information security.

Table 3. The Number of Fundamental Theories or Models Used in the Identified Publications

Used Theories/Models	Count
Theory of Reasoned Action (TRA) / Theory of Planned Behavior (TPB)	13
Protection Motivation Theory (PMT)	10
Health Belief Model (HBM)	5
General Deterrence Theory (GDT)	2
Knowledge Attitude Behavior Model (KAB)	2
Technology Acceptance Model (TAM)	1
Behaviourism Theory (BT)	1
Technology Threat Avoidance Theory (TTAT)	1
No Theory/Model used	1

behavior, knowledge and skills are always very precise in practical application. For example, the person knows what makes a password secure.

Quite a few factors can be assigned to 'Attitude' in the IBM. The factors 'Trust' and 'Previous, Past or Prior Experience' generate affective feelings that are evoked by the past performance of a behavior. The feelings can be positive, such as 'Trust', or negative like 'Computer Anxiety'. These feelings are assigned to 'Experiental Attitude'.

Another 21 factors could be assigned to 'Instrumental Attitude'. All of these factors represent cognitive behavioral beliefs and manifest as a person's judgment of what the effects of a particular behavior may be. The factors 'Perceived Susceptibility', 'Perceived Severity of Threat', 'Perceived Vulnerability', 'Risk', and 'Risk Perception and Threat Appraisal' describe the belief that a non-compliant behavior poses a danger or a risk. The higher and the more probable the perceived danger appears, the higher the effect on the intention to perform a compliant behavior. The factors 'Sanctions', 'Perceived Certainty of Sanctions', and 'Perceived Severity of Sanctions' describe beliefs that a non-compliant behavior is accompanied by sanctions. Again, the likelihood and the level of those expected sanctions influences the intention. The opposite direction includes the factors 'Perceived Benefits', 'Rewards', and 'Intrinsic Benefit'. These factors are about beliefs with respect to intrinsic and extrinsic rewards for conforming behavior. The three factors 'Motivational Outcome Expectancies', 'Planning Outcome Expectancies', and 'Action Outcome Expectancies' generally describe beliefs that a behavior will lead to a particular outcome. The beliefs are distinguished in the motivational, planning, and action phases. The beliefs behind the factors 'Perceived Usefulness' and 'Perceived Effectiveness' refer to the added value of a behavior. The 'Perceived Response Efficacy' factor, on the other hand, includes beliefs about whether a particular behavior actually eliminates a perceived threat. The factor is part of the higher-level 'Coping Appraisal' factor. The 'Interest in IS' factor is associated with beliefs about the importance of the issue. The factor 'Psychological Ownership' deals with beliefs regarding the perceived responsibility and perceived personal value of an item. Employees do not perceive information, information systems, or the company's infrastructure as their own property, and therefore value these less. Potential damage may therefore be considered less severe. The same applies to the factor "Vulnerability of Resources", which describes beliefs about the expected damage in the event of non-compliant behavior.

Some factors could be assigned to the factor 'Perceived Norm' in the IBM. For the 'Injunctive Norm' the synonym 'Subjective Norm', and 'Cultural Assumptions and Beliefs' were identified. 'Perceived Peer Behavior' was assigned to the 'Descriptive Norm'.

A large number of factors could be assigned to the construct 'Personal Agency'. The 'Perceived Control' factor of the IBM describes a person's beliefs about the control of their own behavior in the face of the influence of factors from the environment. These are negatively influenced by barriers from the environment. The factor 'Perceived Behavioral Control' is a synonym for this term. The terms 'Perceived Response Cost', 'Perceived/Intrinsic Cost', 'Perceived Ease of Use', 'Perceived Barriers', and 'Work Impediment' represent beliefs for 'Perceived Control'. The term 'Coping Planning' is also associated. It describes the mental simulation of overcoming anticipated barriers in relation to a behavior (Sniehotta et al., 2005). The factor 'Self-efficacy' appeared frequently in the reviewed ISA models. 'Self-efficacy' is about one's own ability to perform a behavior. The factors 'Pre-Action Self-efficacy' and 'Recovery Self-efficacy' detail 'Self-efficacy' for specific situations. While 'Pre-Action Self-efficacy' describes the motivation for a behavior, 'Recovery Self-efficacy' is about the resumption of a behavior after a setback. 'Perceived Working Experience' also represents a conviction of one's own abilities. The overarching term 'Control Appraisal', which was already introduced for the 'Instrumental Attitude' factor, also includes 'Self-efficacy' in addition to 'Perceived Response Efficacy'.

Table 4. Mapping the Factors of the identified Models to the IBM based Understanding of ISA

Factors Identificated in Literature Research	Equivalent Factor in Own Understanding of ISA
IT-Expertise, Experience with Cyber Security Practice	Knowledge and Skills
Trust, Previous/Past/Prior Experience, Computer anxiety.	Intention: Experiental Attitude
Perceived Susceptibility, Perceived Severity of Threat, Perceived Vulnerability, Risk, Risk Perception, Threat Appraisal, Sanctions, Perceived Certainity of Sanctions, Perceived Severity of Sanctions, Perceived Benefits, Rewards, Intrinsic Benefit, Motivational Outcome Expectancies, Planning Outcome Expectancies, Action Outcome Expectancies, Perceived Usefulnes, Perceived Effectivness, Perceived Response Efficacy, Coping Appraisal, Interest in IS, Psychological Ownership, Vulnerability of resources.	Intention: Instrumental Attitude
Subjective Norm, Cultural Assumption and Belief	Intention: Injunctive Norm
(Perceived) Peer Behavior.	Intention: Descriptive Norm
Perceived Behavioral Control, Perceived Response Cost, Perceived/Intrinsic Cost, Perceived Ease of Use, Perceived Barriers, Work impediment, Action/Coping Planning.	Intention: Perceived Control
Pre-Action Self-efficacy, Recovery Self-efficacy, Perceived working experience, Coping Appraisal.	Intention: Self-efficacy
Cues to Action	Salience
Early Conformance Behavior	Habit

In addition, we were able to assign the factors 'Cues to Action' to the factor 'Salience' and 'Early Conformance Behavior' to the factor 'Habit'.

In addition to the factors, we also reviewed the various definitions for ISA used in the literature. Table 2 shows the search results with the detailed definitions. The following statements can be found frequently in the definitions.First, the understanding of the importance of ISA: Employees should have a comprehensive understanding of the importance of ISA. This includes an awareness of possible consequences of errors. (Alohali et al., 2017; Bélanger et al., 2017; Gundu & Flowerday, 2013; Hanus et al., 2018; Rocha Flores et al., 2014) Second, to encourage IS compliant behavior: IS compliant behavior has to be promoted and supported. Employees need to be encouraged to behave in a conscious manner. (Connolly et al., 2018; Gundu & Flowerday, 2013) Third, Training on ISA topics and behavior: Employees must be trained on information security compliant behavior. They must also be teached about relevant topics such as social engineering techniques. (Cox, 2012; Grassegger & Nedbal, 2021; Gundu & Flowerday, 2012; Ng et al., 2009; Rocha Flores et al., 2014) Forth, the use of knowledge and skills: Training on safety-related topics alone is not enough; employees must also be able to apply knowledge and skills and react in appropriate situations. (Alohali et al., 2017; Hanus et al., 2018; Parsons et al., 2017; Rocha Flores et al., 2014) Fifth, to provide rules and guidelines: Companies should provide rules and guidelines regarding information security and inform employees about them. (Cox, 2012; Simonet & Teufel, 2019)

The collected topics from the ISA definitions in the literature also support the IBM based ISA understanding. Employees gain the necessary understanding about how their behavior influences information security through comprehensive training. To promote IS compliant behavior, companies may use training and awareness measures. In addition, restrictions from the environment should be kept to a minimum. The other points of training on ISA topics, knowledge and skills, and provision of regulations and guidelines can also be linked to the IBM's 'Knowledge and Skills' factor.

5. Discussion

The literature review revealed 22 publications with models that explain ISA and list different factors or constructs that influence or are part of ISA. All factors from the models could be assigned to corresponding factors of the IBM. With respect to Q1, this leads us to conclude that the initially described understanding of ISA includes all the important constructs of the research field ISA. We therefore encourage researchers to base their future research into ISA on the IBM.

Even though the IBM represents all identified factors, many interesting theories and constructs were identified in the literature review that increase the

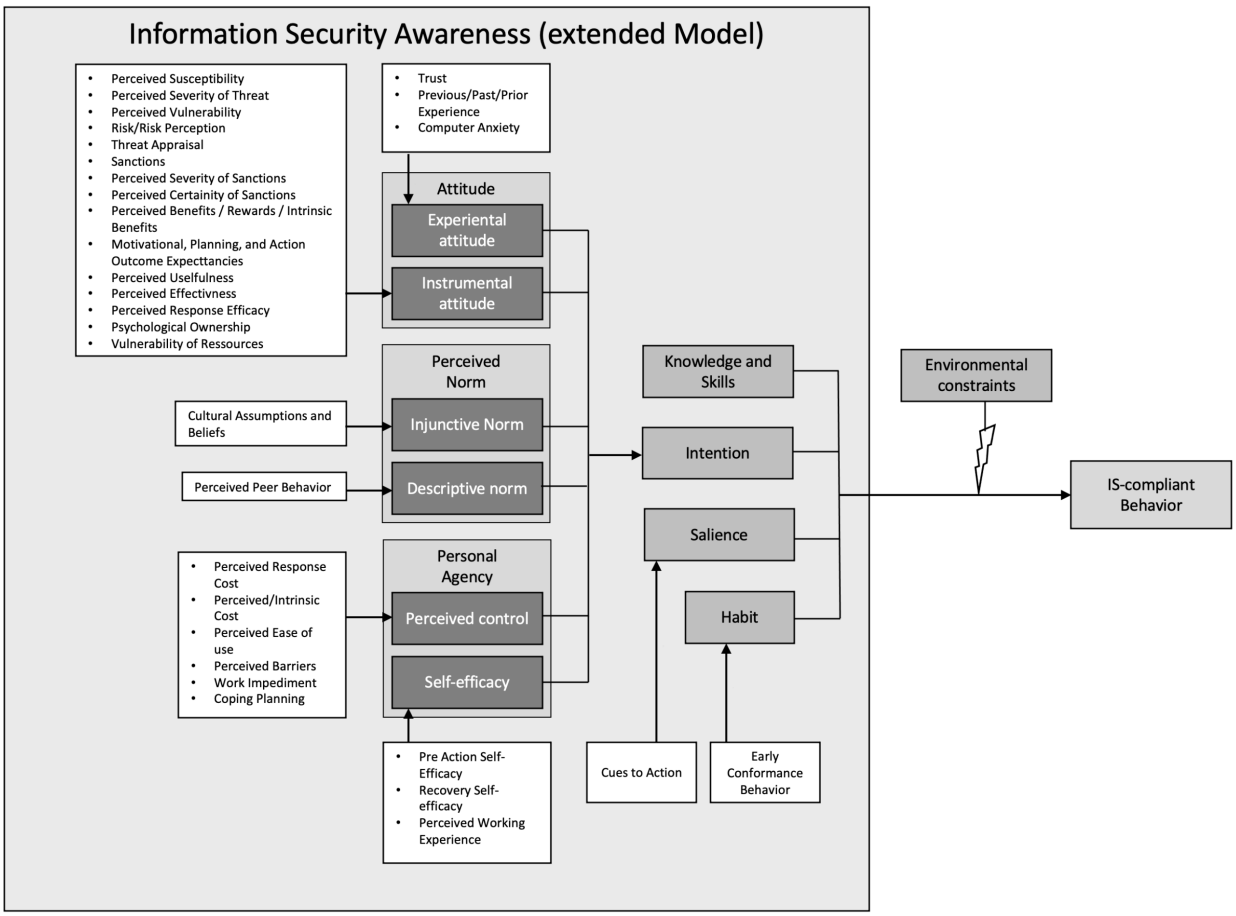

Figure 2. Extended Model of Information Security Awareness.

understanding of ISA and explain the factors in the IBM in more detail. Even if the basic model does not need to be expanded, the identified factors can be included in a model with a higher level of detail. This more complex model can be used to further explain relationships among ISA constructs. In addition, the extended model helps to "translate" findings between different research models. Research question Q2, whether constructs from the research field ISA can be used to extend the understanding of ISA based on the IBM, can therefore be answered with a "yes". Figure 2 shows the extended model. The synonymous terms from Table 5 have been aggregated to on term in the figure.

Research question Q3 dealt with the primary models, theories and definitions used to explain ISA. The answers to these questions were presented in Table 2 and Table 3. Almost all identified publications are based on common theories from social psychology, which also underlie the IBM. This explains the high degree of agreement among the factors. As can be seen in Table 3, the TRA/TPB were used particularly frequently by other researchers. The two theories have a particularly high degree of agreement with the IBM, but do not themselves represent all of the factors of the IBM. The widespread use of findings from social psychology confirms that ISA researchers should use these findings in an interdisciplinary manner. The many different factors show that sensitization the complex nature of targeted and individualized sensitization.

6. Conclusion

To validate the appropriateness of the understanding of ISA based on the IBM, a structured literature review has been conducted. The goal was to reveal publications that include models explaining ISA. In the 22 appropriate publications, we found that almost all authors elaborate on models that adapt findings from popular social psychology theories. When analyzing the individual factors and components in these models, we found that the IBM based understanding of ISA already covers all of them. However, many of the identified

factors can still help to increase the understanding of ISA. Therefore, this paper suggests an extended model of the IBM that has a higher level of detail. The complex representation of ISA shows that awareness can only be raised on a very individual and targeted basis. Standardized measures according to the motto "one size fits all" do not align with the complexity of the construct ISA.

With the model presented, it is possible to analyze the reasons for non-compliant behavior of employees. For example, instead of a lack of knowledge, an overly complex process could lead to a lack of intention of behaving compliantly. With this input, truly targeted actions can then be taken to improve employee behavior. In this way, the human factor can efficiently contribute to better information security. We encourage researchers to use the validated understanding of ISA in their research. The extended model can help to explain questions from the research field ISA in detail. The extended model also helps to transfer existing ISA understanding into the presented understanding. We also encourage researchers to extend the model even further. Also, besides the model, this paper gives researchers an overview of the theories, models, and definitions used in the research field.

In order to keep the complexity of the subject area within bounds, we have only identified affective and cognitive factors in this work. In future work, this can be expanded to include influencing factors from outside, for example from the organization. In addition, we did not consider individual and only hardly changeable personality traits of a person. This provides opportunities for further expansion of the model. Both are not to be understood as part of ISA, but can help to develop measures or interventions to increase the ISA of a person. This should be done in companies in an orderly process. Therefore, these insights can be used to help companies to enhance their ISA in a systematic way.

Acknowledgements

Authors were supported by the BayWISS Consortium Digitization.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, (50), 179–211.

Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. *Human Behavior and Emerging Technologies*, *2*(4), 314–324. https://doi.org/10.1002/hbe2.195

Alohali, M., Clarke, N., Furnell, S., & Albakri, S. (2017). Information security behavior: Recognizing the influencers. *2017 Computing Conference*, 844–853. https://doi.org/10.1109/SAI.2017.8252194

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Bada, M., Sasse, A. M., & Nurse, J. R. (2014). Cyber security awareness campaigns: Why do they fail to change behaviour? *Global Cyber Security Capacity Centre: Draft Working Paper*, 188–131.

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*, *54*(7), 887–901. https://doi.org/10.1016/j.im.2017.01.003

Bosworth, S., & Kabay, M. E. (2002). *Computer security handbook* (4th ed.). Wiley.

Bredenkamp, I. E., Kritzinger, E., & Herselman, M. (2021). A Conceptual Framework for Consumer IS Compliance Awareness: South African Government Context. In R. Silhavy (Ed.), *Informatics and Cybernetics in Intelligent Systems* (pp. 682–701). Springer International Publishing. https://doi.org/10.1007/978-3-030-77448-6_66

Brocke, v. J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., & Cleven, A. (2009). Reconstructing the giant: On the importance of rigour in documenting the literature search process. *ECIS*.

Connolly, L. Y., Lang, M., & Tygar, D. J. (2018). Employee Security Behaviour: The Importance of Education and Policies in Organisational Settings. In N. Paspallis, M. Raspopoulos, C. Barry, M. Lang, H. Linger, & C. Schneider (Eds.), *Advances in Information Systems Development* (pp. 79–96). Springer International Publishing. https://doi.org/10.1007/978-3-319-74817-7_6

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior*, *28*(5), 1849–1858. https://doi.org/10.1016/j.chb.2012.05.003

Curry, M., Marshall, B., Crossler, R. E., & Correia, J. (2018). Infosec process action model (ipam): Systematically addressing individual security behavior. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *49*(SI), 49–66. https://doi.org/10.1145/3210530.3210535

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.*, *13*(3), 319–340. https://doi.org/10.2307/249008

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Addison-Wesley Pub. Co.

Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*, *181*, 59–66. https://doi.org/10.1016/j.procs.2021.01.103

Gundu, T., & Flowerday, S. V. (2013). Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal*, *104*(2), 69–79. https://doi.org/10.23919/SAIEE.2013.8531867

Gundu, T., & Flowerday, S. V. (2012). The enemy within: A behavioural intention model and an information security awareness process. *2012 Information Security for South Africa*, 1–8. https://doi.org/10.1109/ISSA.2012.6320437

Hanus, B., Windsor, J. C., & Wu, Y. (2018). Definition and multidimensionality of security awareness: Close

encounters of the second order. *SIGMIS Database*, *49*(SI), 103–133. https://doi.org/10.1145/3210530.3210538

Hassan, N. H., & Ismail, Z. (2015). A Conceptual Model Towards Information Security Culture in Health Informatics. In K. Ab. Hamid, O. Ono, A. M. Bostamam, & A. Poh Ai Ling (Eds.), *The Malaysia-Japan Model on Technology Partnership* (pp. 187–196). Springer Japan. https://doi.org/10.1007/978-4-431-54439-5_17

Hiscox Ltd. (2021, April). *Hiscox cyber readiness report 2021* (tech. rep.). Hamilton, Bermuda, Hiscox Ltd. https://www.hiscoxgroup.com/sites/group/files/documents/2021-04/Hiscox%5C%20Cyber%5C%20Readiness%5C%20Report%5C%202021.pdf

Huaman, N., Skarczinski, v. B., Stransky, C., Wermke, D., Acar, Y., Dreißigacker, A., & Fahl, S. (2021). A large-scale interview study on information security in and attacks against small and medium-sized enterprises. *30th USENIX Security Symposium (USENIX Security 21)*, 1235–1252. https://www.usenix.org/conference/usenixsecurity21/presentation/huaman

Humaidi, N., Balakrishnan, V., & Shahrom, M. (2014). Exploring user's compliance behavior towards health information system security policies based on extended health belief model [[Online; accessed 2021-11-14]]. *2014 IEEE Conference on e-Learning, e-Management and e-Services (IC3e)*, 30–35. https://doi.org/10.1109/IC3e.2014.7081237

ISACA. (2021). *State of cybersecurity 2021. part 2: Threat landscape, security operations and cybersecurity maturity* (tech. rep.). Schaumburg, IL, USA, ISACA. https://securitydelta.nl/media/com_hsd/report/425/document/hcl-isaca-state-of-cybersecurity-2021-part-2.pdf

Jaeger, L. (2018). Information security awareness: Literature review and integrative framework. *Proceedings of the 51st Hawaii International Conference on System Sciences*.

Kasprzyk, D., Montaño, D. E., & Fishbein, M. (1998). Application of an integrated behavioral model to predict condom use: A prospective study among high hiv risk groups1. *Journal of Applied Social Psychology*, *28*(17), 1557–1583. https://doi.org/10.1111/j.1559-1816.1998.tb01690.x

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' information security awareness and behavior: A literature review. *2013 46th Hawaii International Conference on System Sciences*, 2978–2987. https://doi.org/10.1109/HICSS.2013.192

Moletsane, T., & Tsibolane, P. (2020). Mobile information security awareness among students in higher education : An exploratory study. *2020 Conference on Information Communications Technology and Society (ICTAS)*, 1–6. https://doi.org/10.1109/ICTAS47918.2020.233978

Montaño, D. E., & Kasprzyk, D. (2008). Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. In K. Glanz, B. K. Rimer, & K. Viswanath (Eds.), *Health behavior and health education. theory, research and practice. 4th edition* (pp. 67–96). Jossey-Bass.

Nasir, A., Arshah, R. A., & Ab Hamid, M. R. (2017). Information security policy compliance behavior based on comprehensive dimensions of information security culture: A conceptual framework. *Proceedings of the 2017 International Conference on Information System and Data Mining - ICISDM '17*, 56–60. https://doi.org/10.1145/3077584.3077593

Ng, B.-Y., Kankanhalli, A., & Xu, Y. ((2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (hais-q): Two further validation studies. *Computers & Security*, *66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

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

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Schütz, A. E. (2018). Information security awareness: It's time to change minds! *Proceedings of International Conference on Applied Informatics Imagination, Creativity, Design, Development - ICDD 2018*.

Schütz, A. E., Weber, K., & Fertig, T. (2020). Assessing the information security awareness of university students. *PACIS 2020 Proceedings*. https://aisel.aisnet.org/pacis2020/54

Simonet, J., & Teufel, S. (2019). The Influence of Organizational, Social and Personal Factors on Cybersecurity Awareness and Behavior of Home Computer Users. In G. Dhillon, F. Karlsson, K. Hedström, & A. Zúquete (Eds.), *ICT Systems Security and Privacy Protection* (pp. 194–208). Springer International Publishing. https://doi.org/10.1007/978-3-030-22312-0_14

Sniehotta, F. F., Schwarzer, R., Scholz, U., & Schüz, B. (2005). Action planning and coping planning for long-term lifestyle change: Theory and assessment. *European Journal of Social Psychology*, *35*(4), 565–576. https://doi.org/10.1002/ejsp.258

Straub, D. W. (1990). Effective is security: An empirical study. *Information Systems Research*, *1*(3), 255–276. https://doi.org/10.1287/isre.1.3.255

Thompson, N., McGill, T. J., & Wang, X. (2017). "security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376–391. https://doi.org/10.1016/j.cose.2017.07.003

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), xiii–xxiii.

Yoon, C., Hwang, J.-W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, *23*(4), 407–415.