Computers & Security 97 (2020) 101970

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

An application and empirical test of the Capability Opportunity Motivation-Behaviour model to data leakage prevention in financial organizations

Rick van der Kleij[a,b,*], Remco Wijn[a], Tineke Hof[a]

[a] Human Behavior and Organisational Innovations, TNO, P.O. Box 23, 3769 ZG Soesterberg, the Netherlands
[b] Cybersecurity & SMEs Research Group, The Hague University of Applied Sciences, P.O. Box 13336, 2501 EH The Hague, the Netherlands

ARTICLE INFO

Article history:
Received 24 January 2020
Revised 23 June 2020
Accepted 16 July 2020
Available online 17 July 2020

Keywords:
Security behaviour
Human vulnerability
Compliance
Information assurance
COM-B

ABSTRACT

It is widely agreed that technology alone cannot prevent cyber incidents. Organizations often need to rely on the cooperation of employees, for instance to report cyber incidents and to follow security policies. This research article presents a model of how the psychological constructs capability, opportunity and motivation interact to produce employee security behaviours that are assumed to help prevent data leakage incidents. To validate this model we surveyed 384 bank employees about their data leakage prevention behaviour. Results generally show that capability (i.e., knowledge) is uniquely related to data leakage prevention behaviour, and that motivation and opportunity are uniquely related to capability. Our findings suggest that although knowledge is pivotal for achieving desired behaviour, increasing motivation and opportunity may be key to influence knowledge acquiring and consequently data leakage prevention behaviour. Implications for information security practice are discussed.

Introduction

For financial institutions in the Netherlands, in the first half of 2018 alone, 2736 data leakage incidents were reported to the authority responsible for data leakage prevention, the Dutch Data Protection Authority (2020). The number of incidents has more than doubled since 2017 and appears to be the continuation of an ongoing trend. A wide range of risks may lead to data leakage. According to the Dutch Data Protection Authority, in 86 percent of the cases that were reported in 2018, disclosure of information originated from inside the organization, caused by employees (see also, Wong et al., 2019). More than two-thirds (63%) of these cases involve personal data, such as name and address data, payroll data or citizen service numbers, sent to an incorrect recipient.[1]

Data leakage incidents are a large problem for any organization, but particularly for financial institutions, as a nation's critical infrastructure. Data leakage may lead to reputational damage, declining trust, and direct and indirect financial costs. For instance, the banking group Capital One faced a major data leak in 2019, which led to a 6% drop in their share price as a sign of reputational damage and reduced trust, and an incremental cost of $100 million to $150 million to cover customer notifications, credit monitoring, technology costs and legal support (AON, 2020; Lu, 2019). Because of these massive consequences, financial institutions are adopting sophisticated, technical Data Leakage Prevention (DLP) solutions to manage the risks of data leakage incidents (Camillo, 2017). These solutions offer different approaches to monitor and protect confidential data. Technical measures alone, however, are often insufficient to prevent data leakage (Hauer, 2015). Because there is no technological fail-safe method to prevent leakage, organizations often need to rely on the cooperation of employees, for instance to report incidents (Shabtai et al., 2012).

The most common behavioural approaches to help prevent data leakage are information security policies and awareness campaigns (Blythe and Coventry, 2018). Information security policies describe employees' proper and prohibited behaviours and their responsibilities in preventing security incidents. Awareness campaigns usually intent to increase employees' knowledgeability on cyber risks and cyber security, so that they can better understand why and how they should comply with information security regulations. However, information security policies and awareness campaigns often have limited success for several reasons. Information security policies regularly conflict with employees' productivity goals (Beautement et al., 2008; D'Arcy and Teh, 2019). For example, a

* Corresponding author.
E-mail address: rick.vanderkleij@tno.nl (R. van der Kleij).

[1] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-ontvangt-bijna-21000-datalekken-2018

https://doi.org/10.1016/j.cose.2020.101970
0167-4048/

high demand or pressure on employees to get things done may lead them to bypass procedures or adopt less secure but more productive behaviours (Kirlappos et al., 2015).

Limited success of awareness campaigns is often a result of incorrect assumptions about why people do or do not behave securely (Bada and Sasse, 2014; Blythe and Coventry, 2018; see also Bullée et al., 2016). For instance, awareness campaigns are launched from the assumption that knowledge on cyber security is lacking amongst employees while in fact other factors are causing non-compliance with policy, such as neutralization techniques (i.e., rationalizations to condone one's own undesirable behaviours; Siponen et al., 2020), or a reluctance to relinquish personal security routines, even when a viable or better substitute is offered (Renaud et al., 2019). But maybe most importantly, the focus on awareness neglects other aspects relevant to behaviour, such as motivation and opportunity.

A big challenge for organisations to develop effective behavioural approaches to help prevent data leakage is a sound quantification of behaviours and underlying components that relate to data leakage prevention. A review by the European Union Agency for Network and Information Security (ENISA; 2018) shows that most companies consider collecting cyber security metrics as challenging, especially given the lack of universally accepted measures of desirable behaviours. And many organizations do not collect metrics at all. Moreover, when metrics are collected, often only the net incident results are collected, such as number of tickets related to data leakage incidents, audit results, responses to tests, such as phishing tests, or performance metrics, such as number of staff trained (ENISA; 2018; for a library of cyber resilience metrics, see Kerkdijk, 2017). Behaviours that precede data leakage incidents and the sources of these behaviours are often not explicated or neglected (Vishwanath et al., 2020). As a result, these net incident results fail to provide insights in the underlying causes of data leakage.

We use the Capability Opportunity Motivation-Behaviour (COM-B) model to acquire insights into the underlying causes of data leakage prevention and adopt operationalisations of the specific elements from the Theoretical Domains Framework (TDF) (Huijg et al., 2014; Atkins et al., 2017). The COM-B model states that people's behaviour can be explained by their capabilities, opportunities, motivations and the interaction between these components (Michie et al., 2014, 2011). Capability is defined as the individual's psychological and physical capacity to engage in the activity concerned. It includes having the necessary knowledge and skills. Opportunity is defined as all the factors that lie outside the individual that make the behaviour possible or prompt it. Examples of opportunity are the availability of technical or social support. Motivation is defined as all those brain processes that energize and direct behaviour, not just goals and conscious decision-making. It includes habitual processes, emotional responding, as well as analytical decision-making. We posit that these very specific insights into why employees behave as they do are needed to develop effective strategies that actually influence employee data leakage prevention behaviour. The TDF has been presented as a refinement of the COM-B model (Cane et al., 2012; Michie et al., 2014), providing a more granular understanding of capability, opportunity and motivational processes.

An important reason to utilize the COM-B model to understand data leakage prevention behaviours of banking employees is that it is part of a larger framework aimed at developing behaviour change interventions: The Behaviour Change Wheel (Michie et al., 2011, 2014). This means that the COM-B model holds the power to link interventions to the outcomes of behavioural analysis. In the context of cyber security, the framework could serve the need for more 'fit for purpose interventions' to effectively support data leakage prevention from a behavioural perspective (Van der Kleij and Leukfeldt, 2019). A clear understanding of antecedents of desirable security behaviours should help financial organizations to assess and improve weaknesses or aspects of capabilities, opportunities and motivations regarding data leakage. Consequently, this should enable financial organizations to develop effective interventions to prevent data leakage behaviours amongst employees, and to assess the effects of behaviour change interventions, such as redesign of security measures, aimed at improving cyber safety and data leakage prevention at the individual employee level.

Present research

The present research has two goals. First, in spite of clear rules and regulations and awareness campaigns, data leakage incidents show that the reasons and psychological mechanisms behind non-compliance in relation to data leakage prevention are thus far not fully understood. In order to develop effective measures to prevent data leakage incidents, a better understanding of the antecedents of compliance is essential (Wong et al., 2019). This research article aims to contribute to a better understanding of reasons and psychological mechanisms behind employee data leakage prevention behaviours. We examine how capability, opportunity, and motivation interact to enable security behaviours related to data leakage incidents.

The second goal supports the first. That is, we specify and operationalize employee data leakage prevention behaviours and employees' capabilities, opportunities and motivations for doing so, and create reliable scales to measure those. This is a necessary step in order to assess and counter data leakage incidents and promote alternative, cybersecure behaviours (see also, Stanton et al., 2005). However, organisations often differ from each other at the level of specific behaviours for employees to follow or to avoid in order to prevent data leakage. We aimed to harmonize desirable behaviours across the Dutch banking sector, beyond compliancy behaviours.

In the remainder of this research article we describe the measuring method for behaviours and underlying components that relate to data leakage prevention. We then present our research findings and conclude with a discussion of the implications of our work and provide directions for future research on the topic of data leakage prevention.

Method

Participants

A total of three hundred and eighty-four employees of two banking organisations in The Netherlands participated in our study.[2] The first bank is a global bank with over 50,000 employees that serve around 38.4 million customers, corporate clients and financial institutions in over 40 countries. Approximately 200 employees of two departments within this bank were asked to participate via email by their manager. A total of 124 employees within this bank completed the survey. The second bank has offices in 15 countries, most of which are based in the Netherlands. Nearly 2000 employees of one department within this bank were asked to participate via a general monthly newsletter. In total 260 employees completed the survey within this bank. Participants of the first bank were invited by an email from their manager, and participants from the second bank were invited through a general invitation in an online newsletter to participate and anonymously fill out a questionnaire related to data leakage prevention. The email contained a link to the questionnaire hosted on an external server.

[2] We did not ask for participants' age, sex or other demographic characteristics in the questionnaire for brevity reasons.

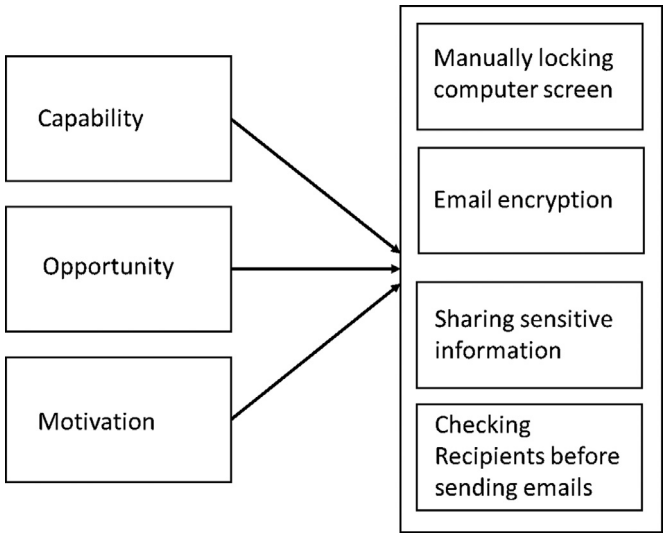

Fig. 1. Framework of employee behaviours within financial organizations related to preventing data leakage, including causes underlying these behaviours.

Procedure

In order to harmonize desirable behaviours across the Dutch banking sector we analysed information security codes of conduct of financial organizations, norms and standards, such as the ISO/IEC 27,002 information security standard, and cyber safety frameworks. We also studied the general literature on cyber security behaviour to identify security behaviours in the context of data leakage prevention. We subsequently held in-depth interviews with middle-level bank managers and employees to help us refine the anticipated employee data leakage prevention behaviours. This led to four specific and generally agreed top priority employee behaviours to prevent data leakage. Specifically, these were:

(1) Manually locking the computer screen when leaving the computer;
(2) Encrypting sensitive information before sending it out via email to external recipients;
(3) Sharing sensitive information with authorized entities only; and
(4) Checking recipients before sending out emails.

To measure capability, opportunity and motivation for these data leakage prevention behaviours we selected and adapted relevant items from the TDF-based questionnaire developed by Huijg et al. (2014). The research by Huijg et al. (2014) covered 14 domains: Knowledge, Skills, Social/professional role and identity, Beliefs about capabilities, Optimism, Beliefs about consequences, Reinforcement, Intentions, Goals, Memory, attention and decision processes, Environmental context and resources, Social influences, Emotion and Behavioural regulation.

Based on findings from our interviews with financial organisation representatives and the literature we focussed on the domains Knowledge, Social/professional role and identity, Beliefs about capabilities, Beliefs about consequences, Intentions, Memory, attention and decision processes, Environmental context and resources, Social influences, and Goals. The domains Knowledge and Memory, attention and decision processes map on the capability construct, the domains Environmental context and resources and Social influences map on the opportunity construct and Social/professional role and identity, Beliefs about capabilities, Beliefs about consequences, Intentions, and Goals map on the motivation construct of the COM-B model (Atkins et al., 2017). Fig. 1 shows our framework demonstrating how the psychological constructs capability, opportunity and motivation relate to employee security behaviours that are assumed to help prevent data leakage incidents.

In total, we constructed sixteen items for each data leakage prevention behaviour to measure the capability, opportunity, motivation, and behaviour constructs. The first item assessed the incidence with which the participant performed this behaviour (e.g., "I encrypt sensitive information before sending it out via email to external recipients") on a five point Likert-type scale (1 = *never*, 2 = *rarely*, 3 = *sometimes*, 4 = *often*, and 5 = *always*). Further, three items measured capability, three opportunity and nine items measured motivation. These items were presented as statements and responses were recorded on five-point Likert scales (1 = *strongly disagree*; 5 = *strongly agree*; see Table 1). The complete questionnaire consisted of four blocks of 16 questions each. This amounted to a total of sixty-four items for each respondent. To avoid order bias in the questionnaire, the four blocks of items relating to data leakage prevention behaviours were presented to the respondents in random order.

Results

The departments of both banks that participated were selected based on similarities in their work. None of the analyses yielded significant differences between results of the two banks. We therefore discuss the aggregated results.

Reliability

To test whether the items measuring the four data leakage prevention behaviours are systematically and reliably related, and thus could constitute an overarching scale for data leakage prevention behaviour, we calculated Cronbach's alpha as a measure of internal reliability. We found a low internal consistency ($\alpha = 0.25$). Dropping one or two items from this analysis did not improve internal consistency. We conclude that the four behaviours are not related constructs and further analyses are performed on the separate data leakage prevention behaviours.

For each of the four data leakage prevention behaviours we submitted the items measuring capability, opportunity, or motivation to a reliability analysis. Cronbach's alpha's for both motivation and capacity were larger than 0.70 for all of the four behaviours. For opportunity Cronbach's alpha's varied between 0.57 and 0.69, indicating low to modest reliability[3]. For the present purposes, and in light of the relatively low number of participants (note that Cronbach alpha's increase with number of participants) we found these reliabilities sufficiently high to use them to validate our model of data leakage prevention (see also, Zimbardo and Boyd, 1999).

Model validation

The means and standard deviations for COM-factors of each of the four data leakage prevention behaviours are presented in Table 2.

To test to what extent employee data leakage prevention behaviours are associated with capability, opportunity, and motivation, we submitted our data to the Qgraph package for R (Epskamp et al., 2012). Qgraph plots the variables as nodes connected by edges in a network. Edges represent partial correlations between two variables. The partial correlations between each node and all other nodes are directly related to the multiple regression coefficients of one variable when regressed on all other variables

[3] For combining items to create 1 construct, it is assumed that the Cronbach's alpha should be a minimum of .6 (Nunnally & Bernstein, 1994).

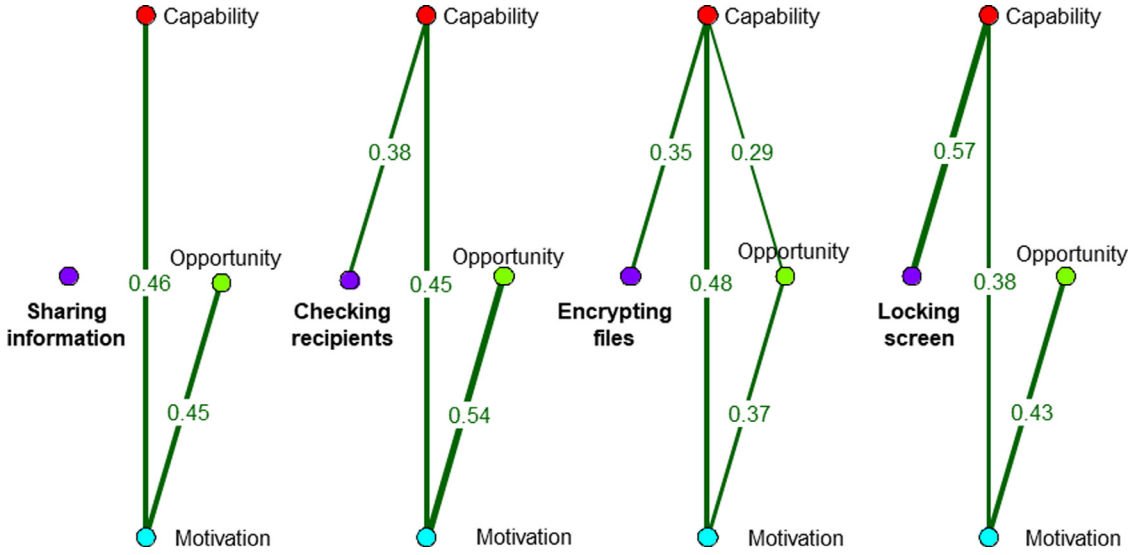

Fig. 2. Partial correlations between Capability, Opportunity, and Motivation for each of the four employee data leakage prevention behaviours: Sharing sensitive information with authorized entities only, checking recipients before emails are sent out, email encryption, and manually locking computer screen.

Table 1
Example items for measuring employee data leakage prevention behaviour: Manually locking the computer screen when leaving the computer, related Capability, Opportunity, Motivation factors, TDF domains and scoring scales. The original questions were in Dutch.

Example item to measure Behaviour:
When I leave my workstation I lock my computer: never, rarely, sometimes, often, always
Example item to measure Capability (i.e. TDF domain: Knowledge):
I know how to lock my computer screen following the guidelines: totally disagree, disagree, neutral, agree, totally agree
Example item to measure Opportunity (i.e. TDF domain: Social influences)
As far as I know, my colleagues lock their computer screen when they leave their workstations: totally disagree, disagree, neutral, agree, totally agree
Example item to measure Motivation (i.e. TDF domain: Beliefs about capabilities):
Locking my computer when I leave my workstation is easy for me: totally disagree, disagree, neutral, agree, totally agree

Table 2
Means (M) and Standard deviations (SD) for COM-B factors of each of the four data leakage prevention behaviours ($N = 384$).

Data leakage prevention behaviour:	COM-B factor:	M:	SD:
Sharing sensitive information	C	4,58	0,53
	O	4,02	0,62
	M	4,29	0,47
	B	4,85	0,53
Checking recipients	C	4,08	0,70
	O	3,92	0,63
	M	4,13	0,52
	B	4,45	0,76
Encrypting sensitive information	C	3,21	0,76
	O	3,14	0,76
	M	3,37	0,60
	B	2,57	1,50
Manually locking the computer screen	C	4,08	0,75
	O	4,15	0,67
	M	4,17	0,59
	B	4,46	0,80

in the dataset (Pourahmadi, 2011). Hence, the strength of partial correlations can be interpreted as predictive quality between two nodes. A path in the network, such as node A is connected to node B and node B is connected to node C, can be interpreted as a mediation effect of node B on the predictive quality between node A and C. Qgraph uses an adaptive LASSO penalty to estimate a sparse network in which weak relations are eliminated from the model. We adopted Qgraph rather than structural equation modelling (SEM) for this analysis because of the exploratory nature of the present analysis. Whereas SEM is useful for testing strict theories, Qgraph allows for cyclic processes and assumes no directionality of relations. As such it optimally predicts each node given all others.

Results of the analyses are presented in Fig. 2. Analyses of the questionnaire data show that for all data leakage prevention behaviours the constructs capability, opportunity, and motivation are not simultaneously and directly related to the item measuring the frequency with which participants performed this behaviour. This contrasts with what we expected based on the theorizing of Michie et al. (2011) who suggest that these constructs all directly influence the target behaviour. Rather, our analyses show that in three of the four specific behaviours, only the capability construct shares unique variance and is directly related to the item measuring behaviour. In the specific case of sharing sensitive information with unauthorised individuals, none of the proposed antecedents of behaviour seems related to that behaviour. It should be noted, however, that scores on this behavioural item are collectively high ($M = 4{,}85$; $SD = 0{,}53$) leaving little space for variance, thus potentially resulting in a ceiling effect.

For all data leakage prevention behaviours, motivation shares unique variance with capability. This may be a double-edged sword: capability (i.e., measured through knowledge on how to enact the specific behaviour) may motivate individuals such that awareness of the risks certain behaviours may pose leads to increased motivation to prevent these risks from materializing. At the same time, a coping strategy for those motivated not to become victimized may be to acquire knowledge on risks and mitigation strategies.

Also for all data leakage prevention behaviours, opportunity is not uniquely related to the behaviour items, but it is related to motivation. Speculating on the directionality of this relationship, we find it more likely that a motivation to prevent risks will lead to opportunities to prevent these risks than that the opportunity to prevent risks in itself motivates individuals to prevent them.

In other words, motivation likely leads to a search for and use of knowledge and facilities such as encryption tools, or time taken and cognitive energy awarded to perform data leakage prevention behaviours, such as double checking the correct addressing of emails, then the other way around. If this is indeed true, this means that motivation does not mediate the relationship between opportunity and capability. This implies that, for the behaviours researched here, opportunity is a redundant construct for explaining or influencing desired behaviours.

Taken together, these findings suggest that at the very least individuals need to be aware of how to enact specific data leakage prevention behaviours. Motivation is not related to behaviour directly, but its effect is mediated by capability. Although not congruent with theorizing by Michie et al. (2011), this finding does make sense from the perspective that motivation without direction does not lead to the proper actions. In other words, being motivated to prevent data leakage is only helpful insofar one knows which risks to look out for and knows how to behave more appropriately.

Importantly, the behaviours researched here all relate to data leakage prevention. Within this niche, we found small but potentially meaningful differences in relationships between the various constructs. This may point to the fact that these relationships are dependant on type of behaviour and not as ubiquitous as may be assumed.

Discussion

This research article aims to contribute to a better understanding of reasons and psychological mechanisms behind employee data leakage prevention behaviours. To this end, we specified and operationalized data leakage prevention behaviours and bank employees' capabilities, opportunities and motivations for doing so. Specifically, the behaviours we identified through literature review and interviews within Dutch banks were: (1) Manually locking the computer screen when leaving the computer; (2) Encrypting sensitive information before sending it out via email to external recipients; (3) Sharing sensitive information with authorized entities only; and (4) Checking recipients before sending out emails. We created reliable scales to measure capability, opportunity and motivation for explaining these data leakage prevention behaviours, and set out a questionnaire within two Dutch banks to test our proposed model.

The present research study shows that the four specific data leakage prevention behaviours we identified are unrelated, not construing an overarching scale of data leakage prevention. Hence, compliance on one of the four behaviours does not necessarily constitute compliance on any of the other three employee behaviours related to data leakage prevention. Further, we show that, generally, capability (i.e., knowledge) is uniquely related to data leakage prevention behaviour, and that motivation and opportunity are uniquely related to capability. These findings suggest that although knowledge is pivotal for achieving desired behaviour, increasing motivation and opportunity may be key to influence knowledge acquisition and subsequently data leakage prevention behaviour.

The finding that only capability (and not opportunity and motivation) is uniquely related to behaviour seems not in line with the COM-B model as put forth by Michie et al. (2011), which suggests that interactions between capability, opportunity and motivation are necessary conditions for the occurrence of behaviour. Possibly, specific relationships between the factors differ per behaviour, or type of behaviour (e.g., preventative or promotive actions). Current findings can be used to further examine to what extent the interaction between capability, opportunity and motivation is explained by type of security behaviours (e.g., preventative or promotive actions). For example, it may be beneficial to explore the relationship between capability, opportunity and motivation and other behaviours relevant to information security, such as password management, handling emails to prevent social engineering attempts and the use of shadow IT.

This research provides an important contribution to information security practice. First, this research provides information security professionals with greater understanding of the factors contributing to data leakage prevention within their organizations. The instrument that was developed in this study enables the development and assessment of appropriate intervention initiatives that may even be personalised, such as training programs aiming to increase specific knowledge, redesign of security measures to provide for better opportunity, or training based on principles of cognitive dissonance theory for reducing individuals' use of neutralization techniques when motivation is lacking (see, for more details on this motivational training intervention, Siponen et al., 2020).

A second practical application of the present research is to use the instrument to create foresight. An important aspect of cyber security is the ability to anticipate potential disruptions, novel demands or constraints, new opportunities, or changing operating conditions (De Boer, Bakker, Boertjes, Wilmer, Raaijmakers and Van der Kleij, 2019). Inputs that may help to develop strategic visions and anticipatory intelligence can thus be of great value to information security practice. The instrument that was developed in this study does not only offer approaches and methods to information security professionals to identify or monitor current trends in data leakage prevention from a behavioural perspective, but also to inform policy makers about relevant future developments. These developments are important to consider in policy design for sustainable strategies in cyber security, since the success of this rapidly evolving field depends on the ability to anticipate vulnerabilities, developments and potential threats. When periodically measured, the instrument allows timely responses to undesirable trends, or notice effects of interventions and external events on data leakage prevention behaviours and underlying constructs within the organizational context.

Third, the framework may aid in cultivating a data leakage prevention culture. Culture encompasses the norms a group shares about how the world operates; shaping their perceptions, thoughts, feelings and behaviours (Schein, 2010; see also, Wiley et al., 2020). An information security culture propagates cyber security behaviour that is conducive to minimising risks and that contributes to achieving the organisation's cyber security objectives (Da Veiga and Eloff, 2010; Wiley et al., 2020). Hence, it shapes employee's motivation towards the prevention of data leakage incidents in the long run (Chen et al., 2015). As such, the framework provides guidance for a mitigation strategy to cultivate a data leakage prevention culture within financial organizations, helping to shape the perceptions, thoughts, and feelings towards preventing data leakage incidents. This research is therefore important in guiding subsequent research and enabling information security professionals to provide evidence-based advice on how to foster a data leakage prevention culture in organisations.

Conclusions

This research has shown how the psychological constructs capability, opportunity and motivation interact to produce employee behaviours that are assumed to help prevent data leakage incidents within banks. Our findings suggest that capability is pivotal for preventing data leakage in financial organizations. Increasing motivation and opportunity may be key to influence capability acquisition. This research contributes to a better understanding of employee behaviours in the context of information security. We are confident that such better understanding will lead to meaningful

behavioural interventions that not only address employees' knowledgeability on cyber risks and cyber security but also motivational and opportunity aspects, and as such will contribute to an integrated effort to prevent data leakage within organizations.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Rick van der Kleij: Conceptualization, Funding acquisition, Project administration, Supervision, Visualization, Writing - review & editing, Writing - original draft, Investigation, Validation, Methodology. **Remco Wijn:** Visualization, Writing - review & editing, Writing - original draft, Investigation, Formal analysis, Methodology. **Tineke Hof:** Writing - review & editing, Writing - original draft, Investigation, Methodology.

Acknowledgments

This work was performed within a shared research programme on cyber security, in which Dutch financial institutions and TNO, partially supported by the Ministry of Economic Affairs and Climate, cooperate with the aim to innovate on cyber security. The authors gratefully acknowledge the participating banks for supporting this study. The authors also wish to thank Reinder Wolthuis and Anja Langefeld for their assistance.

References

AON (2020). Reputational damage and cyber risk go hand in hand. Retrieved from: https://www.aon.com/unitedkingdom/insights/reputational-damage-and-cyber-risk.jsp

Atkins, L., Francis, J., Islam, R., O'Connor, D., Patey, A., Ivers, N., Lawton, R., 2017. A guide to using the Theoretical Domains Framework of behaviour change to investigate implementation problems. Implement. Sci. 12 (1), 77. doi:10.1186/s13012-017-0605-9.

Bada, M., Sasse, A., 2014. Cyber Security Awareness Campaigns: why Do They Fail to Change Behavior. Global Cyber Secur. Capacity Centre. Retrieved from http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Awareness%20CampaignsDraftWorkingPaper.pdf.

Beautement, A., Sasse, M.A., Wonham, M., 2008. The compliance budget: managing security behaviour in organisations. Proceedings of the 2008 New Security Paradigms Workshop (pp. 47-58). New York, NY ACM. 10.1145/1595676.1595684.

Blythe, J.M., Coventry, L., 2018. Costly but effective: comparing the factors that influence employee anti-malware behaviours. Comput. Human Behav. 87, 87–97. doi:10.1016/j.chb.2018.05.023.

Bullée, J.W., Montoya, L., Junger, M., Hartel, P.H., 2016. Telephone-based social engineering attacks: an experiment testing the success and time decay of an intervention. Proc. Singapore Cyber-Security Conf. (SG-CRC) 107–114. doi:10.3233/978-1-61499-617-0-107.

Camillo, M., 2017. Cybersecurity: risks and management of risks for global banks and financial institutions. J. Risk Manage. Financ. Inst. 10 (2), 196–200.

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

Chen, Y., Ramamurthy, K., Wen, K.W., 2015. Impacts of comprehensive information security programs on information security culture. J. Comput. Inf. Systems 55 (3), 11–19. doi:10.1080/08874417.2015.11645767.

Da Veiga, A., Eloff, J.H., 2010. A framework and assessment instrument for information security culture. Comput. Secur. 29 (2), 196–207. doi:10.1016/j.cose.2009.09.002.

D'Arcy, J., Teh, P.L., 2019. Predicting employee information security policy compliance on a daily basis: the interplay of security-related stress, emotions, and neutralization. Inf. Manage. 56 (7). doi:10.1016/j.im.2019.02.006.

De Boer, M.H., Bakker, B.J., Boertjes, E., Wilmer, M., Raaijmakers, S., Van der Kleij, R., 2019. Text Mining in Cybersecurity: exploring Threats and Opportunities. Multimodal Technol. Interact. 3 (62), 1–15. doi:10.3390/mti3030062.

Dutch Data Protection Agency (2020). Numbers data leakage 2018. Retrieved from https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken/cijfers-datalekken-2018 24/04/2020

European Union Agency for Network and Information Security (ENISA) (2018). Cybersecurity Culture Guidelines: behavioural Aspects of Cybersecurity, available atwww.enisa.europa.eu

Epskamp, S., Cramer, A., Waldorp, L., Schmittmann, V., Borsboom, D., 2012. Qgraph: network Visualizations of Relationships in Psychometric Data. J. Stat. Softw. 48 (4), 1–18 hdl.handle.net/10.18637/jss.v048.i04.

Hauer, B., 2015. Data and information leakage prevention within the scope of information security. IEEE Access 3, 2554–2565. doi:10.1109/ACCESS.2015.2506185.

Huijg, J.M., Gebhardt, W.A., Crone, M.R., Dusseldorp, E., Presseau, J., 2014. Discriminant content validity of a theoretical domains framework questionnaire for use in implementation research. Implement. Sci. 9 (11). doi:10.1186/1748-5908-9-11.

Kerkdijk, R. (2017). Library of cyber resilience metrics. Retrieved from http://publications.tno.nl/publication/34626166/Xuq2bL/participants-2017-library.pdf

Kirlappos, I., Parkin, S., Sasse, M.A., 2015. "Shadow Security" as a tool for the learning organization. ACM SIGCAS Comput. Soc. 45 (1), 29–37. doi:10.1145/2738210.2738216.

Lu, J. (2019). Assessing The Cost, Legal Fallout Of Capital One Data Breach. Available at SSRN: https://ssrn.com/abstract=3438816. https://dx.doi.org/10.2139/ssrn.3438816

Michie, S., Van Stralen, M.M., West, R., 2011. The behaviour change wheel: a new method for characterising and designing behaviour change interventions. Implement. Sci. 6 (42). doi:10.1186/1748-5908-6-42.

Michie, S., Atkins, L., West, R., 2014. The Behaviour Change Wheel—a guide to Designing Interventions. Silverback Publishing, Great Britain.

Nunnally, J.C., Bernstein, I.H., 1994. Psychometric Theory, 3rd ed. McGraw-Hill, Inc, New York, NY.

Pourahmadi, M., 2011. Covariance estimation: the GLM and regularization perspectives. Stat. Sci. 26 (3), 369–387.

Renaud, K., Otondo, R., Warkentin, M., 2019. "This is the way 'I' create my passwords"... does the endowment effect deter people from changing the way they create their passwords? Comput. Secur. 82, 241–260. doi:10.1016/j.cose.2018.12.018.

Shabtai, A., Elovici, Y., Rokach, L., 2012. A survey of data leakage detection and prevention solutions. Springer Science & Business Media.

Siponen, M., Puhakainen, P., Vance, A., 2020. Can individuals' neutralization techniques be overcome? A field experiment on password policy. Comput. Secur. 88. doi:10.1016/j.cose.2019.101617.

Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J., 2005. Analysis of end user security behaviors. Comput. Secur. 24 (2), 124–133. doi:10.1016/j.cose.2004.07.001.

Schein, E.H., 2010. Organizational culture and leadership (Vol. 2). John Wiley & Sons.

Van der Kleij, R., Leukfeldt, R., 2019. Cyber Resilient Behavior: integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security. Proceedings of the International Conference on Applied Human Factors and Ergonomics (pp. 16-27). Springer, Cham doi:10.1007/978-3-030-20488-4_2.

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. Decis. Support Syst. 128. doi:10.1016/j.dss.2019.113160.

Wong, W.P., Tan, H.C., Tan, K.H., Tseng, M.L., 2019. Human factors in information leakage: mitigation strategies for information sharing integrity. Ind. Manage. Data Syst. 119 (6), 1242–1267. doi:10.1108/IMDS-12-2018-0546.

Wiley, A., McCormac, A., Calic, D., 2020. More than the individual: examining the relationship between culture and Information Security Awareness. Comput. Secur. 88. doi:10.1016/j.cose.2019.101640.

Zimbardo, P.G., Boyd, J.N., 1999. Putting time in perspective: a valid, reliable individual difference metric. J. Pers. Soc. Psychol. 77 (6), 1271–1288.

Dr. Rick van der Kleij is a Industrial/Organizational psychologist and expert in social aspects of cyber security. He works as a senior researcher Human Factors in Cybersecurity at the Netherlands Organisation for Applied Scientific Research. Rick is also senior researcher at the centre of Expertise Cybersecurity at The Hague University of applied sciences. His-current work focuses on cyber resiliency, cyber behaviour, and the performance of teams that are professionally involved in cybersecurity, such as Computer Security Incident Response Teams and the employees of Cybersecurity Operations Centers. Rick is convinced that behavioural aspects are key to improving cyber security within organizations and society as a whole.

Dr. Remco Wijn is a social psychologist and expert in social and behavioural aspects of physical and cyber security. He works as a researcher and consultant at the Human and Organizational Innovations research group at the Netherlands Organization for Applied Scientific Research. His-current work focusses on ways to promote cyber secure behaviour, resistance to crime, and prevention of radicalization and terrorism. On these topics, Remco Wijn has written and co-authored a range of popular and scientific articles, and offers clients valuable insights and advice.

Tineke Hof MSc holds majors in Social Psychology and Industrial/Organizational Psychology. She is currently working at TNO as a research scientist focusing on understanding and measuring human behaviour in the workplace. Her research activities are in the field of developing and evaluating tailor-made behaviour change interventions in organizations. She is also a member of the Behavioural Insights Team of the Dutch Ministry of Infrastructure and Water Management. In that role, she applies behavioural insights from social psychology research to public policy and services.