Computer Systems Science & Engineering
DOI:10.32604/csse.2022.018468
Article

Tech Science Press

Organizational Data Breach: Building Conscious Care Behavior in Incident Response

Adlyn Adam Teoh[1], Norjihan Binti Abdul Ghani[1,*], Muneer Ahmad[1], Nz Jhanjhi[2], Mohammed A. Alzain[3] and Mehedi Masud[4]

[1]Department of Information Systems, Faculty of Computer Science & Information Technology, Universiti Malaya, 50603, Kuala Lumpur, Malaysia
[2]School of Computer Science and Engineering SCE, Taylor's University, Subang Jaya, 47500, Malaysia
[3]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[4]Department of Computer Science, College of Computers and Information Technology, Taif University,Taif, 21944, Saudi Arabia
*Corresponding Author: Norjihan Binti Abdul Ghani. Email: norjihan@um.edu.my
Received: 09 March 2021; Accepted: 09 May 2021

Abstract: Organizational and end user data breaches are highly implicated by the role of information security conscious care behavior in respective incident responses. This research study draws upon the literature in the areas of information security, incident response, theory of planned behaviour, and protection motivation theory to expand and empirically validate a modified framework of information security conscious care behaviour formation. The applicability of the theoretical framework is shown through a case study labelled as a cyber-attack of unprecedented scale and sophistication in Singapore's history to-date, the 2018 SingHealth data breach. The single in-depth case study observed information security awareness, policy, experience, attitude, subjective norms, perceived behavioral control, threat appraisal and self-efficacy as emerging prominently in the framework's applicability in incident handling. The data analysis did not support threat severity relationship with conscious care behaviour. The findings from the above-mentioned observations are presented as possible key drivers in the shaping information security conscious care behaviour in real-world cyber incident management.

Keywords: End user computing; organizational behavior; incident response; data breach; computer emergency response team; cyber-attack

1 Introduction

Technology is not a cure-all. With no industry safe from information security ("InfoSec") incidents, large scale data breaches where a substantial volume of confidential data is unintentionally or purposely released to outside parties can be detrimental for an organization [1–7]. Particularly vulnerable are critical information infrastructure ("CII") deemed crucial for a nation such as those from healthcare, financial services, and government. In 2018, a cyber-attack of extraordinary significance and complexity was

carried out on the patient database of Singapore Health Services Private Limited ("SingHealth"). The data breach resulted in almost 1.5 million patient personal demographics being exfiltrated to a suspect nation state actor in which 159,000 outpatient medication details were also accessed. In particular, the country's Prime Minister's personal and outpatient medication data was specifically targeted and repeatedly accessed. Besides SingHealth, other major organizations globally have also experience breaches resulting in material privacy breaches, reputational harm and economic consequences [8]. The breach at JP Morgan Chase (a major U.S. financial services provider) in 2014 resulted in the compromise of personally identifiable information, while the 2011 Sony incident resulted in the leakage of both personal and financial data. In both incidents, over 70 million users were impacted [9,10]. The severity and complexity of the breaches faced by both companies are proportionate to that experienced by SingHealth.

A key problem for organizations is the increasing severity and scale of threats that take place. The constitution of a threat event, for instance a hostile cyber-attack, could be so elaborate that it would require connecting hundreds or thousands of data points in a multi-layered organization-wide incident handling effort [3,11–14]. Such scrutiny requires conscious care behavior, in which employees deliberate the outcomes of their actions towards their organization's security posture [15,16]. Ultimately it would be a group of people, and not an algorithm or tool, that determines if a chain of events are simply disparate incidents or a crafty effort to undermine the security of an organization [17].

To look more closely, Verizon's annual Data Breach Investigation Report showed that 68% of breaches took two months or longer to discover [18]. The lack of readiness to identify and respond to such incidents is evident. The slow response times, particularly from occurrence to discovery and containment, exists notwithstanding the fact incident response processes, security technologies, and trained staff were in place. Security readiness requires not only having the mentioned capabilities in place within the security team, but more importantly, requires a holistic, organization-wide top-down and bottom-up approach.

To this extend, several gaps were identified in existing literature. First, although human factors have been acknowledged as critical to information security [19–23], the focus has primarily been related to policy compliance [1,22,24–29] with less clarity on incident response handling. Strong incident response capabilities mark the cornerstone of a robust information security posture in an organization yet the manner that an incident response team responds to a serious data breach in large, complex organizations are not entirely known. Second, despite the large number of empirical information security research based on the theory of planned behaviour ("TPB") and protection motivation theory ("PMT"), most studies have focused on behavioral intention rather than actual behaviour [30–32]. In contrast, this work captured reported user behaviour in an actual cyber-attack through the SingHealth case study. This establishes one of the major strengths of this study and ensures a valued insight into information security. Leading to this is the review of the information security conscious care behaviour framework proposed by Safa et al. [15]. The original framework that formed the basis of the study did not review all factors that form the PMT. For instance, the factors that make up PMT's threat appraisal were not reviewed and further, only a single factor from coping appraisal was analyzed.

To address the gaps identified above, the study used a qualitative approach by way of in-depth single case study to enrich insights into data breach incident handling. Each framework factor was reviewed and subcategories within the factors were further identified and examined. By merging the different streams studied, the main research objectives of this study were:

- To identify the cause-and-effect of how information security conscious care behaviors are demonstrated during a major data breach incident handling event;
- Based on the aspects identified, to propose an enhanced information security conscious care behaviour framework;
- To empirically validate an expanded information security conscious care behaviour framework.

Data breaches are no longer an anomaly. As such, it is critical to understand how a breached organization can best manage their incident management responses to uphold customer trust and fulfil their organizational and regulatory compliance requirements.

2 Literature Review

A major theory in explaining behaviour formation is the theory of planned behaviour ("TPB"). It goes by the premise that if we plan to do something then we are more likely to do it, with intention serving as the best predictor of behaviour. The TPB, an advancement of the Theory of Reasoned Action, proposed by social psychologist Icek Ajzen [33] advances three key variables that shape intention and latterly guides behaviour. The variables are attitude, subjective norms, and perceived behavioral control. The TPB has been broadly used to support our comprehension of a diverse range behaviors, among them health-related behaviors, environmental psychology, and purchasing behaviors. In organizational behaviour research, the TPB can be particularly advantageous insomuch to be aware of how we can change the behaviour of people.

According to the TPB, first predictor of intention is behavioural attitudes. This relates to how a person thinks and feels about a behaviour and subsequently influences their expectations and assessment of the behaviour. An individual's belief of a certain behaviour makes a positive or negative contribution to someone's life. The second predictor, subjective norms, centres on everything around the individual, including group beliefs, cultural norms, and social network. The last predictor is perceived behavioral control which expresses a person's belief on how easy or hard it is to display certain behaviour or act in a certain way.

The TPB has received a fair amount of attention in information security literature [25–27,30,34]. One of the earliest studies in TPB related to information systems was Mathieson's study in 1991 when the usage of computer systems was still quite new amongst organization employees. Taylor and Todd [31] proposed a decomposed TPB to offer an improved comprehension of behaviour with the context of systems interaction. Herath and Rao [32] put forward a unified model based by expanding on Taylor and Todd's decomposed TPB and further incorporated constructs from the theories of general deterrence and protection motivation. This model examined employees' compliance intentions towards their organization's InfoSec policy. Their findings indicated that social influence and organisational commitment have a substantial influence on compliance intentions. More recently, Cuganesan et al. [30] examined informal workplace dynamics, specifically norms and senior management support, alongside formal controls in its influence towards attitudes and self-efficacy.

Together, the theory predicts that a positive attitude toward an act or behaviour, favourable social norms, and a high level of perceived behavioural control are the best predictors for forming a behavioural intention, and in turn will lead to a displayed behaviour or act. Several limitations have cropped up in which this theory does not consider a person's needs or emotions which can impact beliefs or other constructs within the model. Another argument is that behavioural intention may not necessarily lead to actual behaviour. Thus, behavioural intention is not the sole construct actual behaviour. Nonetheless, planned behaviour continues to be well applied across a multitude of studies including information security and remains a much-used theory in understanding the different predictors of intentions.

The protection motivation theory ("PMT") formulated by Rogers [35–36] initially proposed to explain fear appeals, contains four main factors which guide protection motivation and subsequently protective response. The PMT proposes that people are motivated to protect themselves based the perceived probability of the occurrence, or vulnerability, the threat severity, the response efficacy, and self-efficacy. The construct has since been expanded [36] to include two additional constructs of maladaptive rewards and response costs. PMT is a type of social cognitive model that predicts people's responses to prevent the onset of a threat. This model posits that individuals employ rational calculation when deciding about

a specific behaviour. The two appraisal processes that dictate the theory are threat and coping appraisals. The threat appraisal consists of maladaptive rewards, threat vulnerability, and threat severity, while the coping appraisal consists of response efficacy, self-efficacy, and response costs [37,38].

PMT has been used extensively in InfoSec to exhibit how policy compliance can reduce risky user behaviour [15,26,32,38,39–43]. PMT is currently one of the principal theoretical foundations used in InfoSec research to support individuals in motivating them to change their security-related behaviors to defend themselves and protect their organizations. Hanus and Wu [42] utilized threat appraisal and coping appraisal constructs in studying awareness on desktop security behaviour. Their survey found that self-efficacy and response-efficacy were noteworthy predictors of reported security behaviour. Interestingly, threat appraisals were found not to predict the behaviour related to the secure use of a desktop. Meanwhile, Aurigemma and Mattson's [39] study applied threat appraisal PMT constructs, threat vulnerability and threat severity, in observing a voluntary user action of adopting the use of a password manager to handle the issue of multiple passwords. Interestingly, they found a negative relationship between uncertainty avoidance and protection motivation.

Several studies have merged factors from several theories to form InfoSec behaviour compliance models [15,32,44]. The Herath and Rao [32] study integrated three social cognitive theories, Taylor and Todd's decomposed TPB, general deterrence theory, and PMT to study employees' policy compliance intentions. The study posited that coping appraisals of response efficacy, self-efficacy, and response costs were likely to shape InfoSec policy attitudes. Meanwhile, Ifinedo [44] proposed a security policy compliance behavioral intention model which combined constructs from PBT and PMT. This model argued that the self-efficacy factor exists in both theories, albeit with one theory using a different term, perceived behavioral control, in PBT. However, these constructs have been argued to be two distinct constructs, rather than one [45].

Safa et al. [15] proposed an information security conscious care behaviour model integrating constructs from PBT and PMT to explain compliance intention. 8 factors were studied in this model, which were InfoSec awareness, policies, experience and involvement, attitude, subjective norms, perceived behaviour, threat appraisal, and self-efficacy. The study noted all constructs apart from one, perceived behavioral control, had positive effects on the formation of InfoSec conscious care behaviour. The framework is displayed in Fig. 1 with H1 to H8 denoting the factors studied in the development of the multi theory-based model.

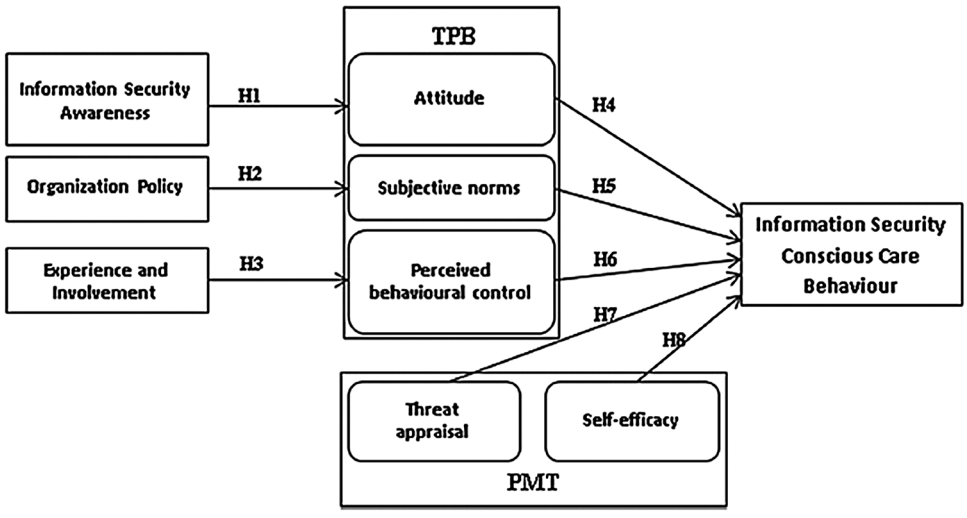

Figure 1: Information security (InfoSec) conscious care behaviour framework [15]

It is widely agreed in information security studies that positive results have been demonstrated between intention and behaviour. As such, this study believed that the literature around the TPB and PMT provided an appropriate theoretical basis for the study of incident response behaviors during a data breach within a case study setting. This study drew on the InfoSec conscious care behaviour ("ISCCB") framework proposed by Safa et al. [15] as a base. In the original framework, Safa et al. [15] grouped the threat appraisal construct as a single general factor rather than separating the elements of maladaptive rewards, threat vulnerability, and threat severity. In addition, the original framework only contained one factor from the coping appraisal category, namely self-efficacy. The factors of response efficacy and response costs were not examined. This research expanded the ISCCB framework proposed by Safa et al. [15] by incorporating all 6 factors from PMT. Tab. 1 compares the framework factors. In addition, this research applied the framework towards actual behaviors exhibited during incident response in a major cyber data breach, rather than a study of behavioral intent.

Table 1: Construct comparison between original and proposed ISCCB framework

Theory	Construct	Original ISCCB Framework [9]	Proposed ISCCB Framework
TPB	InfoSec Awareness	✓	✓
TPB	InfoSec policies	✓	✓
TPB	Experience and Involvement	✓	✓
TPB	Attitude	✓	✓
TPB	Subjective Norms	✓	✓
TPB	Perceived Behavioural Control	✓	✓
PMT	Maladaptive Rewards	✓	✓
PMT	Threat Vulnerability	✓	✓
PMT	Threat Severity	✓	✓
PMT	Response Efficacy	✗	✓
PMT	Self-Efficacy	✓	✓
PMT	Response Costs	✗	✓

3 Methodology

The aim of this qualitative case study was to gain a deeper understanding of factors that lead to employees' information security conscious care behaviour when an organization in a highly regulated industry experiences a major data breach. This entailed a thorough analysis of decision-making factors influencing choices made and causes of delayed action. Therefore, an interpretivist research paradigm allowed for interpreting realities through social constructs, paired with an understanding a phenomenon through a real-life context with the adoption of a case study methodology.

A case study of an organization from the highly regulated field of healthcare services, Singapore Health Services ("SingHealth"), was selected for understanding factors influencing conscious care behaviour. The selection of the case study was based on the requirement of data sources originating from organizations within highly regulated industries and magnitude of the breach. A six-step thematic analysis protocol [46] was used for this study (Fig. 4):

1. *Data familiarization*. The objectives for the first step were to obtain a certain degree of familiarity with the data on-hand. This involved transcribing, reading, and re-reading the data source. The first step also involved writing down first thoughts and initial ideas;
2. *Code generation*. Words and phrases were coded systematically across the whole data set, and data was collated according to the individual code;
3. *Theme search*. Codes were gathered into possible themes thus matching together all relevant data to a matching theme;
4. *Theme review*. Themes were inspected against coded extracts and complete data set, in which the output was a thematic analysis map;
5. *Theme definition and naming*: Themes were derived from the 8 constructs of the initial framework proposed by Safa et al. [15]. The remaining coding categories were based PMT constructs that was proposed to be part of the expanded framework presented in this research. Compelling extract examples can be reviewed in Appendix A—Description of Emerging Themes;
6. *Report production*. The last stage comprised of analysis of the themes and report write-up.

A thematic deduction was based on a document published by the Singapore Ministry of Communications and Information, the "Public Report of the Committee of Inquiry ("COI") into the cyber-attack on Singapore Health Services Private Limited's Patient Database in and around 27 June 2018". The process of data collection and analysis for this study was a combination of using the initial framework developed by Safa et al. [15] and a result of iterative findings from literature review and document analysis. The document analysis uncovered the meanings drawn from lived experiences of managing an information security incident. As such, a holistic understanding of the "how's" and "whys" of incident response behaviour were studied. Past studies have focused on predicting users' intention to engage in protective behaviors [30,32,47] while others have measured reported security behaviors based on survey data [42,44] or in controlled experiments [40].

4 Research Findings

SingHealth is Singapore's largest healthcare group. It encompasses of the Singapore General Hospital, KK Women's and Children's Hospital, 5 national specialty centers (Cancer, Eye, Neurosciences, Dental and Heart) and 9 primary health polyclinics. The patient electronic medical records are stored in the SingHealth Sunrise Clinical Manager ("SCM") database. The SCM database is accessed by users via Citrix Servers, which operate as an intermediary between front-end workstations and the SCM database. At the time of the occurrence, SingHealth was the owner of the SCM system and Integrated Health Information Systems Private Limited ("IHiS") was in charge of managing the system. IHiS was also responsible for executing cybersecurity measures, and security incident response and reporting.

In total, the Committee heard testimony from 37 witnesses, wherein 34 were witnesses of fact and 3 were expert witnesses. It is noted in the report that the testimony of the witnesses was presented by way of Conditioned Statements or reports, complemented by oral evidence. It is important to note that Committee of Inquiry public report contained Witness Markings (i.e., W1, W2, W3) alongside the witnesses' full name. However, as the Witness Markings were not made available for all 37 witnesses in the Public Report, this present study used a different witness marking system, namely Participant Marking (i.e., P1, P2, P3) to match against the individual's designated role for 21 individuals. Refer to Appendix B—Participant Markings in SingHealth Case Study.

The study developed a framework to demonstrate the factors contributing towards information security conscious care behaviour during an incident response event. The purpose was to understand the factors thus enabling the formation of conscious care behaviour that would lead to a timelier and considered response

during a malicious attack. Overall, the proposed InfoSec conscious care framework consists of 13 constructs. 7 constructs were derived from the original framework base while 6 new constructs were introduced, namely response efficacy, response costs, maladaptive rewards, threat vulnerability, threat severity, and communications.

To cross-validate the findings from the literature review and thematic document analysis, the draft model shown in Fig. 2 was presented and interview were conducted with four information technology and security practitioners. Their experiences ranged from 10 to 25 years and they work in large organizations that have over 10,000 employees which is of similar size to SingHealth. Thus correspondingly, the nature of information systems used within these organizations are like that of the case study—multifaceted and complex. The demographics of the interview group are presented in Fig. 3. For the purposes on ensuring reliability, the research instrument was validated by an expert panel reviewer, a senior lecturer of information systems in a national university in Malaysia.

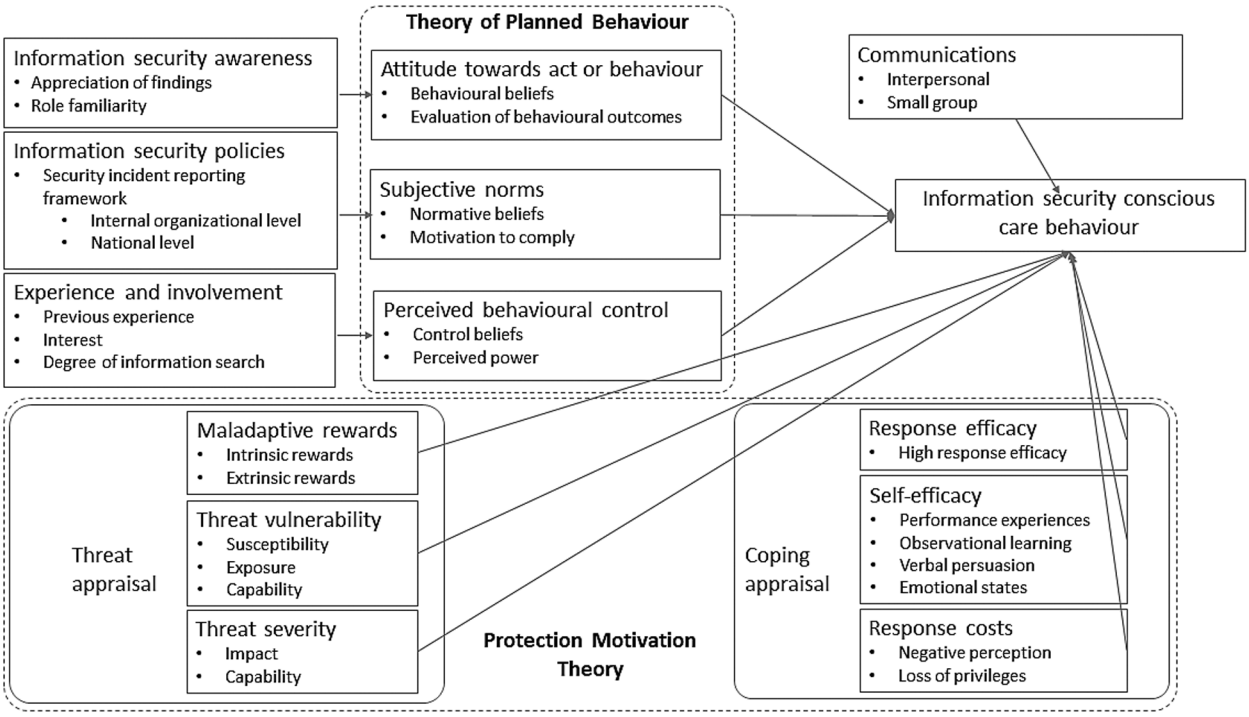

Figure 2: Information security (InfoSec) conscious care behaviour expanded draft framework

Workplace culture and communications, which emerged prominently during the thematic analysis, was initially classified as an individual new factor in the framework. Interpersonal and small-group communications in the workplace generally works in a context that is both relational and social with workplace culture shaping how individuals communicate in the context of their organization. Indeed, social influence in groups have been studied by social psychologists noted that two types of social influence exist, namely informational and normative, where group members are persuaded by the content of what they see and hear to accept an opinion [48] and where group members voice the opinion of the majority [49] respectively. These linked closely to the motivation to comply; thus, this factor sub-category was placed under subjective norms.

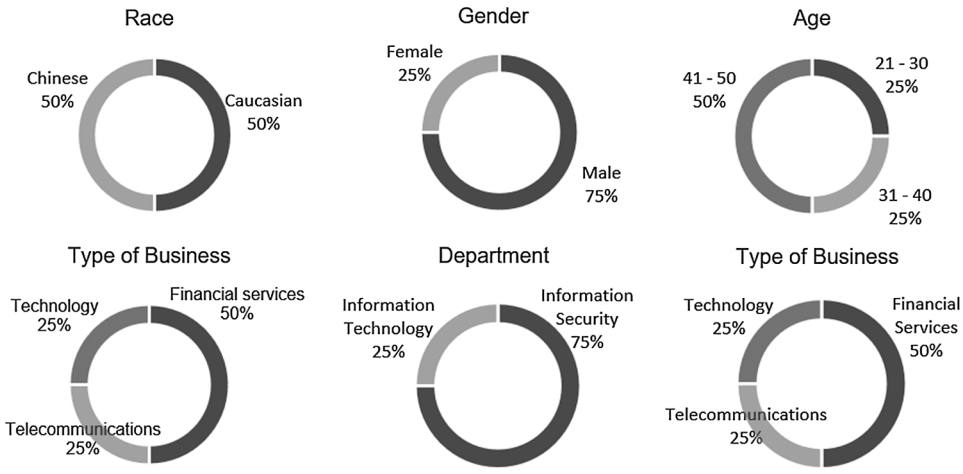

Figure 3: Demographics of interview respondents for framework validation

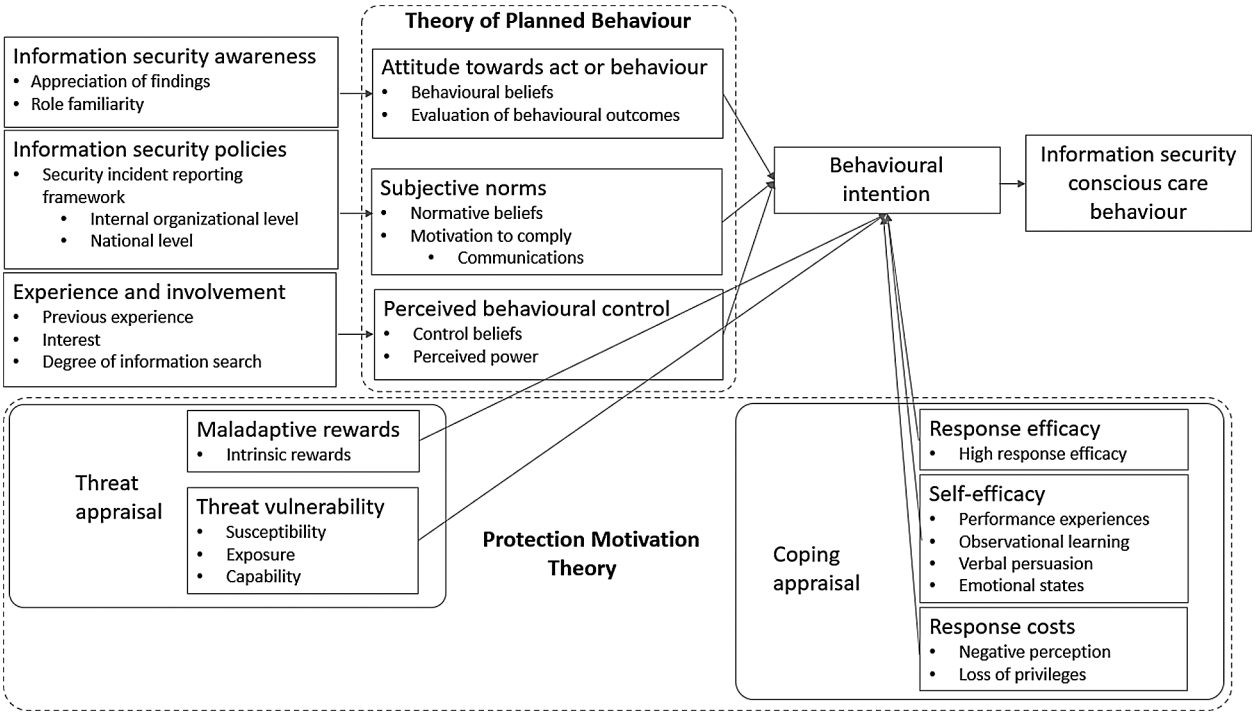

Figure 4: Information security (InfoSec) conscious care behaviour final framework

The final and revised framework is presented in Fig. 4 with the following enhancements from the base framework, (i) focus on incident response, (ii) addition of factors from the protection motivation theory, namely maladaptive rewards, threat vulnerability, threat severity, response efficacy, and response cost. (iii) expansion on each factor by examination of factor sub-categories. The potential for organizations to use the framework as a starting point to develop practical tools to use within an organization to instill information security conscious care behaviour was also acknowledged. In relation to the scope of the proposed framework, the interview respondents deemed that the framework adequately addressed the key

thrusts and foci of conscious care behaviour formation. The interview respondents also noted that the factors identified leads to behavioral intention, rather than directly towards behaviour.

It was observed that incident response timeliness can indeed be influenced by information security conscious care behaviour. If the individuals within the case study had behaved with conscious care, such as escalating the incident quicker and communicating clearly, it would have been likely that the exfiltration of patient data could have been avoided altogether. On average, it typically takes 66 days [18] for organizations to discover an incident from the time of initial occurrence. Malicious attackers often stay dormant for months while silently gaining further access prior to the actual data exfiltration.

There are some caveats that must be deliberated in understanding this present study's results. First, this study used literature review, document analysis, and thematic deduction to derive the initial draft framework. It must be noted that the document analysis and thematic development were based on the case study's single secondary source document, the publicly available COI report. As such, there are other information that we did not examine, such as the COI's confidential report that might have provided additional details. Our objective was to provide a holistic analysis, given the information currently available to the public.

Although this research observed human factors in a cyber-breach attack, it must be noted that this goes hand-in-hand with technical capabilities. In this case study, the COI report noted that "tools and technologies in place were shown to be inadequate during the cyber-attack in two respects whereby (a) callbacks to C2 (command and control) servers went undetected for months; and (b) lateral movements by the attacker through numerous systems similarly went undetected." Had the network cyber stack been enough and individual front liners displayed more security conscious care behaviour, these stages could have been interrupted or even stopped at one, or even both, of these phases.

5 Conclusion

The manner in which individuals in large organizations, in particular organizations that belong to the CII sectors, such as public healthcare institutions and financial services, respond to information security incidents have not been fully established. Past research studies have directed focus on preventative security measures and their effectiveness rather than to reactionary security measures that are used when an information security incident occurs. Consequently, there were many unanswered questions regarding the unique behavioral elements of incident response. These unanswered questions were deemed be best fulfilled by exploring the SingHealth case study as a lived experience of a malicious cyber-attack where the day-to-day incident response handling could be examined.

In conclusion, our work can guide practitioners in better understanding factors that can shape organization-wide conscious care behaviour in data breach handling. Future studies may establish framework efficacy against healthcare and other CII sectors. Necessarily, as in-depth interviews were conducted for the purpose of validating the proposed framework and not as exploratory tools, the area of framework development could also be explored and expanded.

Funding Statement: Taif University Researchers Supporting Project number (TURSP-2020/98).

Conflict of Interest: The authors declare that they have no conflicts of interest to report in the present study.

References

[1] F. Heikkila, "An analysis of the impact of information security policies on computer security breach incidents in law firms," Ph.D. dissertation. Nova Southeastern University, Florida, USA, 2009.

[2] L. Johnson, *Computer incident response and forensics team management: Conducting a successful incident response*. Waltham, MA: Elsevier, 2013.

[3] National Institute of Standards and Technology, *Computer security incident handling guide*. Washington, D.C: U.S. Department of Commerce, 2012.

[4] E. Schultz, *Incident response: A strategic guide to handling system and network security breaches*. Carmel, IN: Sams Publishing, 2001.

[5] A. Sterneckert, *Critical incident management*. Boca Raton, FL: Auerbach Publications, 2003.

[6] BakerHostetler, "2019 Data security incident response report," 2019. [Online]. Available at: https://f.datasrvr.com/fr1/119/33396/BH18098-2019_CyberReport_interactive_FINAL.pdf.

[7] J. W. Stroup, "The current mind-set of federal information security decision-makers on the value of governance: An exploratory study," Ph.D. dissertation. Capella University, Minnesota, USA, 2014.

[8] Privacy Rights Clearinghouse, "Data breaches," 2019. [Online]. Available at: https://privacyrights.org/data-breaches.

[9] N. E. Weiss and R. S. Miller, "The target and otherfinancial data breaches: Frequently asked questions," *Congressional Research Service, Prepared for Members and Committees of Congress*, vol. 4, 2015.

[10] S. Goode, H. Hoehle, V. Venkatesh and S. Brown, "User compensation as a data breach recovery action: An investigation of the Sony playstation network breach," *MIS Quarterly*, vol. 41, no. 3, pp. 703–727, 2017.

[11] A. Sterneckert, *Critical incident management*. Boca Raton, FL: Auerbach Publications, 2003.

[12] M. F. Tannian, "Business impact visualization for information security and compliance events," Ph.D. dissertation. Iowa State University, Iowa, USA, 2013.

[13] S. Roberts and R. Brown, *Intelligence-driven incident response: Outwitting the adversary*. Sebastopol, CA: O'Reilly Media, Inc, 2017.

[14] C. Skelton, *Major incident management for IT operations*. London, U.K: ITIL—Axelos, 2017.

[15] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. Abdul Ghani *et al.,* "Information security conscious care behaviour formation in organizations," *Computers and Security*, vol. 53, pp. 65–78, 2015.

[16] H. S. Rhee, C. Kim and Y. U. Ryu, "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Computers and Security*, vol. 28, no. 8, pp. 816–826, 2009.

[17] D. Rajnovic, *Computer incident response and product security.* Indianapolis, IN: Cisco Press, 2011.

[18] Verizon, "Data breach investigations report," 2018. [Online]. Available at: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf.

[19] S. Furnell and N. Clarke, "Power to the people? The evolving recognition of human aspects of security," *Computers and Security*, vol. 31, no. 8, pp. 983–988, 2012.

[20] H. W. Glaspie and W. Karwowski, "Human factors in information security culture: A literature review," in *Advances in Intelligent Systems and Computing*. Cham: Springer, pp. 269–280, 2017.

[21] S. Kraemer and P. Carayon, "Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists," *Applied Ergonomics*, vol. 38, no. 2, pp. 143–154, 2007.

[22] N. S. Safa and R. von Solms , "An information security knowledge sharing model in organizations," *Computers in Human Behavior*, vol. 57, pp. 442–451, 2016.

[23] H. Stewart and J. Jürjens, "Information security management and the human aspect in organizations," *Information and Computer Security*, vol. 25, no. 5, pp. 494–534, 2017.

[24] S. Bauer, E. Bernroidera and K. Chudzikowski, "Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks," *Computers and Security*, vol. 68, pp. 145–159, 2017.

[25] L. Cheng, Y. Li, W. Li, E. Holm and Q. Zhai, "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory," *Computers and Security*, vol. 39, pp. 447–459, 2013.

[26] P. Ifinedo, "Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition," *Information and Management*, vol. 51, no. 1, pp. 69–79, 2014.

[27] G. Moody, M. Siponen and S. Pahnila, "Toward a unified model of information security policy compliance," *MIS Quarterly*, vol. 42, no. 1, pp. 285–231, 2018.

[28] B. Netschert, "Infosec readiness and compliance in the healthcare industry," Ph.D. dissertation. Stevens Institute of Technology, New Jersey, USA, 2008.

[29] O. Santos, *Developing cybersecurity programs and policies*. London, England: Pearson Education Inc, 2018.

[30] S. Cuganesan, C. Steele and A. Hart, "How senior management and workplace norms influence information security attitudes and self-efficacy," *Behaviour & Information Technology*, vol. 37, no. 1, pp. 50–65, 2017.

[31] S. Taylor and P. A. Todd, "Understanding information technology usage—a test of competing models," *Information Systems Research*, vol. 6, no. 2, pp. 144–176, 1995.

[32] T. Herath and H. R. Rao, "Protection motivation and deterrence: A framework for security policy compliance in organizations," *European Journal of Information Systems*, vol. 18, no. 2, pp. 106–125, 2009.

[33] I. Ajzen, "The theory of planned behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, pp. 179–211, 1991.

[34] J. Bryce and J. Fraser, "The role of disclosure of personal information in the evaluation of risk and trust in young peoples' online interactions," *Computers in Human Behavior*, vol. 30, pp. 299–306, 2014.

[35] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," *Journal of Psychology*, vol. 91, no. 1, pp. 93–114, 1975.

[36] R. W. Rogers, *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation*. NY, New York: Guilford, 1983.

[37] R. W. Rogers and S. Prentice-Dunn, "Protection motivation theory," in *Handbook of Health Behavior Research I: Personal and Social Determinants, D.S. Gochman*. NY, New York: Plenum Press, 1997.

[38] S. Boss, D. Galletta, B. P. Lowry, G. Moody and P. Polak, "What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors," *MIS Quarterly*, vol. 39, no. 4, pp. 837–864, 2015.

[39] S. Aurigemma and T. Mattson, "Exploring the effect of uncertainty avoidance on taking voluntary protective security actions," *Computers and Security*, vol. 73, pp. 219–234, 2018.

[40] R. Bavel, N. Rodríguez-Priego, J. Vila and P. Briggs, "Using protection motivation theory in the design of nudges to improve online security behavior," *International Journal of Human-Computer Studies*, vol. 123, pp. 29–39, 2019.

[41] R. E. Crossler and F. Bélanger, "An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument," *Database Advances in Information Systems*, vol. 45, no. 4, pp. 51–71, 2014.

[42] B. Hanus and Y. A. Wu, "Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective," *Information Systems Management*, vol. 33, no. 1, pp. 2–16, 2016.

[43] P. Menard, G. Bott and R. Crossler, "User motivations in protecting information security: Protection motivation theory versus self-determination theory," *Journal of Management Information Systems*, vol. 34, no. 4, pp. 1203–1230, 2017.

[44] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers and Security*, vol. 31, no. 1, pp. 83–95, 2012.

[45] M. Tavousi, A. R. Hidarnia, A. Montazeri, E. Hajizadeh, F. Taremian *et al.,* "Are perceived behavioral control and self-efficacy distinct constructs?," *European Journal of Scientific Research*, vol. 30, no. 1, pp. 146–152, 2009.

[46] V. Braun and V. Clark, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, pp. 77–101, 2006.

[47] A. J. Burns, C. Posey, T. L. Roberts and P. B. Lowry, "Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals," *Computers in Human Behavior*, vol. 68, pp. 190–209, 2017.

[48] M. Sherif, "A study of some social factors in perception," *Archives of Psychology*, vol. 27, pp. 187, 1935.

[49] S. E. Asch, "Studies of independence and conformity: 1. A minority of one against a unanimous majority," *Psychological Monographs*, vol. 70, no. 9, pp. 416, 1956.