Responsible Digital Security Behaviour: Definition and Assessment Model

Clara Maathuis[1] and Sabarathinam Chockalingam[2]
[1]Open University of the Netherlands, Heerlen, Netherlands
[2]Institute for Energy Technology, Halden, Norway
clara.maathuis@ou.nl
sabarathinam.chockalingam@ife.no

Abstract: Digital landscape transforms remarkably and grows exponentially tackling important societal challenges and needs. In the modern age, futuristic digital concepts are ideated and developed. These digital developments create a diverse pallet of opportunities for organizations and their members like decision makers and financial personnel. Simultaneously, they also introduce different factors that influence users' behaviour related to digital security. However, no method exists to determine whether users' behaviour could be considered responsible or not, and in case this behaviour is irresponsible, how it could be managed effectively to avoid negative consequences. Thus far, no attempt was made to investigate this to the best of our knowledge. Then this research aims to: (i) introduce 'responsible digital security behaviour' notion, (ii) identify different factors influencing this behaviour, (iii) design a Bayesian Network model that classifies responsible/irresponsible digital security behaviour considering these factors, and (iv) draw recommendations for improving users' responsible digital security behaviour. To address these, extensive literature review is conducted through technical, ethical, and social lenses in a Design Science Research approach for defining, building, and exemplifying the model. The results contribute to increasing digital security awareness and empowering in a responsible way users' behaviours and decision-processes involved in developing and adopting new standards, methodologies, and tools in the modern digital era.

Keywords: Bayesian networks, cyber security, digital governance, digital security, responsible security, security behaviour

1. Introduction

"We are all connected by the Internet, like neurons in a giant brain." (Stephen Hawking)

During each industrial revolution, the humankind experienced a transition to a new phase of giving life to old dreams and ideas manifested as discoveries that did not seem possible to materialize and further projecting them to technological developments. In the 18th century, the First Industrial Revolution brought the use of steam engines and production mechanization. In the 19th century, the Second Industrial Revolution introduced electricity use and assembly line production. In the 20th century, the Third Revolution brought increased automatization and Information and Communication Technology (ICT) systems e.g., programmable devices like computers and robots. Nowadays, in the 21st century, the Fourth Revolution implies using ICT technologies at large scale in different industries e.g. cyber-physical production-systems and digital twins (Desoutter, 2021). Accordingly, in the last decade and during the ongoing pandemic, we see digital technologies evolve/change the way we as a society function. Digital transformation has dramatically changed the way businesses build their strategies (Puriwat, W., & Tripopsakul, 2021), and encourages further innovations through large-scale efforts while generating significant benefits and opportunities (McKinsey, 2018; OECD, 2021). Nevertheless, digital technologies could pose (un)known risks experienced by (digital)agents e.g., critical infrastructure organizations in different stages/activities implying major consequences inside/outside the digital arena. Besides the importance of organizations' strategies for building/using digital means, employees' role is vital since they could represent a direct threat to organizations unintentionally e.g., improper awareness and incorrectly/insufficiently applying security mechanisms, or intentionally e.g., insider threat (Vroom & Von Solms, 2004; Lobschat et al., 2021; OECD, 2021). It is then a shared responsibility to assure that proper mechanisms are considered and applied when needed. This relates to how agents' security behaviour could be assessed and from there we can strengthen it appropriately. While security behaviour was classified by now as malicious/non-malicious, prompted/non-prompted, informed/un/mis-informed, responsive/preventive, and actual/intended (Chowdhury, Adam & Teubner, 2020), to the best of our knowledge, no attempt to assess user's digital security behaviour as responsible/irresponsible exists. This would benefit organizations to strengthen digital security awareness, training programs, and other security mechanisms. It also aims to open a research avenue on modelling and strengthening responsible digital security behaviour for scientific and practitioner communities. Hence, the following objectives are formulated:

- To introduce and define the "responsible digital security behaviour" notion.
- To identify and classify factors that influence digital security behaviour.

- To design a BN-based model that classifies digital security behaviour as responsible/irresponsible considering these factors.
- To propose recommendations for improving/make responsible users' digital security behaviour.

To achieve these objectives, multidisciplinary research is conducted merging extensive literature review with building an intelligent model following a Design Science Research approach.

The remainder of this paper is structured as follows. Section 2 addresses relevant research regarding theoretical and practical aspects. Section 3 discusses the methodological approach taken. Section 4 introduces the proposed definition. Section 5 discusses influential factors used for classifying responsible digital security behaviour building an AI model. Section 6 presents the design and implementation of the model proposed. Section 7 provides recommendations for creating/strengthening this behaviour. Conclusively, Section 8 discusses the findings and future ideas.

2. Related work

With the increase of multi-source data availability and expansion in development and use of AI in digital security, several challenges e.g., intrusion detection and impact assessment are addressed by academic and practitioner communities. Hence, we highlight below related work positioning this research in the existing body of knowledge.

For grasping and defining responsible digital security behaviour, research on understanding security behaviour, culture, or hygiene is relevant since techno-social aspects of security behaviour are considered. Accordingly, Da Veiga et al. (2020) proposed a model for information security culture, and consider that the workforce should be aware, knowledgeable, and compliant with company's policies based on mutual trust and integrity. Aligned with this, (Vroom & Von Solms, 2004) appraise that understanding employee's security behaviour is crucial in organizations and call for assessment methods. Moreover, Lobschat et al. (2021) defined corporate digital responsibility i.e., norms and values with respect to four main processes: technology creation and data capture, operation and decision making, inspection and impact assessment, and data and technology refinement. These processes are relevant for modelling digital security behaviour. Gratian et al. (2018) correlated human characteristics with cyber security behaviour intentions e.g., password generation, proactive awareness, and updating mechanisms. Regarding employees' awareness, Li et al. (2019) found that employees are aware of their company's information security policies/procedures, and the ones aware are more effective in managing security tasks than the ones not. Conceptually, AlHogail (2015) proposed a framework for developing a comprehensive information security culture in organizations, and positions responsibility as a main dimension influencing it. Moreover, Gillam & Foster (2020) consider as avoidance factors affecting cyber security behaviours labelled as risky the following: self-efficacy, perceived susceptibility, perceived severity, perceived effectiveness, and perceived cost. Vishwanath et al. (2020) defined cyber hygiene, its dimensions e.g., use backup solutions and manage social media privacy, and advance the following approach to contain it: conceptualization, measures' development, model specification, scale evaluation and refinement, and validation. We incorporate these dimensions in this research. Conclusively, OECD (2015) and OECD (2019) addressed the issue between responsibility and capacity as some actors have responsibility but lack the necessary capacity, while other actors lack responsibility but might have the capacity to tackle digital security risks and incidents.

As the digital environment makes use at large scale of intelligent techniques, the AI research domain also includes relevant studies. Thelisson, Morin & Rochel (2020) define the digital responsibility concept to account the responsibility of actors involved and propose an index for restoring trust in a data-driven economy. Along these lines, (Dignum, 2019) argues for building and using intelligent systems for/with good intentions respecting human norms and values while not producing harm. Furthermore, the author considers that responsibility is an aspect that should be considered at individual and collective level in the processes involved. This vision is incorporated in our research. Lima et al. (2014) proposed BN-based personality prediction system considering social media text using the Big Five model which classifies personality trait as: extroversion, neuroticism, agreeableness, conscientiousness, and openness to experience. Jitwasinkul et al. (2016) developed a BN model to predict/classify work behaviour (safe/at-risk) using organizational and human factors. Peng et al. (2021) developed a BN model for predicting dangerous driving behaviour using indicators like sharp acceleration and deceleration control indicator, frequent acceleration, and deceleration control indicator. These models

demonstrate BNs' potential in classification-related problems, so they are used as basis for defining model's structure.

3. Research methodology

For defining and modelling digital responsible security behaviour, this research adopts a multidisciplinary approach creating an artefact that serves social purposes objectively (Venable, Pries-Heje & Baskerville, 2017) following the Design Science Research methodology (Hevner, March & Park, 2004; Peffers et al., 2007; Peffers, Tuunanen & Niehaves, 2018). The artefact represents to the best of our knowledge the first attempt in this sense, is able to justify its design choices i.e., is a transparent and explainable model (Maathuis, 2022), and aims to support current/future digital security decision making processes (Offermann et al., 2009; Peffers, Tuunanen & Niehaves, 2018) related to assessing digital security behaviour and awareness. Accordingly, the following research-steps are considered:

- Problem identification and motivation: with the exponential increase in development and use of digital means and considering the role and impact that companies have/encounter from security incidents, is important to tackle the need for properly assessing through effective techniques the way how 'front soldiers' i.e., security employees behave and deal with corresponding digital security aspects, and from there classify their behaviour as responsible/irresponsible so that relevant mechanisms are adopted. Hence, extensive literature review was conducted in digital security, cyber security, AI, and behavioural science.
- Solution objectives: the aim is to define and assess responsible digital security behaviour through an intelligent model i.e., BN-model built from scratch given the existing body of knowledge.
- Design and development: the definition and model are developed and proposed.
- Demonstration: the context of the model is described through exemplification.
- Evaluation: the results are analysed and observing/experimenting with the model is discussed using future incident and employee data.
- Communication: the results obtained are disseminated through this article and presentations.

4. Responsible digital security behaviour definition

Bringing ideas to life and assure technological progress is what drives modern societies to innovate; in this 'solutionist' perspective, innovation is advancing in a relative future moment something improperly framed or unsolved not-yet innovated (Burgess et al. 2018). Transposing this into the digital domain implies addressing technological progress for tackling existing and future digital aspects while benefiting of the opportunities of intelligent techniques easily/directly deployed in this domain. Further scoping to addressing responsible digital security behaviour implies acknowledging that all stakeholders involved in building and using them should be accountable and responsible for their actions (OECD, 2015). Accordingly, while responsibility represents one of the fundamental issues tackled in philosophy and law, implies two aspects relevant to the digital domain: understanding the meaning of and understanding who holds responsibility, mentioning that responsibility should be defined always in a specific context (Thelisson, Morin & Rochel, 2020). The authors consider that responsibility relates to freedom performing actions respecting specific decisions, and that responsibility is: (i) negative - relates to acts/omissions that should not be done, and (ii) positive - relates to a moral relevant situation. Furthermore, Thelisson, Morin & Rochel (2020) distinguish between retrospective responsibility i.e., past action and prospective responsibility i.e., future action. Furthermore, both perspectives apply to digital responsibility, however the digital environment might create new types of (sub-)responsibilities. For security employees, the factors that cumulate to define their digital responsibility relate to context (e.g., organization, motivation), role, alignment with management and security policies (Thelisson, Morin & Rochel, 2020) as depicted in Section 5.

Moreover, Puriwat & Tripopsakul (2021) scrutinize that digital social responsibility is accepted as valuable strategic movement, and that corporate social responsibility 'encompasses the economic, legal, ethical, and discretionary (philanthropic) expectations that society has of organizations at a given point in time'. Liyanaarachchi, Deshpande & Weaven (2020) define corporate digital responsibility as "the set of values and specific norms that govern an organizations' judgements and choices in matters that relate specifically to digital issues". Moreover, Da Veiga et al. (2020) suggest that related concepts like cyber/information security culture show how people e.g., employees perceive security aspects/issues using organizational systems. Vroom & Van Solms (2004) stress that ideally employees follow established guidelines voluntarily, generally such a culture is

defined on assumptions on perceptions and attitudes accepted and encouraged to incorporate security characteristics. Specifically, Da Veiga & Martins (2017) reason that information security culture contains "the attitudes, assumptions, beliefs, values, and knowledge that employees/stakeholders use to interact with the organization's systems and procedures" and this changes over time. Furthermore, in different interactions, acceptable or unacceptable behaviour occurs, fact that translates in this research as classifying digital security behaviour as responsible/irresponsible.

Aligned with the abovementioned perspectives, we define responsible digital security behaviour as:

Responsible Digital Security Behaviour = the way an agent acts in relation to a digital system in a given organizational (digital) context in respect to the agreed norms, procedures, and values of agent's organization.

The elements contained are:

- *Way:* activity/action taken by an agent.
- *Agent:* individual/group of employees of an organization.
- *Digital system:* software, hardware, or communication system belonging to an organization.
- *Organizational (digital) context:* setting in which the agent exists or deals with in an organization.
- *Agreed norms, procedures, and values:* well-established and voluntarily agreed norms, procedures, and values that represent the (digital) vision of an organization that agents should respect/embed in their daily (digital)activities as agreed.

5. Influential factors

Seeing the aim of this research, we consider the approach of (Da Veiga et al. 2020; Maathuis et al., 2018) which relates security behaviour to interaction between human, technology/infrastructure, and policy factors, as discussed below, depict in Figure 1, and express in Table 1:

- *Human:* employees make several decisions given their perspective, experience, background, and organization's vision (Donalds, C., & Osei-Bryson, 2020). These decisions (in)directly impact organization's internal/external processes, reputation, and (long-term)-existence.
- *Infrastructure:* since a significant part of the digital environment has an invisible and intangible nature (De Bruijn & Janssen, 2017), its physical projections and connections interact with employees during their design, implementation, and use (AlHogail, 2015).
- *Policy:* organizations use digital security policies by establishing procedures and guidelines that should be followed by employees for effective functioning, risk management, legal compliance, and business goals achievement (Lobschat et al., 2021).

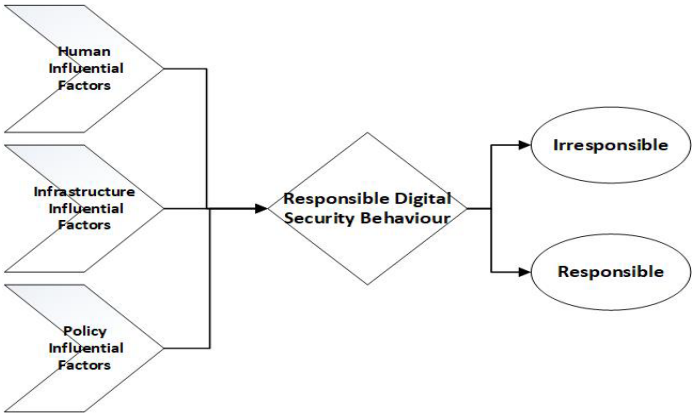

Figure 1: Influential factors

Table 1: Influential factors

Human Factors (Vroom & Von Solms, 2004; Da Veiga & Eloff, 2017; OECD, 2015; Henshel et al., 2016; FindLaw, 2018; Gratian et al., 2018; Strom, 2018; Dignum, 2019; Li et al., 2019; Trim & Lee, 2019; Chowdhury, Adam & Teubner, 2020; Da Veiga et al., 2020; Gillam & Foster, 2020; Moustafa, Bello & Maurushat, 2021)	Attitude, Motivation, Job Satisfaction, Cooperation Prior experience, Dealing with existing/similar vulnerability, Lack of knowledge/expertise Self-efficacy, Response efficacy (Un)intentional errors Time/space pressure Ethical values and conduct Decision making style: rational, avoidant, dependent, intuitive, and spontaneous Social influence, Peer behaviour, Mutual trust, Timing and manager's mood Personal traits: agreeableness, conscientiousness, neuroticism, openness, and extraversion Procrastination, Impulsivity Emotional condition, Fatigue, mood, and health Demographics, Cultural aspects (e.g., geographic, organizational, ideological expressed at individual and group levels)
Infrastructure Factors (OECD, 2015; Da Veiga & Eloff, 2007; Gratian et al., 2018; Li et al., 2019; Gillam & Foster, 2020; Vishwanath et al., 2020)	Security measures/mechanisms application Incident management Monitor software and hardware processes, Updates, Backups Device securement: locking using passwords, PINs etc., Choice of passwords, Change default passwords, Enable and use two/multi-factor authentication Proactive awareness of web content, Internet browsing using Incognito or Private mode E-mail security verification, Profile and information authenticity awareness in social media, Manage privacy settings in social media Perceived susceptibility, Perceived vulnerability, Perceived severity, Perceived effectiveness, Perceived cost
Policy Factors (Saridakis et al. 2016; Da Veiga & Eloff, 2017; Van Schaik et al. 2017; Da Veiga et al., 2020)	Security policy application/compliance Incident management Security risk management Risk perception

6. BN model structure and demonstration

This section provides a background to BNs, describes the model proposed, and demonstrates it using illustrative examples.

BNs consist of both qualitative and quantitative components (Darwiche, 2008). The qualitative component is a Directed Acyclic Graph (DAG) as in Figure 2, i.e., a set of variables and directed edges between them. The directed edges represent the cause-effect relationship between variables. Each variable has a finite set of mutually exclusive states. The quantitative component is the Conditional Probability Tables (CPTs) as in Figure 2, which includes conditional probabilities for all possible combinations of the child and parent variable states. For a variable without any parent, the CPT includes prior probabilities of the corresponding variable. This example contains two layers. The upper layer has "Pollution", "Smoking" factors/variables that increase the likelihood of a patient having lung cancer. The lower layer contains the variable which we want to query ("Lung Cancer") with evidence for variables in the upper layer. When the evidence for variables is obtained, the posterior probabilities of non-evidenced variables would be updated. This process is named belief updating, inference, or probability propagation.

BNs support four types of reasoning: predictive, diagnostic, intercausal, and combined. Predictive reasoning is from cause (e.g., smoking) to effects (e.g., lung cancer). Then, the evidence for a variable in the upper layer (cause) is provided which helps querying the posterior probabilities of non-evidenced variable in the lower layer (effect). This is relevant for our application.

BNs are used for e.g., medical decision support systems, fault diagnosis, security support. (Kahn Jr et al., 1997) built a three-layer BN (MammoNet) for breast cancer diagnosis. The upper layer contains five patient-history features, the middle layer is a target variable (breast cancer) aimed to query, and the lower layer includes two

physical findings and 15 mammographic features. Once the evidence for variables in the upper/lower layer is provided, target's posterior probability is updated. (Chockalingam et al., 2021) developed a three-layer BN that helps operators in distinguishing between attacks and faults. The upper layer has contributory factors like easy physical access to sensor, lack of maintenance. The middle layer is a target variable aimed to query. And the lower layer includes observations (or test results) e.g., the redundant sensor also sends incorrect water level measurements. Once the evidence for variables in the upper/lower layer is provided, the posterior probability of the target variable is updated.

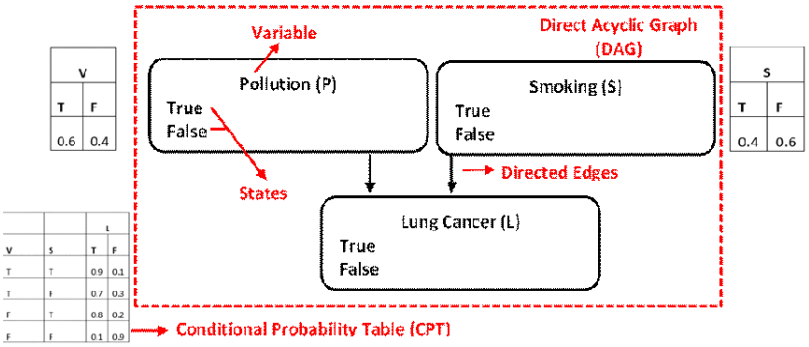

Figure 2: BN example

BNs are able to tackle our problem considering the related work plus their capability to incorporate expert knowledge and empirical data - essential in cyber security considering the well-known challenge regarding empirical data availability. Moreover, the graphical structure enhances the explainability aspect i.e., critical aspect of a model deployed. Therefore, we use BNs for modelling and consider the above-mentioned models as starting point for defining the proposed model.

Our model consists of three layers as in Figure 3. The upper layer contains factors corresponding to human, infrastructure, and policy. The middle layer has intermediate nodes (i.e., human, infrastructure, and policy) which help keeping the CPT size of the child node (i.e., the target variable) manageable using the parent divorcing technique. The lower layer embeds the target variable aimed to query with evidence for variables in the upper layer. A subset of factors from Table 1 is used for model development together with relationships between the considered variables ensuring the causality (cause-effect) aspect. The CPT values used are examples for demonstrating the BN-based approach in distinguishing digital security behaviour. Typically, CPTs are elicited from expert knowledge and empirical data.

We demonstrate the model on two illustrative scenarios to show its applicability. In the first scenario, the decision maker sets evidence for variables in the upper layer based on available information about the specific user/user-group (Lack of Job Satisfaction="True"; Time Pressure="True"; Monitor Processes="False"; Security Risk Management ="False"). Then, the posterior probability is computed by the model for other variables without any evidence. Figure 4 shows that user's digital security behaviour is irresponsible. This could be a scenario of a disgruntled employee. Additionally, this model could help selecting appropriate recommendations. Thus, putting in place appropriate measures to improve job satisfaction and monitor processes would help avoiding irresponsible security behaviour of the specific user/user-group.

In the second scenario, the decision maker sets evidence for variables in the upper layer based on available information about the specific user/user-group (Lack of Job Satisfaction="False"; Lack of Cyber Security Expertise="False"; Enforce Multi-Factor Authentication="True"; Security Policy Compliance="True"; Security Risk Management="True"). Then, the posterior probability is computed for other variables without any evidence. Figure 5 shows that user's digital security behaviour is responsible. This could be a scenario of a cyber security personnel. Moreover, this model could help selecting appropriate recommendations. Thusly, considering appropriate measures to reduce fatigue would help avoiding irresponsible security behaviour of the specific user/user-group.

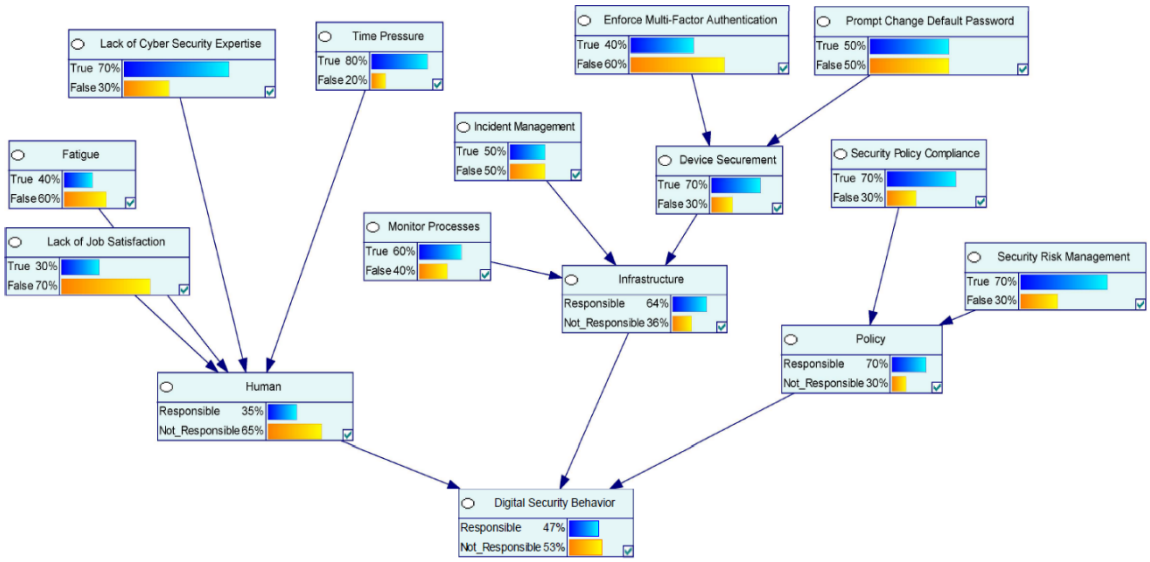

Figure 3: Developed BN model – no evidence provided

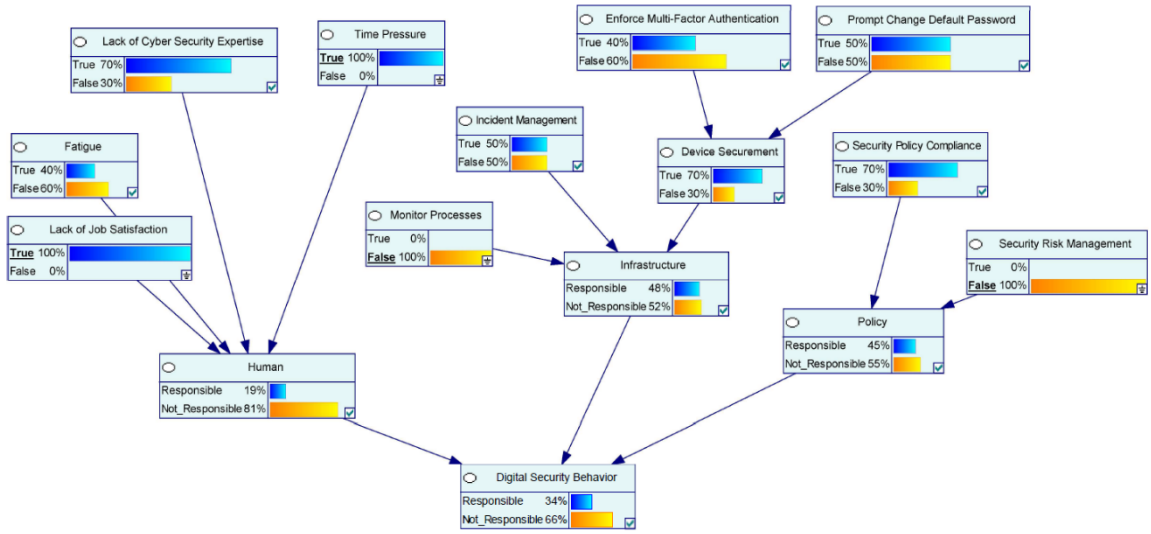

Figure 4: Developed BN model – first illustrative scenario

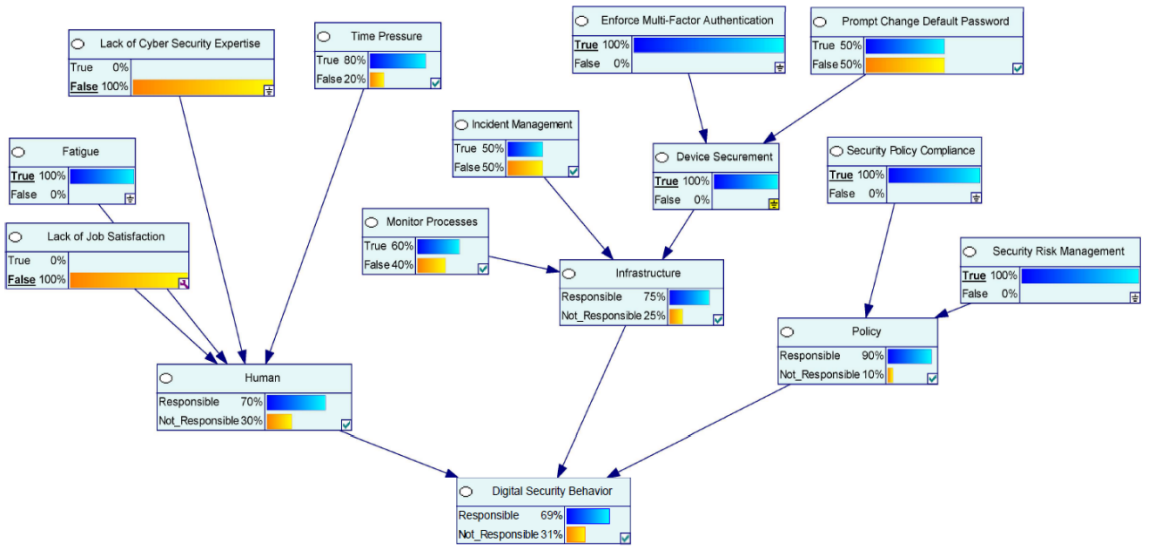

Figure 5: Developed BN model – second illustrative scenario

7. Recommendations

A model for classifying responsible digital security behaviour was introduced considering influencing factors. To facilitate model's operationalization, recommendations are considered adopting two stances: a set of recommendations that aim at controlling, limiting, or avoiding the case when irresponsible digital security behaviour is detected; and a set of recommendations that aim at supporting and strengthening when a responsible digital security behaviour is detected. The model also helps putting in place specific recommendations. To tackle both perspectives, technical-governance recommendations applicable when building and using digital technologies respecting the aspects involved in all phases of a security incident are considered. Accordingly, the following recommendations (Steen & Van de Poel, 2012; AlHogail, 2015; OECD, 2015; OECD, 2019; Alshaikh, 2020; Lobschat et al., 2021) are advised in Table 2:

Table 2: Technical and governance recommendations

Recommendation	Controlling, limiting, or avoiding irresponsible digital security behaviour	Supporting and strengthening digital security behaviour
Technical	Encourage the adoption of organization's digital security technologies, methodologies, and tools compliant with organization's policy through the use of concrete examples. Define control and advise mechanisms for tackling specific issues/factors that conduct to irresponsible behaviour.	Define challenges and competitions for tackling different digital security issues that the organization deals with.
	Design and integrate modelling and simulation environments for active learning purposes.	
Governance	Encourage and support innovation through active communication and collaboration using dedicated funds and infrastructure by merging departments and teams for well-defined and scalable shared goals. Design and implement employee's assessment and monitoring digital security metrics and solutions.	
	Build or adapt human capacity through relevant awareness campaigns, training, education, and R&D using international digital security standards, technologies, methodologies, and tools compliant with organization's digital security vision and policy. Define or upgrade explicit policies with concrete definitions of organization's norms, values, and applicable terms. Build a digital security network and hub at organizational level.	

8. Conclusions

While building the digital security field of science, several discourses and studies are conducted around facts like understanding the digital environment, grasping the potential and further development of diverse digital technologies during digital transformation, finding and combating (new)attack vectors, and managing risks through socio-technical lenses. While the resources studied provide a strong theoretical perspective on digital security challenges and opportunities, they do not focus on security employees which are in the first line in the battlefield against digital security incidents. Accordingly, in this research, the digital security behaviour of security employees is analysed through the eyes of responsibility by structuring factors that facilitate its classification as responsible/irresponsible. Moreover, a series of technological and governance recommendations are provided for controlling or avoiding irresponsible digital security behaviour and strengthening the responsible digital security behaviour. We do this through extensive literature review and building a novel Bayesian Belief Network model following a Design Science Research approach.

This research continues by advancing the proposed model considering additional dimensions that allow extending the variables and relationships, and conducting case studies on digital security incidents and users' behaviour in organizations with scientific and industry experts for operationalizing the model by capturing useful data and draw relevant socio-technical recommendations for controlling and strengthening digital security behaviour which contributes to a more responsible, accountable, and trustable digital environment.

References

AlHogail, A. (2015). Design and validation of information security culture framework. Computers in human behavior, 49, 567-575.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003.

Baskerville, R., Baiyere, A., Gregor, S., Hevner, A., & Rossi, M. (2018). Design science research contributions: Finding a balance between artifact and theory. Journal of the Association for Information Systems, 19(5), 3.

Burgess, J. P., Reniers, G., Ponnet, K., Hardyns, W., & Smit, W. (Eds.). (2018). Socially responsible innovation in security: Critical reflections. Routledge.

Chockalingam, S., Pieters, W., Teixeira, A., & van Gelder, P. (2021). Bayesian network model to distinguish between intentional attacks and accidental technical failures: a case study of floodgates. Cybersecurity, 4(1), 1-19.

Chowdhury, N. H., Adam, M. T., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. Computers & Security, 97, 101931.

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. Computers & Security. 70, 72-94. doi: 10.1016/j.cose.2017.05.002.

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers & Security, 92, 101713.

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34(1), 1-7.

Darwiche, A. (2008) Bayesian Networks, Foundations of Artificial Intelligence, vol. 3, pp. 467-509.

Desoutter (2021). Industrial Revolution – From Industry 1.0 to Industry 4.0. Available from: https://www.desouttertools.com/industry-4-0/news/503/industrial-revolution-from-industry-1-0-to-industry-4-0.

Dignum, V. (2019). Responsible artificial intelligence: how to develop and use AI in a responsible way. Springer Nature.

Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. International Journal of Information Management, 51, 102056.

FindLaw (2018). What are Legal Ethics and Professional Responsibility? Available from: https://www.findlaw.com/hirealawyer/choosing-the-right-lawyer/ethics-and-professional-responsibility.html

Gillam, A. R., & Foster, W. T. (2020). Factors affecting risky cybersecurity behaviors by US workers: An exploratory study. Computers in Human Behavior, 108, 106319.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. computers & security, 73, 345-358.

Henshel, D., Sample, C., Cains, M., & Hoffman, B. (2016). Integrating cultural factors into human factors framework and ontology for cyber attackers. In Advances in human factors in cybersecurity, pp. 123-137.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS quarterly.

Jitwasinkul, B., Hadikusumo, B. H., & Memon, A. Q. (2016). A Bayesian Belief Network model of organizational factors for improving safe work behaviors in Thai construction industry. Safety science, 82, 264-273.

Kahn Jr, C. E., Roberts, L. M., Shaffer, K. A., & Haddawy, P. (1997). Construction of a Bayesian network for mammographic diagnosis of breast cancer. Computers in biology and medicine, 27(1), 19-29.

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. Journal of Business Research, 122, 875-888.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13-24.

Lima, A. C. E., & De Castro, L. N. (2014). A multi-label, semi-supervised classification approach applied to personality prediction in social media. Neural Networks, 58, 122-130.

Liyanaarachchi, G., Deshpande, S., & Weaven, S. (2020). Market-oriented corporate digital responsibility to manage data vulnerability in online banking. International Journal of Bank Marketing.

Maathuis, C., Pieters, W. and Van Den Berg, J. (2018). A computational ontology for cyber operations. In Proceedings of the 17th European Conference on Cyber Warfare and Security, pp. 278-288.

Maathuis, C. 2022. On Explainable AI Solutions for Targeting in Cyber Military Operations. In Proceedings of the 17th International Conference on Cyber Warfare and Security. Academic Publishing.

McKinsey (2018). Unlocking Success in Digital Transformations. McKinsey & Company.

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. Frontiers in Psychology, 12.

OECD (2015). Digital Security Risk Management for Economic and Social Prosperity. OECD Recommendation and Companion Document.

OECD (2019). Policies for the Protection of Critical Information Infrastructure. No. 275. OECD Publishing.

OECD (2021). Recommendation of the Council on Digital Security of Critical Activities. OECD Legal Instruments.

Offermann, P., Levina, O., Schönherr, M., & Bub, U. (2009). Outline of a design science research process. In Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of management information systems, 24(3), 45-77.

Peffers, K., Tuunanen, T., & Niehaves, B. (2018). Design science research genres: introduction to the special issue on exemplars and criteria for applicable design science research.

Peng, Y., Cheng, L., Jiang, Y., & Zhu, S. (2021). Examining Bayesian network modeling in identification of dangerous driving behavior. PLoS one, 16(8), e0252484.

Puriwat, W., & Tripopsakul, S. (2021). The impact of digital social responsibility on preference and purchase intentions: The implication for open innovation. Journal of Open Innovation: Technology, Market, and Complexity, 7(1), 24.

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102*, 320-330.

Steen, M., & Van de Poel, I. (2012). Making values explicit during the design process. *IEEE Technology and Society Magazine*, *31*(4), 63-72.

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). Mitre att&ck: Design and philosophy. *Technical report*.

Thelisson, E., Morin, J. H., & Rochel, J. (2020). AI Governance: Digital Responsibility as a Building Block. *Science*, *107*, 111.

Trim, P. R., & Lee, Y. I. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing Management*, *83*, 224-238.

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547-559.

Venable, J. R., Pries-Heje, J., & Baskerville, R. L. (2017). Choosing a design science research methodology.

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, *128*.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & security*, *23*(3), 191-198.