An Empirical Investigation into the Factors that Influence Employees to Report Cyber Security Incidents in the Workplace

[redacted]

This thesis is submitted in partial fulfilment of the degree of Master of Psychology (Organisational and Human Factors)

School of Psychology

The University of Adelaide

December 2022

Word Count: 7664

Author's Note: This manuscript has been prepared for the Journal of Computers & Security, which accepts all reference styles. Therefore, APA 7 style was used throughout. Excluding the cover page and general order, the manuscript has been prepared using the journal's style guidelines. The cover page is written in accordance with university examination guidelines and will be altered for publication according to the journal standards. No biographical information about the author, including contact details, is provided for examination purposes. This manuscript was completed as part of the Industry Experience Placement agreement between the University of Adelaide and the Defence Science and Technology Group.

Table of Contents

Declaration

This thesis contains no material which has been accepted for the award of any other degree or diploma in any University, and, to the best of my knowledge, contains no material previously published except where due reference is made. I give permission for the digital version of this thesis to be made available on the web, via the University of Adelaide's digital thesis repository, the Library Search and through web search engines, unless permission has been granted by the School of Psychology to restrict access for a period.

12 December 2022

Contribution Statement

XX: Topic conceptualisation, methodology, CSIRI conceptualisation, survey and data preparation, statistical analyses, thesis writing, project administration. **XX:** Topic conceptualisation, methodology, CSIRI conceptualisation, statistical analyses guidance, providing resources, supervision, project administration, writing review and editing. **XX:** Topic conceptualisation, methodology, CSIRI conceptualisation, statistical analyses guidance, providing resources, supervision, project administration, writing review and editing. **XX:** Topic conceptualisation, methodology, statistical analyses guidance, writing review and editing.

Acknowledgements

First, I wish to express my deepest gratitude to my project supervisors XXX and XXX. You're both not only kind, compassionate, and all-round incredible people, but you're also doing incredible work in the cyber security space – I really admire this. Thank you for having trust and faith in my abilities and taking me on this journey. I hope we can work together in future; I look forward to it.

Second, to XXX – thank you for being a friendly face to turn to for data and statistical analyses advice. I greatly appreciate your help – your expertise allowed me to make sense of the large amount of data in the most robust way.

Third, to my lovely friends and family and everyone else who believed me, backed me, supported me, listened to me, or sent me well wishes. Your kindness, compassion, and sensitivity kept me going.

Last, I must acknowledge my efforts. It took grit and resilience to persevere through this degree despite experiencing great hardship.

Thank you to everyone who helped me on this journey, I will forever appreciate it.

Tables and Figures

Tables

Chapter 3: Results

Figures

Chapter 1: Introduction

Abstract

Background: Cyber security incidents pose a major threat to organisations and are only increasing in sophistication to threaten their money, data, and reputation. Reporting cyber security incidents and providing organisations with information about their true nature, type, and volume, is an important strategy to inform risk-based decisions. Despite the importance of reporting cyber security incidents, little research has addressed what motivates people to do this. *Aim:* To investigate the factors that influence employees to report cyber security incidents using the Theory of Planned Behaviour as a theoretical framework. *Method:* Survey data was collected from a sample of 549 working Australian adults. Personal and organisational demographics were gathered, in addition to data using the Cyber Security Incident Reporting Inventory (CSIRI) – a Theory of Planned Behaviour survey designed for this project to look at organisational cyber security incident reporting. *Results:* It was found that attitude towards reporting, subjective norms, and perceived behavioural control each significantly predicted intention-to-report cyber security incidents. Perceived behavioural control also significantly predicted actual cyber security incident reporting behaviour. Participants were also significantly more likely to intend on reporting cyber security incidents if they were managers, identified cyber security as being either primary or related to their job, and if their organisation had a cyber security policy, regardless of whether it was formal or informal. Interestingly, the results showed that intention-to-report cyber security incidents did not predict actual cyber security incident reporting behaviour, suggesting that there may be other factors related to the cyber security context that mediated this relationship. *Conclusion:* The present study makes a unique contribution to science by investigating the factors that influence employees' to report cyber security incidents using an estabished theoretical framework. Theoretically, the results of this study validate the application of the Theory of Planned Behaviour to the cyber security incident reporting context. Practically, these findings

can be applied in organisations to inform the development of strategies that increase employees' cyber security incident reporting behaviour, such as introducing cyber security policies, as well as targeted training and development opportunities. Applying the findings can ultimately safeguard organisations from cyber-attacks, minimise the extent of damage, and prevent similar attacks from re-occurring.

Keywords: Cyber security, cyber security incident reporting, organisational incident reporting, Theory of Planned Behaviour

1. Introduction

Threats to cyber security present a major risk to organisations and recent evidence suggests that they are increasing in frequency, severity, and magnitude. Cyber security refers to the "ability to protect or defend the use of cyber space from cyber-attacks" (National Institute of Standards and Technology [NIST], n.d.). The terms 'information security' (InfoSec) and 'cyber security' are often used interchangeably. However, InfoSec refers to the protection of information and its systems more generally (NIST, n.d.). The term 'cyber security' will be exclusively used in the present study. Cyber-threats often eventuate into cyber security incidents – these are attacks that compromise the confidentiality, integrity, or availability of data (Saltzer & Schroeder, 1975). Cyber-attacks are said to present a top two social risk to society in the next decade (AXA, 2021). This attention is well-founded – in 2021, Australia saw a 13% increase of cyber-crime reports compared to the prior financial year (Australian Cyber Security Centre [ACSC], 2021). An IBM (2022) report revealed that 83% of organisations in 2022 experienced more than one data breach. Small to medium sized organisations are also at particular risk of cyber security incidents due to their lack of resources and security expertise to employ sophisticated defence strategies (Brooks, 2022).

The widespread use of technology has increased the attack surface for malicious actors – there are simply more vulnerabilities that make organisations prone to cyber-attacks, which are ultimately exploited (ACSC, 2021). For example, malicious actors tend to capitalise on external access to business-critical applications from weakened security protocols from the use of a remote workforce or under-utilising multifactor authentication methods (ACSC, 2021). In addition, the COVID-19 pandemic forced organisations to become more reliant on technology to comply with 'stay-at-home' mandates (ACSC, 2021). The pandemic prompted working arrangements that were heavily dependent on technology outside of the safety of the usual office environment, rendering both individuals and

organisations more vulnerable (Hayes et al., 2022). Further, an Ernst & Young (EY) survey revealed that 81% of executives felt that COVID-19 forced organisations to bypass cyber security processes (EY, 2021). Employees worked from either organisational or personal devices from home; however, organisations could not sufficiently control for factors such as device age or use of security measures (e.g., anti-virus software) on personal devices. Organisations could also not control for the level of physical security in remote workers' environments (Ponemon Institute, 2020). These factors not only increased the frequency of cyber security incidents, but also contributed to malicious cyber actors' success in targeting what is most important to organisations: their money, data, and reputation (ACSC, 2021).

The costs of cyber security incidents are not only substantial, but widespread. The average cost of a single data breach to an organisation is US$4.35 million (IBM, 2022), with an annual global figure expected to reach US$10.5 trillion in 2025 (Morgan, 2020). Indirect financial losses include reputational damage, loss of customer confidence, as well as theft of data and intellectual property, which can cause loss of commercial advantage over competitors (CIEHF, 2022; Morgan, 2016). Cyber security incidents within the national security sector for example, could have catastrophic effects for countries, organisations, and individuals alike (CIEHF, 2022; Harper, 2013).

Organisations traditionally rely upon technical infrastructures to mitigate risk (i.e., use of firewalls to block malicious domains; Gundu, 2019; Marques et al., 2021). However, research indicates that these measures fail to target the primary cause of cyber security incidents: human error. Despite actions being negligent or intentional, employees who do not comply with policy are the weakest link in protecting an organisation's cyber security (Schneider, 2003). To gain access to organisational networks, malicious outsiders often attempt to take advantage of employees' internal access (Gundu, 2019). Social engineering techniques are commonly employed and prompt users to perform an action, such as clicking

unsecure links or downloading files (Neria et al., 2017; Priestman et al., 2019). Verizon's 2022 Data Breach Investigations Report revealed that 82% of all cyber security incidents in the last year involved the human element – whether that be with the use of stolen credentials, phishing, misuse, or by simply making an error (Verizon, 2022). These statistics highlight the profound protective capacity that employees have for cyber security.

Research indicates that increasing users' information security awareness is an effective strategy in protecting an organisation's cyber security (Corallo et al., 2022; Grassegger & Nedbal, 2021; Lee & Kim, 2022). Increased information security awareness can prevent employees from performing unsafe actions that facilitate cyber-incidents. However, organisations are competing with the increasing sophistication of cyber-attacks. Educational tools must constantly be updated to maintain up-to-date information security awareness to combat this issue. Therefore, increasing user information security awareness as a strategy when used alone is likely to be insufficient.

A popular catchphrase within the security sector is, "*if you see something, say something*" (Homeland Security, n.d.; Lillebuen, 2014). 'Saying something' (i.e., reporting cyber security incidents) ensures that security teams are provided with accurate information about the true nature, type, and volume of incidents to make informed risk-based decisions (Humphrey, 2017). It takes 277-days on average to identify and contain a singular cyber security incident (IBM, 2022); therefore, prompt reporting can minimise the extent of damage. Reporting also allows an organisation to learn about the cause of incidents to prevent them from reoccurring in future (Grispos et al. 2014; Mitropoulos et al., 2006). Reporting cyber security incidents can mitigate risk by launching cyber security initiatives or re-educating staff and ultimately safeguard an organisation from past, present, and future cyber-attacks (Lee et al., 2016).

Despite the growing awareness of cyber security incidents among the workforce in society, organisational security teams and employees often have different priorities regarding reporting cyber security incidents to protect an organisation's cyber security. Research indicates that under-reporting of cyber security incidents is rife – Crime Survey for England and Wales data indicates that at best, 2% of computer crimes were reported in 2019 (Correia, 2022). Further, other research found that 62% of respondents believe cyber-crime is under-reported (ISACA, 2020). Therefore, it is important to understand which factors influence employees in reporting cyber security incidents. Identifying these factors can inform strategies to increase reporting behaviour to better protect organisations from cyber-attacks by making use of evidence-based practice.

To the best of our knowledge, there appears to be no prior empirical research investigating the factors associated with reporting cyber security incidents. This research aims at extending the application of Ajzen's (1985) Theory of Planned Behaviour to the cyber security context to better understand which factors influence employees to report cyber security incidents at work. Of note, the Theory of Planned Behaviour has previously been applied in research investigating the determinants of other human aspects of cyber security threats, such as phishing (Jalali et al., 2020; Shahbaznezhad et al., 2021) and general online safety behaviours (Burns & Roberts, 2013). A discussion of the theoretical background of the Theory of Planned Behaviour, its components, and associated hypotheses will be covered in the following sections.

1.1. Theoretical Underpinnings and Hypotheses Development

1.1.1. Attitude Towards Cyber Security Incident Reporting Intention

The current study uses the *attitude* construct from Ajzen's (1991; 1985) Theory of Planned Behaviour model – the first of three determinants of intention. The attitude construct relates to the degree to which a person makes positive or negative evaluations about a given

behaviour (Ajzen, 1991). These evaluations are based on a person's belief about the consequences that may arise from performing the behaviour. The theory predicts that a person is more likely to perform a behaviour if they think that doing so will lead to a positive outcome, and vice versa (Ajzen, 1991). Within the context of the present study, an employee may be more likely to report a cyber security incident if they perceive a positive outcome from doing so (e.g., promotion). On the other hand, if an employee fears any negative consequences (e.g., demotion), they may be less likely to report a cyber security incident.

Prior research has demonstrated an empirical relationship between attitude and behaviour in the cyber security field. Two studies showed that positive attitude was a significant predictor of self-reported information security awareness behaviour (McCormac et al., 2017; Parsons et al., 2017). Other research also demonstrates a strong positive relationship between attitude and intention-to-report incidents in the whistleblowing (May-Amy et al., 2020), medical (Lee et al., 2016), and social work (Xu et al., 2021) fields. Based on these results, attitude is also assumed to be an independent factor that could have a direct impact on employees' intention-to-report cyber security incidents. Therefore, the following hypothesis is proposed:

H1: Positive attitudes towards cyber security incident reporting have a positive effect on employees' cyber security incident reporting intentions.

1.1.2. Subjective Norms and Cyber Security Incident Reporting Intention

The second predictor of intention is a social factor called *subjective norm* – this refers to the perceived social pressure to perform, or avoid, a given behaviour (Ajzen, 1991). Subjective norms are a function of normative beliefs within specific behavioural contexts and influence a person's decision to perform a behaviour (Alanazi et al., 2022; Paramita et al., 2018). In the Theory of Planned Behaviour, subjective norms represent the positive or negative social pressures from peers, friends, family, or colleagues regarding the performance

of a behaviour (Ajzen, 1991). The social pressure experienced is compounded by the strength of influence as well as the person's own motivation to comply (Ajzen, 1991). If a person is strongly influenced to perform a behaviour and is motivated to comply, they are more likely to intend performing the behaviour. Within the context of the present study, this means that an employee may be more likely to report a cyber security incident if this is accepted cultural behaviour within the workplace and if they feel supported by their colleagues and supervisor to report, and vice versa.

A body of research demonstrates a positive relationship between subjective norms and behavioural intentions. Alanazi and colleagues (2022) noted that subjective norms (i.e., social influence from those considered important to the respondent) strongly influenced young adults' intentions to practice cyber security behaviours. Other research also identifies a link between subjective norms and nurses' intention-to-report medical incidents (Lee et al., 2016) and employees' intention-to-report organisational misconduct (Carpenter & Reimers, 2005; May-Amy et al., 2020; Owusu et al., 2020; Park & Blenkinsopp et al., 2009; Siallagan et al., 2017; Utami et al., 2018; Xu et al., 2021). These results highlight the strong impact of the social influence of colleagues. These findings inform the formulation of the second hypothesis:

H2: Subjective norms have a positive effect on employees' intention-to-report cyber security incidents.

1.1.3. Perceived Behavioural Control and Cyber Security Incident Reporting Intention

The third factor of the Theory of Planned Behaviour is *perceived behavioural control*. Ajzen (1991) defines this as the perceived ease or difficulty of performing a behaviour. It is also assumed to reflect both past experience and anticipated obstacles related to the behaviour in a specific context. Perceived behavioural control is determined by a person's confidence in their ability to perform a behaviour, which also depends on the resources and opportunities

available to them. Thus, perceived behavioural control has implications for a strong motivation towards intention (May-Amy et al., 2020). Therefore, the higher a person's perceived behavioural control, the more likely they are to intend performing a given behaviour (Ajzen, 1991). When applying this to the present study, perceived behavioural control relates to employees' perceived ease or difficulty of reporting cyber security incidents. Employees' confidence in reporting cyber security incidents may be affected by available resources and opportunities such as organisational cyber security policies and incident reporting protocols, use of an intuitive reporting channel, or their own prior reporting experience.

Previous research documents an empirical relationship between perceived behavioural control and behavioural intentions (Alanazi et al., 2022; Lee et al., 2016; Mansor et al., 2020; May-Amy et al., 2020; Rustiarini & Sunarsih, 2017; Tripermata et al., 2022). Rustiarini and Sunarsih (2017) noted that perceived behavioural control significantly predicted intention-to-report fraudulent accounting activity within an organisation. Here, ease or difficulty of performing whistleblowing was measured with respondents' confidence, ability, and control in reporting, as well as whether choosing to report was their own decision. Based on these findings, perceived behavioural control is also assumed to be a factor that has a positive influence on employees' intention-to-report cyber security incidents, resulting in the following hypothesis:

H3: Perceived behavioural control has a positive effect on employees' intention-to-report cyber security incidents.

1.1.4. Perceived Behavioural Control and Cyber Security Incident Reporting Behaviour

Research also suggests that perceived behavioural control can directly predict behavioural achievement (Ajzen, 1991; May-Amy et al., 2020; Rustiarini & Sunarsih, 2017). One of Ajzen's (1991) rationales behind this is that the effort expended to successfully

complete a behaviour, holding intention constant, is likely to increase with perceived behavioural control. Those confident in performing a behaviour are more likely to persevere than those who doubt their ability. If requisite resources and opportunities are available, these increase and decrease a person's confidence and doubt in their own ability, each respectively, which increases their likelihood of persevering and performing the behaviour (May-Amy et al., 2020). Within the context of the present study, the greater the resources and opportunities that employees have access to, such as cyber security policies, incident reporting protocols, intuitive reporting channels, or prior reporting experience and the fewer obstacles anticipated, the greater their actual cyber security incident reporting behaviour. Therefore, the fourth hypothesis is as follows:

H4: Perceived behavioural control has a positive effect on employees' actual reporting behaviour of cyber security incidents.

1.1.5. Cyber Security Incident Reporting Intention and Cyber Security Incident Reporting Behaviour

Intention refers to a person's motivation, willingness, and effort they are prepared to expend in performing a behaviour (Ajzen, 1991). According to the Theory of Planned Behaviour, intention is assumed to be the immediate antecedent of behaviour (Ajzen, 2006). The stronger a person's behavioural intention, the more likely they are to perform the behaviour. Intention can only find expression in behaviour if it is under volitional control, i.e., if a person can decide at will to perform the behaviour (Ajzen, 1991). Within the context of the present study, cyber security incident reporting intention refers to an employees' probability of choosing to report a cyber security incident. Meanwhile, behaviour refers to the actual behaviour of a person, and in this case, is the cyber security incident reporting action.

The evidence base for the relationship between intention and behaviour is growing. Alanazi and colleagues (2022) found that young adults' intentions to practice cyber security

behaviour had a significant positive influence on their actual cyber security behaviour. Research within the organisational misconduct field also notes a significant positive relationship between intention to whistleblow and actual whistleblowing behaviour (May-Amy et al., 2020; Rustiarini & Sunarsih, 2017). Based on these results, it is assumed that intention-to-report cyber security incidents will be directly related with actual cyber security incident reporting behaviour; thus, the following hypothesis is proposed:

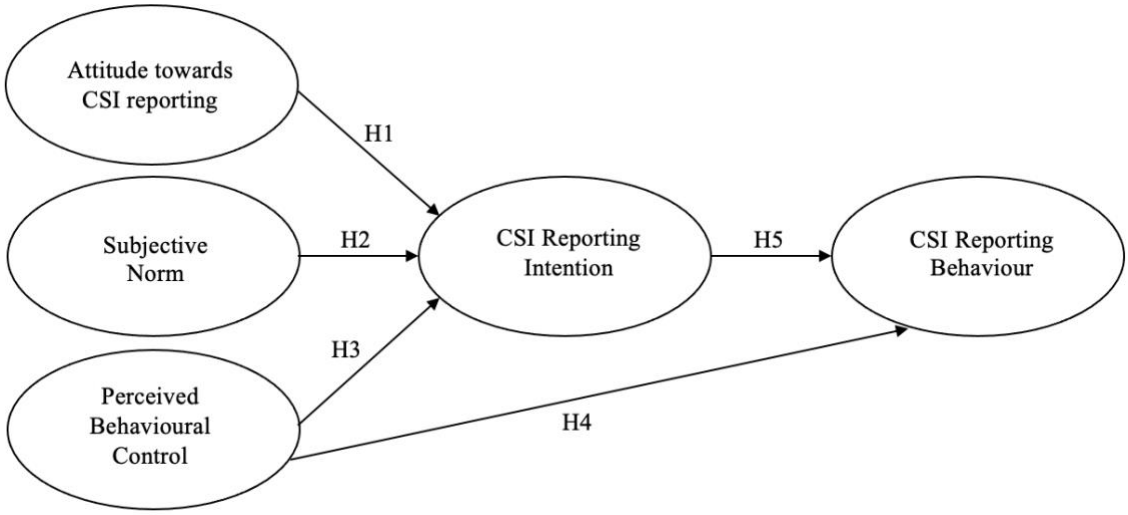
H5: Employees' intention-to-report cyber security incidents predicts their actual reporting behaviour.

1.2. Proposed Conceptual Framework

Based on the Theory of Planned Behaviour, literature review, and hypotheses formulated, a conceptual framework for this present study is proposed (Figure 1).

Figure 1

Theoretical Framework



Note. CSI: Cyber security incident

2. Method

Data collection involved use of an online survey administered through Qualtrics – a web-based survey software. Data was collected over a 6-day period. Ethics approval was granted by the Defence Science and Technology Group (DST Group) Human Research Ethics Review Panel.

2.1. Participants

Five-hundred and forty-nine working Australian adults completed the survey. Of these, 273 were female, 257 were male, 5 were non-binary, and 14 used a different term to describe their gender. Further, 24% were aged between 18 and 29 years old, 23% between 30 and 39 years, 21% between 40 and 49 years, 16% between 50 and 59 years, and 16% were aged 60 years or above.

Participants were required to be over the age of 18, currently employed, and working within Australia. To ensure data quality, participant responses were excluded if they completed the survey in less than half of the median duration of all participants (n = 28) and failed to comply with an attention check item where participants were directed to respond with, ‘Strongly Disagree’ (n = 122).

2.2. Measures

2.2.1. Demographic Information

Participants were asked to provide individual demographics, such as age, gender, and education status. Organisational demographics were also gathered and included awareness of cyber security incident reporting obligations, position level, organisational tenure, frequency of access to sensitive information, the relevance of cyber security to their job role, and whether their workplace has rules around the use of a computer and information security.

2.2.2. Cyber Security Incident Reporting Inventory (CSIRI)

The Cyber Security Incident Reporting Inventory (CSIRI) measures incident reporting intentions and behaviour specific to the cyber security field. This inventory was developed for use in the present study – no existing incident reporting scales were relevant or appropriate to cyber security.

The CSIRI is comprised of five subscales in accordance with the Theory of Planned Behaviour: (a) attitude towards reporting cyber security incidents; (b) subjective norms; (c) perceived behavioural control; (d) intention-to-report cyber security incidents; and (e) actual cyber security incident reporting behaviour.

A meta-analysis of 64 studies showed that past behaviour predicts future behaviour (Ouellette & Wood, 1998). Frequency of past behaviour may reflect habit strength and have a direct effect on future performance. Measuring actual behaviour within a cyber security reporting context provides objective data that can be extended to strongly predict future behaviour. However, we were unable to assume that an adequate proportion of the present study's sample encountered a cyber security incident at work. Therefore, intention-to-report cyber security incidents was measured in addition to actual cyber security incident reporting behaviour. This ensured that adequate data was gathered on intended or actual behaviour regardless of whether a cyber security incident had been encountered. This approach is in accordance with the Theory of Planned Behaviour, which functions on the assumption that intention predicts behavioural achievement (Ajzen, 1985; 1991). Evidence for strong intention-behaviour relationships has been observed in early research relating to the Theory of Reasoned Action (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1977), as well as more recent meta-analytic research (Webb & Sheeran, 2006).

Given the paucity of research in reporting cyber security incidents, to ensure content validity of the inventory, the items used were grounded in research from the healthcare and organisational misconduct fields. The adopted construct items were therefore, contextualised

to fit the purpose of the study. Three papers were imperative in informing the adaptation of items for use in the CSIRI (Ajzen, 2006; Lee et al., 2016; Rustiarini & Sunarsih, 2017) (Refer to Appendix A for additional details on the CSIRI including adaptation source, questions, items, and scales used). Research indicates that using a combination of positively and negatively worded items can cause respondent confusion, change the factor structure of the scale, and threaten validity and reliability of the survey instrument (Chyung et al., 2018; van Sonderen et al., 2013; Zeng et al., 2020). Therefore, positively worded items were used exclusively in the CSIRI.

Participants were asked to respond to the items on a series of different scales. Item scales were either multichotomous (i.e., yes, no, unsure), of a 'select all that apply' structure, or on a Likert scale. A 7-point bipolar scale was on all Likert items in accordance with the Theory of Planned Behaviour questionnaire construction guide (Ajzen 2006; 1985). In the intention-to-report subscale, the participants responded on a Likert scale ranging from 1 = 'Very Unlikely' to 7 = 'Very Likely'. An example item from this subscale is, *"How likely are you to report a cyber security incident that breaches the IT usage policy in your workplace?"*

The Cronbach alpha coefficients for the subscales in the CSIRI are as follows: .93 for attitude, .88 for subjective norm, .95 for perceived behavioural control, and .88 for intention-to-report. These results demonstrate high internal consistency among items within each subscale, respectively.

The CSIRI underwent cognitive testing to receive feedback on the clarity and logic of questions and items with three Master of Psychology students. These students were encouraged to 'think-aloud' when answering items to demonstrate their reasoning when identifying potential issues. The CSIRI also underwent pilot testing on six people – the feedback obtained informed the modification of some items.

3. Results

Total scores for attitude, subjective norms, perceived behavioural control, and intention-to-report were calculated by summing item scores for each respective construct. All statistical analyses were conducted using SPSS (version 28.0.0). First, descriptive statistics were calculated to provide a summary of the data and variables of interest. Second, correlation analyses were undertaken to gauge the strength and direction of relationships between variables. Third, a series of one-way between-groups Analysis of Variance (ANOVA) and post-hoc comparison tests were used to investigate the relationships between intention-to-report, attitude, subjective norm, and perceived behavioural control with the gender, cyber security policy, and organisational position level groups. Fourth, an independent samples t-test investigated the between-group differences of cyber security job relevance on the intention-to-report, attitude, subjective norm, and perceived behavioural control variables. Fifth, a multiple regression was used to assess the extent to which the independent variables predicted intention-to-report. Finally, logistic regression analyses were employed to investigate the predictive power of intention-to-report, and perceived behavioural control, on actual reporting behaviour, each respectively. An overview of the results is provided in the following sections.

3.1. Descriptive Statistics

Tables 1 and 2 present a summary of the descriptive statistics for the key variables assessed in the present study. Frequencies are reported for nominal (age, gender, policy, cyber security job relevance, position level, awareness of reporting obligations, observation of cyber security incidents, actual reporting behaviour) and ordinal (education, access to sensitive information, organisational tenure) variables, see Table 1.

Most of the sample worked as general team members (n = 274), with the remaining employed in management (n = 151), supervisory (n = 105), or other (n = 19) positions.

Comparative to the Australian population (Australian Bureau of Statistics, 2021), these sample demographics were relatively representative with the exception that participants in the 60 year or above age bracket were underrepresented. Thirty-two percent of the sample had worked at their current organisation for 2 or less years, 27% for 3-6 years, 14% for 7-10 years, and 27% for more than 10 years. Regarding the highest level of education attained, 47% of participants had either undergraduate or postgraduate degrees, 31% attended technical college or TAFE, 21% attained a Year 12 or equivalent level qualification, while 2% had completed primary school.

The majority of participants (79%) reported being aware of either formal or informal policies surrounding computer-use and information security, whilst 21% were unsure or did not believe their organisation had such policies in place. Cyber security was irrelevant to 51% of participants' job roles, but relevant to 45%, and was the primary job role of 4% of participants. Regarding participants' frequency with which they have access to sensitive information, 27% always have access, 25% often have access, 19% sometimes have access, while 29% either rarely or never have access.

Means, standard deviations, as well as minimum and maximum scores, are reported for all continuous (intention-to-report, attitude, subjective norm, and perceived behavioural control) variables, see Table 2.

Table 1

Descriptive Statistics for Key Nominal and Ordinal Variables

Variable	*n* (%)
Participants	549 (100.0)
Gender	
Male	257 (46.8)
Female	273 (49.7)
Non-binary	5 (0.9)
Different term	14 (2.6)
Age	
18-29	131 (23.9)
30-39	128 (23.3)
40-49	118 (21.5)
50-59	86 (15.7)
60+	86 (15.7)
Education	
Primary school	9 (1.6)
Year 12 or equivalent	113 (20.6)
Technical college, TAFE or equivalent	169 (30.8)
Undergraduate degree	178 (32.4)
Postgraduate degree	80 (14.6)
Have you observed a cyber security incident?	
Yes	124 (22.6)
No	425 (77.4)
Did you report the cyber security incident?	
Yes	103 (18.8)
No	21 (3.8)
Aware of reporting obligations?	
Yes	470 (85.6)
No	79 (14.4)
Position level	
Leader	151 (27.5)
Supervisor	105 (19.1)
Team member	274 (49.9)
Other	19 (3.5)
Organisational tenure (years)	
< 1	65 (11.8)
1-2	111 (20.2)
3-4	84 (15.3)
5-6	64 (11.7)
7-8	39 (7.1)
9-10	36 (6.6)
>10	150 (27.3)
Access to sensitive information frequency	
Never	72 (13.1)
Rarely	87 (15.8)
Sometimes	105 (19.1)
Often	139 (25.3)
Always	146 (26.6)
Cyber security relevance to job	
Primary	22 (4.0)
Relevant	248 (45.2)
Irrelevant	279 (50.8)
Organisational cyber security policy	
Formal	328 (59.7)
Informal	105 (19.1)
Unsure	54 (9.8)
No policy	62 (11.3)

Note. Min: minimum score; Max: maximum score

Table 2

Descriptive Statistics for Continuous Variables

Variable	Mean	SD	Min	Max
Intention-to-report	22.85	4.93	4.00	28.00
Attitude	18.93	2.54	3.00	21.00
Subjective norm	23.96	3.76	4.00	28.00
Perceived behavioural control	34.47	7.34	6.00	42.00

Note. SD: standard deviation; Min: minimum score; Max: maximum score

3.2. Correlational Analyses

Table 3 presents a correlation matrix to examine the relationships between intention-to-report, attitude, subjective norm, perceived behavioural control, age, and education status. Awareness of reporting obligations, access to sensitive information, and tenure are organisational variables that were also included in the analysis. Intention-to-report had a strong, significant relationship with the attitude, subjective norm, and perceived behavioural control variables. In addition, intention-to-report had weak positive relationships with age, access to sensitive information, and awareness of reporting obligations.

Table 3

Correlations Between Intention-to-report, Attitude, Subjective Norms, Perceived Behavioural Control, Age, Education, Access to Sensitive Information, Organisational Tenure, and Awareness of Reporting Obligations

	1	2	3	4	5	6	7	8	9
1. Intention-to-report	-								
2. Attitude	.61**	-							
3. Subjective norm	.57**	.64**	-						
4. Perceived behavioural control	.51**	.57**	.58**	-					
5. Age	.10*	.08	.07	.14**	-				
6. Education	-.02	.03	.03	.08	.00	-			
7. Access to sensitive information	.21**	.19**	.20**	.27**	-.12**	.24**	-		
8. Organisational tenure	.08	.06	.13**	.19**	.49**	.07	.04	-	
9. Awareness of reporting obligations	.17**	.20**	.26**	.36**	-.01	.17**	.21**	.00	-

Note. *p < .05 (2-tailed); p** < .01 (2-tailed)

3.3. Gender and Intention-to-report, Attitude, Subjective Norms, and Perceived Behavioural Control

A series of one-way between-group ANOVA tests were used to explore the relationships of gender, policy, and position level on intention-to-report cyber security incidents, attitude, subjective norms, and perceived behavioural control.

First, a one-way between-groups ANOVA test was used to explore the effect of gender on intention-to-report, attitude, subjective norms, and perceived behavioural control. There were statistically significant main effects of gender on attitude, $F(3, 545) = 4.45$, $p = .004$, $\eta^2 = .02$, and perceived behavioural control, $F(3, 545) = 3.00$, $p = .030$, $\eta^2 = .02$.

Post-hoc comparisons revealed that the mean attitude score for the 'different term' group was significantly lower compared to the male, $p = .007$, female, $p = .001$, and non-binary, $p = .008$, groups, refer to Table 4.

Additional post-hoc comparisons revealed that the mean perceived behavioural control score for the 'different term' group was also significantly lower when compared to the male, $p = .020$, and non-binary, $p = .049$, groups.

Table 4

Mean Attitude and Perceived Behavioural Control by Gender Group

	Male		Female		Non-binary		Different term	
Variable	Mean	SD	Mean	SD	Mean	SD	Mean	SD
Attitude	18.79	2.86	19.14	2.10	20.40	.89	16.93	3.60
Perceived behavioural control	35.12	7.35	33.96	7.21	38.00	1.87	30.50	9.11

3.4. Policy and Intention-to-report, Attitude, Subjective Norms, and Perceived Behavioural Control

A one-way between-groups ANOVA investigated the effect of cyber security policy on intention-to-report, attitude, subjective norms, and perceived behavioural control. Significant main effects of policy on intention-to-report, $F(3, 545) = 3.53$, $p = .015$, $\eta^2 = .02$, attitude, $F(3, 545) = 10.10$, $p < .001$, $\eta^2 = .05$, subjective norms, $F(3, 545) = 7.92$, $p < .001$, $\eta^2 = .04$, and perceived behavioural control, $F(3, 545) = 21.49$, $p < .001$, $\eta^2 = .11$), were found.

Indeed, post-hoc comparisons found that the mean intention-to-report score for the formal policy group was significantly greater than the 'unsure', $p = .014$, and 'no policy', $p = .018$, groups, but not the informal policy group, $p = .162$, refer to Table 5.

This trend was mostly mirrored in the post-hoc comparisons for the attitude and perceived behavioural control scores. The mean attitude and perceived behavioural control scores for the formal policy group were significantly higher compared to the 'unsure' (Attitude: $p < .001$; Perceived behavioural control: $p < .001$) and 'no policy' (Attitude: $p < .001$; Perceived behavioural control: $p < .001$) groups and had no significant differences to the informal policy group (Attitude: $p = .116$; Perceived behavioural control: $p = .167$).

In addition, post-hoc comparisons revealed that the mean subjective norm score for the formal policy group was significantly higher compared to the informal policy, $p = .030$, 'unsure', $p < .001$, and 'no policy', $p < .001$, groups.

Table 5

Mean Intention-to-report, Attitude, Subjective Norms, and Perceived Behavioural Control by Cyber Security Policy Group

	Formal		Informal		Unsure		No policy	
Variable	Mean	SD	Mean	SD	Mean	SD	Mean	SD
Intention-to-report	23.35	4.60	22.58	3.97	21.57	6.15	21.74	6.40
Attitude	19.32	2.19	18.89	2.17	17.69	3.60	18.02	3.15
Subjective norms	24.53	3.34	23.62	3.94	22.56	3.90	22.69	4.71
Perceived behavioural control	35.88	6.60	34.80	6.52	28.37	7.57	31.77	8.77

3.5. Position Level and Intention-to-report, Attitude, Subjective Norms, and Perceived Behavioural Control

A one-way between-groups ANOVA was used to investigate the effect of employees' position level on intention-to-report, attitude, subjective norms, and perceived behavioural control. Significant main effects were found for intention-to-report, $F(3, 545) = 5.21$, $p = .001$, $\eta^2 = .03$, attitude, $F(3, 545) = 5.91$, $p < .001$, $\eta^2 = .03$, subjective norms, $F(3, 545) = 2.91$, $p = .034$, $\eta^2 = .02$, and perceived behavioural control, $F(3, 545) = 11.62$, $p < .001$, $\eta^2 = .06$.

Post-hoc comparisons found that the mean intention-to-report scores for the leadership group were significantly higher when compared to the supervisor, $p = .005$, team member, $p = .002$, and 'other', $p = .004$, groups, refer to Table 6.

Further, post-hoc comparisons revealed that the mean attitude and subjective norm scores for the leadership group were significantly higher compared to the 'other' group (Attitude: $p < .001$; Subjective norms: $p = .006$), but not when compared to the supervisor (Attitude: $p = .073$; Subjective norms: $p = .149$) and team member groups (Attitude: $p = .087$; Subjective norms: $p = .089$).

Next, post-hoc comparisons found that the mean perceived behavioural control score for the leadership group was significantly higher than the team member, $p < .001$, and 'other', $p < .001$, groups, but not with the supervisor group, $p = .065$.

Table 6

Mean Intention-to-report, Attitude, Subjective Norms, and Perceived Behavioural Control by Position Level Group

	Leader		Supervisor		Team member		Other	
Variable	Mean	SD	Mean	SD	Mean	SD	Mean	SD
Intention-to-report	24.06	4.23	22.31	4.43	22.54	5.27	20.63	5.98
Attitude	19.34	2.41	18.77	2.29	18.91	2.48	16.84	4.31
Subjective norms	24.50	3.90	23.81	3.77	23.85	3.48	22.00	5.61
Perceived behavioural control	36.94	5.65	35.27	6.33	33.05	7.93	30.95	9.52

3.6. Cyber Security Job Relevance and Intention-to-report, Attitude, Subjective Norms, and Perceived Behavioural Control

An independent samples t-test was used to compare the mean differences among cyber security job relevance groups. A collapsed group of participants who described cyber security as being either primary or relevant to their position was compared with a group who described it as being irrelevant. Results revealed statistically significant differences between these groups for intention-to-report, $t(527) = 2.34$, $d = .20$, $p = .019$, attitude, $t(547) = 2.11$, $d = .18$, $p = .035$, subjective norms, $t(547) = 2.14$, $d = .18$, $p = .033$, and perceived behavioural control, $t(493) = 5.85$, $d = .50$, $p < .001$, scores. The primary/relevant group had higher mean scores compared to the irrelevant group for intention-to-report, attitude, subjective norms, and perceived behavioural control, refer to Table 7.

Table 7

Mean Intention-to-report, Attitude, Subjective Norms, and Perceived Behavioural Control by Cyber Security Relevance Group

	Primary/relevant		Irrelevant	
Variable	Mean	SD	Mean	SD
Intention-to-report	23.34	4.30	22.37	5.43
Attitude	19.16	2.32	18.71	2.72
Subjective norms	24.30	3.60	23.62	3.90
Perceived behavioural control	36.27	5.67	32.73	8.30

3.7. Multiple Regression Analyses

3.7.1. Regression Assumptions

Examination of a histogram of residuals indicated that the assumption of normality was met. This was supported by a non-significant Shapiro-Wilk statistic. Next, assessment of a scatterplot of predicted values against residuals indicated that the assumptions of linearity and homoscedasticity were met. Last, examination of the Variance Inflation Factor revealed no issues with multicollinearity.

3.7.2. Results

The degree to which the 12 independent variables (attitude, subjective norms, perceived behavioural control, gender, position level, cyber security policy, awareness of reporting obligations, organisational tenure, access to sensitive information, cyber security relatedness to job, and education) predict intention-to-report cyber security incidents was assessed by a multiple regression. The total variance explained by the model was 43%, $F(19, 529) = 21.29$, $p < .001$, $R^2 = .43$. Attitude, $p < .001$, subjective norms, $p < .001$, perceived behavioural control, $p < .001$, and access to sensitive information, $p = .041$, were statistically significant predictors of intention-to-report cyber security incidents.

Next, a backwards regression was conducted. In the final model, attitude, subjective norms, and perceived behavioural control were significant predictors, outlined in Table 8. Together, these three predictors explained 41% of the variance in intention-to-report cyber security incidents, $F(3, 545) = 127.28$, $p < .001$, $R^2 = .41$.

Table 8

Multiple Regression of Attitude, Subjective Norms, and Perceived Behavioural Control on Intention-to-report Cyber Security Incidents

Variable	β	βeta	*t*	*p*	Unique variance explained (%)
Constant	-.50		-.40	.690	
Attitude	.67	.35	7.72	< .001	9.86
Subjective norms	.22	.17	3.72	< .001	2.50
Perceived behavioural control	.16	.23	5.41	< .001	5.11

Attitude, subjective norms, and perceived behavioural control all uniquely predict intention-to-report cyber security incidents. In addition, β scores indicate that attitude, subjective norms, and perceived behavioural control were all positive predictors of intention-to-report cyber security incidents, controlling for the other variables in the model. Of note, βeta scores revealed attitude as the strongest predictor in the model, followed by perceived behavioural control, and subjective norms, see Table 8.

3.8. Actual Reporting Behaviour

Of the 549 study participants, 124 observed a cyber security incident at work. Of this number, 83% reported the incident, while 17% did not. Simple logistic regression revealed that intention-to-report cyber security incidents was a significant predictor of actual reporting behaviour, Exp(B) = 1.11, $p = .036$. Similarly, a simple logistic regression revealed that

perceived behavioural control was a significant predictor of actual reporting behaviour, Exp(B) = 1.13, $p = .002$.

Multiple logistic regression was used to analyse the relationship between intention-to-report and perceived behavioural control. It was found that, holding all other predictor variables constant, the odds of actual reporting behaviour occurring increased by 13%, 95% CI [1.03, 1.25], $p = .012$, for a one-unit increase in perceived behavioural control. The results also revealed that intention-to-report cyber security incidents was ultimately not a significant predictor of actual reporting behaviour, $p = .957$.

4. Discussion

The aim of this study was to empirically examine the factors that influence employees' intended and actual cyber security incident reporting behaviour. The findings of the present study are critically examined in the sections below, including a discussion of the theoretical and applied implications, study limitations, and directions for future research.

4.1. Findings and Implications

4.1.1. Attitude and Intention-to-report Cyber Security Incidents

In line with hypothesis one, a significant positive relationship was found between attitude and intention-to-report: the more positive employee attitudes were towards reporting cyber security incidents, the higher employee intentions were to report cyber security incidents. This finding is consistent with prior literature (Lee et al., 2016; May-Amy et al., 2020; Xu et al., 2021). This relationship may be explained in terms of the Theory of Planned Behaviour (Ajzen, 1985). Indeed, employees' positive attitudes towards reporting cyber security incidents may, in part, be attributable to their perceptions of positive outcomes that could arise from doing so. Employees may perceive positive outcomes at an organisational level, such as safeguarding the organisation from threats, or at the individual level from receiving a reward like a promotion or bonus. The results justify implementation of organisational initiatives to educate employees on the positive outcomes of reporting, such as the benefits. This strategy could coincide with use of rewards-based systems to help foster positive employee attitudes towards reporting. Research indicates that rewards-based systems are effective strategies to enhance performance within the workplace (Koo et al., 2019; Siwale et al., 2020). Therefore, incentivising reporting cyber security incidents with extrinsic rewards such as promotions or bonuses or intrinsic rewards such as recognition, for example, may help to increase reporting behaviours. Rewards-based schemes should be assessed

periodically in response to the changing needs of employees (Siwale et al., 2020). In addition, reward schemes should be informed by employee input to adequately incentivise.

4.1.2. Subjective Norms and Intention-to-report Cyber Security Incidents

As predicted by hypothesis two, a significant positive relationship was found between subjective norms and intention-to-report: positive social influences from colleagues and managers towards reporting cyber security incidents were associated with higher employee intentions to report cyber security incidents. This finding confirms the findings of earlier studies demonstrating a positive relationship between subjective norms and behavioural intentions (Carpenter & Reimers, 2005; Lee et al., 2016; May-Amy et al., 2020; Owusu et al., 2020; Park & Blenkinsopp et al., 2009; Siallagan et al., 2017; Utami et al., 2018; Xu et al., 2021). It is possible that the relationship between subjective norms and intention-to-report cyber security incidents could be attributed to employees being strongly influenced by and motivated to comply with colleagues or managers who support cyber security incident reporting behaviours, i.e., reporting cyber security incidents is accepted cultural behaviour in the workplace (Ajzen, 1985). These results justify organisations to invest in cultivating strong, positive cyber security reporting cultures where cyber security incident reporting is recognised as standard practice. Considering that culture flows ‘top-down’ (Clark, 1972; Sheppard, 2007), that is, the tendency for leader behaviour to guide subordinate behaviour, it is crucial that leaders perform and promote cyber security behaviours themselves. These results therefore justify implementation of cyber security training initiatives tailored for leaders, managers, and supervisors to generate critical buy-in for cyber security incident reporting.

4.1.3. Perceived Behavioural Control, Intention-to-report Cyber Security Incidents, and Actual Reporting Behaviour

In support of hypotheses three and four, the present study identified a significant positive relationship between perceived behavioural control with intention-to-report and actual reporting behaviour, respectively. In other words, employees' level of control in reporting cyber security incidents predicted both their intention-to-report cyber security incidents, and their actual cyber security incident reporting behaviour. These findings correspond with prior research evidencing a relationship between perceived behavioural control with intentions (Alanazi et al., 2022; Lee et al., 2016; Mansor et al., 2020; Tripermata et al., 2022) and behaviour (Ajzen, 1991; May-Amy et al., 2020; Rustiarini & Sunarsih, 2017).

Perceived behavioural control is determined by a person's confidence in their own ability to perform a behaviour which feeds into their level of motivation, and is influenced by factors such as past experience, anticipated obstacles, and available resources or opportunities (Ajzen, 1991). In considering this, the strong positive relationship found between perceived behavioural control and intention-to-report cyber security incidents may be explained by high employee confidence, and thus motivation, towards intending to report cyber security incidents. It is possible this confidence originates from the availability of resources in the workplace such as cyber security policies, cyber security incident reporting protocols, intuitive reporting channels, dedicated cyber security incident reporting support staff, as well as the employees' own prior reporting experience.

The effort expended in trying to perform a behaviour increases when a person has perceived behavioural control, or the perception of control in achieving a behavioural outcome (Ajzen, 1991). Therefore, the strong positive relationship found between perceived behavioural control and actual reporting behaviour in the present study may also be attributable, in part, to employees having confidence in their ability to report cyber security incidents and thus, expending more effort towards achieving the behavioural outcome of

reporting. The availability of requisite resources and opportunities at work could also have supported employee confidence in this context.

Practically speaking, these findings support the idea that organisations should find ways of increasing employee levels of perceived behavioural control regarding reporting cyber security incidents. Organisations may wish to consider integrating specific training aimed at increasing employees' confidence in reporting cyber security incidents. Training in this context should embed knowledge about cyber security policies, cyber security incident reporting procedures, or which people within the organisation employees can seek support from for reporting. Training should be targeted at both new and existing employees in on-boarding processes and as part of ongoing development.

In predicting intention-to-report cyber security incidents overall, it is noted that only three of the twelve variables explained 41% of the variance. These three key predictor variables are the attitude, subjective norm, and perceived behavioural control constructs from the Theory of Planned Behaviour – validating its use within the context of predicting cyber security incident reporting intentions within organisations. The remaining nine independent variables only explained an additional 2% of variance and of these, access to sensitive information was the only significant predictor.

4.1.4. Intention-to-report Cyber Security Incidents and Actual Reporting Behaviour

Contrary to hypothesis five, our study did not find a significant relationship between intention-to-report and actual reporting behaviour. This meant that employees' behavioural intentions did not predict their actual reporting behaviour of cyber security incidents in the present study. This finding contradicts earlier studies that found significant positive relationships between intentions and behaviour (Alanazi et al., 2022; May-Amy et al., 2020; Rustiarini & Sunarsih, 2017). The Theory of Planned Behaviour posits that intention is the immediate antecedent of behaviour and that the stronger intentions are, the more likely a

behaviour is to be performed. However, the results suggest that theoretically, the Theory of Planned Behaviour may not be applicable in the context of predicting actual cyber security incident reporting behaviour from cyber security incident reporting intentions. It is possible that other unmeasured factors could be mediating this relationship. Therefore, additional research is needed to explore what inhibits employees' cyber security incident reporting behaviour, even when it is within their control to report, to increase cyber security incident reporting to safeguard organisations.

4.1.5. Exploratory Analyses

First, exploratory analyses assessed between-groups differences for gender. Results showed that attitude and perceived behavioural control scores for the 'different term' gender group were significantly lower compared to male, female, and non-binary groups. These findings not only indicate that the 'different term' group had more negative attitudes towards reporting cyber security incidents compared to the other gender groups, but also that they appeared to perceive themselves as having lower levels of control in reporting cyber security incidents. Considering that the 'different term' gender group only comprised 14 people making up just 2.55% of the total sample, it is likely that this group was not fairly represented in the present study. Therefore, the small sample size of the 'different term' gender group likely renders these findings ungeneralisable to the wider population. Use of more inclusive gender groups should continue to be explored in future research to determine if this trend perseveres in larger samples.

Second, between-group differences for policy group were assessed. Results revealed that intention-to-report, attitude, and perceived behavioural control scores for the formal policy group were significantly higher than the 'unsure' and 'no policy' groups, but not the informal group. This indicates that employees had higher intentions to report cyber security incidents, positive attitudes, and felt that reporting cyber security incidents was within their

control if their organisation had a cyber security policy, regardless of whether it was formal or informal. The results also revealed that the formal policy group had significantly higher subjective norm scores compared to all other policy groups. Here, having a formal cyber security policy produced higher subjective norm scores – more employees felt that their colleagues and supervisors would approve of cyber security incident reporting behaviours and would report cyber security incidents themselves. Together these results suggest that at minimum, organisations should have an informal cyber security policy to encourage cyber security incident reporting intentions, foster positive attitudes towards cyber security incident reporting, and increase the perception that reporting cyber security incidents is within employees' control. However, to boost subjective norms, or the social pressures that employees feel to report cyber security incidents, organisations should make use of formal cyber security policies.

Third, between-group differences for employees' position level were investigated. It was found that supervisors' intention-to-report scores were higher than all other groups – indicating that leaders were more likely to intend on reporting cyber security incidents compared to employees at lower hierarchical levels. Further, leaders had higher attitude and subjective norm scores than the 'other' group but were similar with the supervisor and team member groups. These results indicate that leaders shared similar attitudes towards reporting cyber security incidents with employees at the supervisor and team member levels. In addition, leaders, supervisors, and team members felt similarly that their colleagues and supervisors would approve of cyber security incident reporting behaviours and would report cyber security incidents themselves. Regarding perceived behavioural control, the leadership group scored higher compared with the team member and 'other' groups, but not the supervisor group. This means that leaders and supervisors perceived themselves to have similar levels of perceived behavioural control in reporting cyber security incidents. Thus,

employees in more hierarchically senior positions felt to a higher degree that reporting was within their control, which may be attributed to having more prior reporting experience or knowledge of policies, for example. Taken together, these results indicate that additional effort is needed for workers at lower hierarchical levels and justify organisations undertaking cyber security incident reporting training and development tailored for different employee levels.

Last, exploratory analyses assessing cyber security job relevance revealed that employees who considered cyber security as being primary or relevant to their jobs, had higher intention-to-report, attitude, subjective norm, and perceived behavioural control scores, compared with those who considered it irrelevant to their job. Most importantly, this finding shows that employees who thought cyber security was either primary or relevant to their jobs were significantly more likely to intend on reporting cyber security incidents. This item, however, was placed somewhat as a 'trick question.' All respondents should have selected, at minimum, that cyber security was relevant to their jobs. Indeed, it is every employees' job to protect their organisation's cyber security by recognising attempted or completed cyber-attacks and reporting them to dedicated security personnel, for example. This finding ultimately highlights a key gap within organisations that needs to be addressed and integrated into cyber security strategies: organisations need to effectively communicate to their employees that cyber security is everyone's responsibility. This can be achieved with appropriate training and development, organisation resources, and policies for example.

It should be noted that the eta squared effect size values for most exploratory analyses were small. Therefore, these results should be interpreted cautiously.

4.2. Limitations and Future Directions

This study has important theoretical and applied contributions to the cyber security literature; however, a number of limitations are noted. Self-report data was exclusively used,

which enables systemisation, comparability, practicability, and the ability to investigate behaviours or attitudes that may not otherwise be observable (Kormos & Gifford, 2014; Tucker et al., 1990). However, self-report data is a subjective measure that can be prone to common method variance, response bias, social desirability, and boredom effects (Rosenman, et al., 2011; Spector, 1994). Future research could combat these concerns by using more objective and indirect meaures of actual reporting behaviour either exclusively, or alongside self-report data in a mixed-methods design. For example, an ethnographic naturalistic observation approach could be taken to observe actual cyber security incident reporting behaviour within real-world organisational contexts. Indeed, Eby (2011) purports that naturistic observation tends to demonstrate strong construct and face validity due to the high likelihood that behaviours observed in natural settings emanate reality. An applied scenario-based approach may also be taken. Here, participants could be presented with scenarios, either text or image-based (i.e., presentation of a phishing email or pop-up), and then be assessed on their intended or actual behaviour quantitatively based on the scenario provided to them. This approach could help to increase face validity of the study by contextualising items for participants in a naturalistic cyber-setting.

The present study was not exhaustive with regard to its exploration of factors that could influence actual-reporting behaviour within the context of cyber security. Only intention-to-report and perceived behavioural control were measured in accordance with the Theory of Planned Behaviour. In the present study, intention-to-report cyber security incidents was not significantly related with actual reporting behaviour, which is inconsistent with prior research in other disciplines. As discussed previously, other variables may be mediating this relationship. For example, contextual factors related to specific breaches, such as the security culture or nature of the information system or breach, may mediate the relationship between employees' intention and actual reporting behaviour of cyber security

incidents. Due to the present study being the first of its kind to explore cyber security incident reporting in a quantitative survey format, future research may wish to make use of qualitative research methods. In particular, narrative one-on-one interviews could facilitate the collection of 'rich' data and provide insight and into employees' thought processes and reasoning behind choosing not to report cyber security incidents despite their intention to do so. Anderson and Kirkpatrick (2016) argued that narrative interviewing helps researchers better understand peoples' experiences and behaviours and better represent contexts in comparison to quantitative research methods. Narrative interviewing may help to reveal contextual factors related to cyber-attacks, or the cyber security field in general, that may act as barriers for employees in reporting cyber security incidents. Any variables identified from this process could then undergo quantitative assessment.

As previously discussed, future research in this area should also continue to make use of inclusive gender groups when collecting demographic data. Doing so can help to determine whether 'different term' gender groups do indeed have more negative attitudes towards cyber security incident reporting as well as have lower control over reporting cyber security incidents in more representative samples.

4.3. Conclusion

This study is the first to investigate the factors that influence employees' intended and actual cyber security incident reporting behaviour. It was found that attitude, subjective norms, and perceived behavioural control significantly predicted participants' intention-to-report cyber security incidents. It was also found that perceived behavioural control significantly explained participants' actual cyber security incident reporting behaviour. Participants were also significantly more likely to intend on reporting cyber security incidents if they were managers, identified cyber security as being either primary or related to their job, and if their organisation had a cyber security policy, regardless of whether it was formal or

informal. These findings have important theoretical and applied implications. Theoretically, the results of this study validate the application of the Theory of Planned Behaviour to the cyber security incident reporting context. Practically, these findings can be applied in organisations to inform the development of strategies that increase employees' cyber security incident reporting behaviour, such as introducing cyber security policies and providing targeted training and development opportunities. Applying these findings can ultimately safegaurd organisations from cyber-attacks, minimise the extent of damage, and prevent similar attacks from re-occurring.

References

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Action control: From cognition to behavior* (pp. 11-39). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-69746-3_2

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2006). *Constructing a theory of planned behavior questionnaire*. https://people.umass.edu/aizen/pdf/tpb.measurement.pdf

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Prentiss-Hall.

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior, 136*, 107376. https://doi.org/10.1016/j.chb.2022.107376

Anderson, C., & Kirkpatrick, S. (2016). Narrative interviewing. *Int J Clin Pharm, 38*(3), 631-634. https://doi.org/10.1007/s11096-015-0222-0

Australian Bureau of Statistics. (2021). *2021 Census All persons QuickStats* https://abs.gov.au/census/find-census-data/quickstats/2021/AUS

Australian Cyber Security Centre (ACSC). (2021, September 15). *ACSC annual cyber threat report 2020-21*. https://www.cyber.gov.au/sites/default/files/2021-09/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf

AXA. (2021, September 29). *AXA future risks report 2021*. https://www-axa-com.cdn.axa-contento-118412.eu/www-axa-com/31ddaea8-21a7-4c22-be16-bfecbb6301b7_FRR2021_EN_Vdef.pdf

Brooks, C. (2022, Janurary 21). Cybersecurity in 2022 - a fresh look at some very alarming stats. https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=12954c76b616

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

Carpenter, T. D., & Reimers, J. L. (2005). Unethical and fraudulent financial reporting: Applying the theory of planned behavior. *Journal of Business Ethics, 60*(2), 115-129. https://doi.org/10.1007/s10551-004-7370-9

Chartered Institute of Ergonomics & Human Factors (CIEHF). (2022, March 16). *The role of human factors in delivering cyber security*. https://ergonomics.org.uk/resource/the-role-of-human-factors-in-delivering-cyber-security.html

Chyung, S. Y., Barkin, J. R., & Shamsy, J. A. (2018). Evidence-based survey design: The use of negatively worded items in surveys. *Performance Improvement, 57*(3), 16-25. https://doi.org/10.1002/pfi.21749

Clark, B. R. (1972). The organizational saga in higher education. *Administrative Science Quarterly*, *17*(2), 178-184. https://doi.org/10.2307/2393952

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry, 137*, 103614. https://doi.org/10.1016j.compind.2022.103614

Correia, S. G. (2022). Making the most of cybercrime and fraud crime report data: A case study of UK action fraud. *International Journal of Population Data Science, 7*(1), 1-17. https://doi.org/10.23889/ijpds.v7i1.1721

CybSafe. (2020, February 7). *Human error to blame for 9 in 10 UK cyber data breaches in 2019* https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/

Eby, D. W. (2011). Naturalistic observational field techniques for traffic psychology research. In B. E. Porter (Ed.), *Handbook of Traffic Psychology* (pp. 61-72). Academic Press. https://doi.org/10.1016B978-0-12-381984-0.10005-0

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and Behavior: An Introduction to theory and research*. Addison-Wesley Publishing Company.

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

Grispos, G., Glisson, W. B., Bourrie, D., Storer, T., & Miller, S. (2017). *Security incident recognition and reporting (SIRR): An industrial perspective* 2017 Americas Conference on Information Systems (AMCIS 2017), Boston, Massachusetts, United States.

Grispos, G., Glisson, W. B., & Storer, T. (2014). *Rethinking security incident response: The integration of agile principles* 20th Americas Conference on Information Systems, Savannah, Georgia, United States.

Gundu, T. (2019). Acknowledging and reducing the knowing and doing gap in employee cybersecurity compliance. *International Conference on Cyber Warfare and Security*, 1-10.

Harper, E. M. (2013). The economic value of health care data. *Nursing Administration Quarterly, 37*(2), 105-108. https://doi.org/10.1097/NAQ.0b013e318286db0d

Hayes, K., Nankivell, H., Aylward, M. (2022, February). Australia vs the United States: A comparison of cyber crime trends.

https://www.carternewell.com/page/Publications/2022/australia-vs-the-united-states-a-comparison-of-cyber-crime-trends/

Homeland Security. (n.d.). *If you see something, say something*. Retrieved August 4, 2022 from https://www.dhs.gov/see-something-say-something

Humphrey, M. (2017). *Identifying the critical success factors to improve information security incident reporting,* [Doctoral Dissertation, Cranfield University].

IBM Security. (2022). *Cost of a data breach report 2022*. IBM Security. https://www.ibm.com/au-en/security/data-breach

ISACA. (n.d.). *State of cybersecurity 2020*. https://www.isaca.org/go/state-of-cybersecurity-2020

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why employees (still) click on phishing links: Investigation in hospitals. *J Med Internet Res*, *22*(1), e16775. https://doi.org/10.2196/16775

Koo, B., Yu, J., Chua, B.-L., Lee, S., & Han, H. (2020). Relationships among emotional and material rewards, job satisfaction, burnout, affective commitment, job performance, and turnover intention in the hotel industry. *Journal of Quality Assurance in Hospitality & Tourism, 21*(4), 371-401. https://doi.org/10.1080/1528008X.2019.1663572

Kormos, C., & Gifford, R. (2014). The validity of self-report measures of proenvironmental behavior: A meta-analytic review. *Journal of Environmental Psychology, 40*, 359-371. https://doi.org/10.1016/j.jenvp.2014.09.003

Lee, C. S., & Kim, D. (2022). Pathways to cybersecurity awareness and protection behaviors in South Korea. *Journal of Computer Information Systems*, 1-13. https://doi.org/10.1080/08874417.2022.2031347

Lee, Y. H., Yang, C. C., & Chen, T. T. (2016). Barriers to incident-reporting behavior among nursing staff: A study based on the theory of planned behavior. *Journal of Management & Organization,, 22*(1), 1-18. https://doi.org/10.1017/jmo.2015.8

Lillebuen, S. (2014, November 16). *Melbourne's terrorism awareness campaign, 'If You See Something, Say Something', born out of 9/11 by New York ad guru*. The Age. https://www.theage.com.au/national/victoria/melbournes-terrorism-awareness-campaign-if-you-see-something-say-something-born-out-of-911-by-new-york-ad-guru-20141114-11mr0u.html

Mansor, T., Mastiniwati, T., Ariff, M., Hashim, A., & Aishah, H. (2020). Whistleblowing by auditors: The role of professional commitment and independence commitment. *Managerial Auditing Journal, 35*(8), 1033-1055. https://doi.org/10.1108/MAJ-11-2019-2484

Marques, C., Malta, S., & Magalhães, J. (2021). DNS firewall based on machine Learning. *Future Internet, 13*(12), 309. https://doi.org/10.3390/fi13120309

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., & Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. *Australasian Journal of Information Systems, 21*, 1-11.

McMurtrie, K. J., & Molesworth, B. R. C. (2018). Australian flight crews' trust in voluntary reporting systems and just culture policies. *Aviation Psychology and Applied Human Factors, 8*(1), 11-21. https://doi.org/10.1027/2192-0923/a000131

Mitropoulos, S., Patsos, D., & Douligeris, C. (2006). On incident handling and response: A state-of-the-art approach. *Computers & Security, 25*(5), 351-370. https://doi.org/10.1016/j.cose.2005.09.006

Morgan, S. (2016). Cybersecurity business report. https://www.csoonline.com/article/3110467/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html

Morgan, S. (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. *Cybercrime Magazine*. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Neria, M. B., Yacovzada, N.-S., & Ben-Gal, I. (2017). A risk-scoring feedback model for webpages and web users based on browsing behavior. *ACM Transactions on Intelligent Systems and Technology, 8*(4), 1-21. https://doi.org/10.1145/2928274

National Institute of Standards and Technology [NIST]. (n.d.). *Cyber Security*. https://csrc.nist.gov/glossary/term/cyber_security

NIST. (n.d.). *InfoSec*. https://csrc.nist.gov/glossary/term/infosec

Ouellette, J. A., & Wood, W. (1998). Habit and intention in everyday life: The multiple processes by which past behavior predicts future behavior. *Psychological Bulletin, 124*, 54-74. https://doi.org/10.1037/0033-2909.124.1.54

Owusu, G. M. Y., Bekoe, R. A., Anokye, F. K., & Okoe, F. O. (2020). Whistleblowing intentions of accounting students. *Journal of Financial Crime, 27*(2), 477-492. https://doi.org/10.1108/JFC-01-2019-0007

Paramita, S., Isbanah, Y., Kusumaningrum, T., Musdholifah, M., & Hartono, U. (2018). Young investor behavior: Implementation theory of planned behavior. *International Journal of Civil Engineering and Technology, 9,* 733-746.

Park, H., & Blenkinsopp, J. (2009). Whistleblowing as planned behavior – a survey of South Korean police officers. *Journal of Business Ethics, 85*(4), 545- 556. https://doi.org/10.1007/s10551-008-9788-y

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40-51. https://doi.org/https://doi.org/10.1016/j.cose.2017.01.004

Ponemon Institute. (2020, October). *Cybersecurity in the remote work era: A global risk report*. Keeper Security. https://www.keepersecurity.com/en_GB/ponemon2020.html

PricewaterhouseCoopers (PwC). (2021). *Cyber threats 2021: A year in retrospect*. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cyber-threats-year-in-retrospect.html

Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. (2019). Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ Health & Care Informatics, 26*(1), e100031. https://doi.org/10.1136/bmjhci-2019-100031

Rosenman, R., Tennekoon, V., & Hill, L. G. (2011). Measuring bias in self-reported data. *Int J Behav Healthc Res, 2*(4), 320-332. https://doi.org/10.1504/ijbhr.2011.043414

Rustiarini, N. W., & Sunarsih, N. M. (2017). Factors influencing the whistleblowing behaviour: A perspective from the theory of planned behaviour. *Asian Journal of Business and Accounting, 10*(2), 187-214.

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE, 63*(9), 1278-1308.

Schneider, B. (2003). *Beyond fear: Thinking sensibly about security in an uncertain world*. Springer.

Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2021). Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? *Journal of Computer Information Systems, 61*(6), 539-550. https://doi.org/10.1080/08874417.2020.1812134

Sheppard, T. (2007). *The writing on the wall: Reading the signs of business success and failure*. Wrightbooks.

Siallagan, H., Rohman, A., Januarti, I., & M., D. (2017). The effect of professional commitment, attitude, subjective norms and perceived behavior control on whistle blowing intention. *International Journal of Civil Engineering and Technology, 8*(8), 508-519.

Siwale, J., Hapompwe, C. C., Kukano, C., & Silavwe, D. C. (2020). Impact of reward system on organisational performance: A case study of Brentwood Suppliers Limited in Lusaka, Zambia. *International Journal of Scientific and Research Publications, 10*(7), 281-286. https://doi.org/10.29322/IJSRP.10.07.2020.p10335

Spector, P. E. (1994). Using self-report questionnaires in OB research: A comment on the use of a controversial method. *Journal of Organizational Behavior, 15*(5), 385-392. https://doi.org/10.1002/job.4030150503

Tripermata, L., Syamsurijal, S., WahyudIi, T., & Fuadah, L. L. (2022). Whistleblowing intention and organizational ethical culture: Analysis of perceived behavioral control in Indonesia. *The Journal of Industrial Distribution & Business, 13*(3), 1-9. https://doi.org/10.13106/JIDB.2022.VOL13.NO1.1

Tucker, R. W., McCoy, W. J., & Evans, L. C. (1990). Can questionnaires Objectively assess organisational culture? *Journal of Managerial Psychology, 5*(4), 4-11. https://doi.org/10.1108/02683949010000602

Utami, K. K. D., Mimba, N. P. S. H., Rasmini, N. K., & Widananputra, A. A. G. P. (2018). The effect of attitude toward the behavior, subjective norm and perceived behavioral control on whistleblowing intention *Research Journal of Finance and Accounting, 9*.

van Sonderen, E., Sanderman, R., & Coyne, J. C. (2013). Ineffectiveness of reverse wording of questionnaire items: Let's learn from cows in the rain. *PloS One, 8*(7), e68967. https://doi.org/10.1371/journal.pone.0068967

Verizon. (2022). *2022 data breach investigations report*. Verizon. https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

Webb, T. L., & Sheeran, P. (2006). Does changing behavioral intentions engender behavior change? A meta-analysis of the experimental evidence. *Psychological Bulletin, 132*(2), 249-268. https://doi.org/10.1037/0033-2909.132.2.249

Xu, Y., He, N., Lu, W., & Fluke, J. (2021). Understanding factors associated with barefoot social workers' decision making in assessing and reporting child physical abuse in China. *Child Abuse & Neglect, 120*, 105177. https://doi.org/10.1016/j.chiabu.2021.105177

Zeng, B., Hongbo, W., & Junjie, Z. (2020). How does the valence of wording affect features of a scale? The method effects in the Undergraduate Learning Burnout scale *Frontiers in Psychology*, (11), 1-12. https://doi.org/10.3389/fpsyg.2020.585179

Appendix A: CSIRI Details

Table A.1

Cyber Security Incident Reporting Inventory (CSIRI) Question type, Response Type, and Response Option Breakdown for the Attitude, Subjective Norm, Perceived Behavioural Control, Intention, and Behaviour Constructs

Construct	Question	Response Type	Response Options
Attitude, Subjective Norm, and Perceived Behavioural Control	How strongly do you agree or disagree with the following statements?	7-point Likert scale	Strongly Disagree: Disagree; Somewhat Disagree; Neither Agree Nor Disagree; Somewhat Agree; Agree; Strongly Agree
Intention	How likely are you to do the following?	7-point Likert scale	Very Unlikely; Unlikely; Somewhat Unlikely; Neither Likely Nor Unlikely; Somewhat Likely; Likely; Very Likely
Behaviour	Have you ever observed a cyber security incident at work?	Dichotomous	Yes; No
	Did you report the cyber security incident?	Dichotomous	Yes; No

Table A.2

Cyber Security Incident Reporting Inventory Item Adaptation Sources

Theory of Planned Behaviour Construct	Items	Source
Attitude	1: Cyber security incident reporting is valuable.	Lee et al. (2016)
	2: Cyber security incident reporting is beneficial.	Lee et al. (2016)
	3: Cyber security incident reporting is important.	Rustiarini & Sunarsih (2017)
Subjective Norm	1: My supervisor would approve of me reporting a cyber security incident.	Ajzen (2006)
	2: My co-workers would approve of me reporting a cyber security incident.	Ajzen (2006)
	3: My supervisor would report cyber security incidents.	Ajzen (2006)
	4: My co-workers would report cyber security incidents.	Ajzen (2006)
Perceived Behavioural Control	1: I am capable of reporting cyber security incidents.	Lee et al. (2016)
	2: In general, I know how to report cyber security incidents.	Lee et al. (2016)
	3: I have the appropriate resources to support me in reporting a cyber security incident.	Lee et al. (2016)
	4: It is within my control to report a cyber security incident.	Lee et al. (2016)
	5: I am confident that I can report a cyber security incident.	Rustiarini & Sunarsih (2017)
	6: I know the steps I need to take to report cyber security incidents in my workplace.	Lee et al. (2016)
Intention	1: Report a cyber security incident that breaches the IT usage policy.	Ajzen (2006)*
	2: Report myself if I breach the IT usage policy.	Ajzen (2006)*
	3: Report a co-worker if they breach the IT usage policy.	Ajzen (2006)*
	4: Report something I observe that is unusual or suspicious with the IT system.	Ajzen (2006)*

Behaviour	1: Have you ever observed a cyber security incident at work?	Ajzen (2006)*
	2: Did you report the cyber security incident?	Ajzen (2006)*

Note. *These items were created for this study based on Ajzen's (2006) Theory of Planned Behaviour questionnaire construction guide