social sciences

MDPI

Review

Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review

Noor Suhani Sulaiman [1,*], Muhammad Ashraf Fauzi [1,*], Walton Wider [2], Jegatheesan Rajadurai [3], Suhaidah Hussain [1] and Siti Aminah Harun [4]

[1] Faculty of Industrial Management, Universiti Malaysia Pahang, Kuantan 26300, Malaysia
[2] Faculty of Business and Communications, INTI International University, Nilai 71800, Malaysia
[3] College of Business Management and Accounting, Universiti Tenaga Nasional Malaysia, Kajang 43000, Malaysia
[4] Faculty of Education and Social Sciences, Widad University College (WUC), Kuantan 25200, Malaysia
* Correspondence: suhani.sulaiman@gmail.com (N.S.S.); ashrafauzi@ump.edu.my (M.A.F.)

Abstract: Cyber and information security (CIS) is an issue of national and international interest. Despite sophisticated security systems and extensive physical countermeasures to combat cyber-attacks, organisations are vulnerable due to the involvement of the human factor. Humans are regarded as the weakest link in cybersecurity systems as development in digital technology advances. The area of cybersecurity is an extension of the previously studied fields of information and internet security. The need to understand the underlying human behavioural factors associated with CIS policy warrants further study, mainly from theoretical perspectives. Based on these underlying theoretical perspectives, this study reviews literature focusing on CIS compliance and violations by personnel within organisations. Sixty studies from the years 2008 to 2020 were reviewed. Findings suggest that several prominent theories were used extensively and integrated with another specific theory. Protection Motivation Theory (PMT), the Theory of Planned Behaviour (TPB), and General Deterrence Theory (GDT) were identified as among the most referred-to theories in this area. The use of current theories is discussed based on their emerging importance and their suitability in future CIS studies. This review lays the foundation for future researchers by determining gaps and areas within the CIS context and encompassing employee compliance and violations within an organisation.

Keywords: cybersecurity/information security; compliance; policy; violation; systematic review

check for updates

Citation: Sulaiman, Noor Suhani, Muhammad Ashraf Fauzi, Walton Wider, Jegatheesan Rajadurai, Suhaidah Hussain, and Siti Aminah Harun. 2022. Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review. *Social Sciences* 11: 386. https://doi.org/10.3390/socsci11090386

Academic Editors: Sónia Maria Martins Caridade and Maria Alzira Pimenta Dinis

Received: 3 July 2022
Accepted: 30 July 2022
Published: 29 August 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

From the beginning of the internet era, issues of cyber and information security (CIS) began to surface rapidly (Chen et al. 2018). CIS is regarded as the current avenue in today's digital world. Organisations are under threat and at risk of cyber-attack due to phishing activities. The cybersecurity issue is dynamic and has not been well-studied, despite its enormous importance (Gillam and Foster 2020). Cybersecurity threats include criminals, spammers, and threats from other assorted attackers. Developing countries are more at risk of cyber threats due to limited resources to acquire and implement the mechanisms of cybersecurity in their organisations (Kabanda et al. 2018). Organisations have introduced various security technologies, i.e., database security protection, networking security protocols, and intrusion detection methods (among others), to protect their cyber and information technology from cyber threats.

Considered as the weakest link, humans are vulnerable to various forms of cyber threats (Gratian et al. 2018). Poor and dangerous security practises among individuals in an organisation should be identified, and mitigation efforts such as continual education and awareness are needed to prevent cyber-crimes such as phishing and malware attacks on security systems resulting from human intervention. End users, either for personal usage or within organisations, pose the greatest threat (Menard et al. 2017). In light of this

serious problem within organisations, management and stakeholders have established CIS problems as one of their critical agenda items. In response, organisations have made strict rules and policies to avoid persistent cyber threats such as system and data breaches and malicious software (Cram et al. 2017).

At the personal level, there are various measures available to strengthen one's cybersecurity; these include the adoption of antivirus software, antispyware software, cloud-based backup systems, and identity theft avoidance services (Menard et al. 2017). It is undeniable that external factors pose the biggest threat to CIS in an organisation. However, having the most sophisticated system does not protect the organisation if security surveillance is not imposed at the individual level. Personnel are an insider threat that surfaces as a risk for such a threat to happen (Cram et al. 2017). Hence, studies highlighting compliance and violations of CIS security policies provide the best understanding for practitioners of the antecedents that contribute to the most significant risks to CIS in an organisation.

Compliance and violation are considered two different perspectives in studies of CIS in organisations. The underlying elements of individual compliance and violation of CIS policies combine and are a manifestation of human behaviour. The theories of planned behaviour (TPB) (Ifinedo 2014), protection motivation theory (PMT) (Torten et al. 2018), and general deterrence theory (GDT) (Johnston et al. 2016) are among the theories widely used in CIS studies. Apart from these main theories, other relevant theories could provide a significant understanding of individual behaviours that result in compliance or violation of CIS policies. Studies that were reviewed lack in-depth analysis and conceptualisation of the stated theories. There is no integration of theory or production of hybrid models that encapsulate different aspects of CIS behaviour. As a result, this review offers the latest comprehensive critique and recapitulation of how the adaptation of theories in CIS studies has progressed in organisations from the standpoint of CIS compliance and violation caused by human behaviour.

1.1. The Terminology of Cybersecurity

Information and cybersecurity actually overlap, as the latter precedes the former in terms of including the human assets factor (Von Solms and Van Niekerk 2013). Information security is confined within the orbit of information-resources protection and the role of humans in the security process, whereas cybersecurity includes humans as potential targets, with them sometimes participating in a cyber-attack without consciously knowing it. The terminology of cybersecurity relates to protecting an individual's or organisation's virtual perimeter or environment (Althonayan and Andronache 2018). Van Schaik et al. (2017) define cybersecurity as cyberspace protection that includes personnel and organisations involved in cyberspace as well as any of their assets.

Many organisations tend to use these two terms interchangeably when relating them to their reputation, image, and compliance obligations (Althonayan and Andronache 2018). Among other terms used are "information assurance", "information technology security", or "electronic security". In another definition, Yoon and Kim (2013) define computer security as the "protection of information and computer assets" from computer attacks, theft, and other threats. General terminology such as "online safety behavior" (Boehmer et al. 2015) and "online security behavior" (Van Bavel et al. 2019) has also been adapted by several authors.

Due to these variations, the underlying crux of the term is based on managing software, hardware, assets, and humans in an organisation. Hence, this study uses cybersecurity and information security (CIS) terminology that reflects a holistic representation of protecting the cyber–physical aspects and the surrounding assets. This term also avoids confusion caused by variations in terminology that run the risk of researchers missing essential aspects of this field. This review is based on two facets of CIS: the cybersecurity measurement of personnel; and secondly, risk behaviour within cybersecurity. The former is usually reserved for, but not limited to, PMT applications, as well as those of TPB. The latter usually adopts Deterrence Theory, which features personnel deterrence to achieve compliance with security measures.

1.2. Previous Review

This study is not the first to review the literature on CIS. Previous reviews of CIS compliance and violations in organisations are available in the work of Lebek et al. (2014), Sommestad et al. (2014), Nasir et al. (2019), Soomro et al. (2016), Bongiovanni (2019), Cram et al. (2017), and Karlsson et al. 2016. These studies have their strength in reviewing CIS-related studies and, in particular, on focusing on CIS studies in specific disciplines. A study by Sommestad et al. (2014) presented a review of the determinants of information security policy compliance. The study discovered that several variables are found to be the most-adapted variables within specific theories such as TPB/TRA and TAM. The limitation in Sommestad's study is that the review included studies from various sources (17 journals, 3 magazines, 4 conference proceedings, and 5 from books or theses). Nasir et al. (2019) presented a study based on the cultural concept of information security. Their study is deficient in the broader sense of CIS in terms of the theoretical foundation, despite presenting the critical dimensions of information security studies. Other reviewed studies are limited to only higher education information security (Bongiovanni 2019) and a management approach (Soomro et al. 2016). All these reviews were fundamentally lacking in an understanding of cybersecurity as the 'umbrella' that covers all disciplines in organisational security practices.

The closest review paper that can be considered as the predecessor to this paper is the review by Lebek et al. (2014). The authors comprehensively reviewed a total of 144 articles on information security behaviour and the underlying theories used to conduct the studies. The relevance of our reviews compared to Lebek's study is due to several factors. Firstly, Lebek's study included a total of 51 conference papers. In light of the importance of conferences providing empirical findings, systematic review papers require a rigorous peer-review process that can only be processed by a reputable journal. Secondly, the study does not include the scope of cybersecurity behavioural studies. Cybersecurity, even though having a fundamentally similar notion as information security, covers an advanced scope that embraces organisational security entirely (Von Solms and Van Niekerk 2013).

From a methodological perspective, Lebek's study included eight different research methodologies (empirical research, modelling, deductive analysis, case study, action research, literature review, and grounded theory). Including all the different methodologies would not provide a sufficient understanding of the theory's application. Even more, the empirical studies in Lebek's study cover both quantitative and qualitative approaches. In this study, however, only quantitative studies that can be related to the theories based on the structural model and framework were used.

Next, Lebek's work only focused on the four theories adapted mainly from the reviews, comprising TAM, TPB/TRA, PMT, and GDT. By including conference-proceedings studies, the adapted theories might not have strong empirical justification based on the fundamental theory application. Leaving aside other validated theories such as Technology Threat Avoidance Theory or Social Capital Theory, further compromising insights into users' CIS security behaviour might lead to major flaws in the researchers' in-depth understanding of this phenomenon.

Finally, Lebek's study ranged from 2000 to 2014 and is now considered to be outdated. This current paper provides broader and revitalised findings from the CIS behaviour perspective from a new perspective. This dynamic field changes rapidly within 2 or 3 years as far as advancements in digital evolvement is concerned. This review notably stands out from other systematic-based reviews as its focus is within the scope of underpinning theories in CIS. As Lebek's is the only other study to discuss this, this study differs significantly by carrying out the theory integration of two and three theories from previous studies. This is in stark contrast to Lebek's study, which only focuses on four theories. Table 1 provides a summary of the previous systematic reviews or literature reviews of CIS in organisations.

Table 1. Previous review studies of cybersecurity/information security.

Author	Number of Studies	Year Range	Strength	Limitation
Nasir et al. (2019)	79	2000 to 2017	Information security culture.	Included conference and Ph.D. and Master thesis.
Soomro et al. (2016)	67	2004 to 2014	Role of manager.	Included qualitative studies.
Bongiovanni (2019)	40	2005–2017	Focus on higher education security management.	Limited to only higher education scope. Other organisations would have different contextual and relevant variables needed to understand employee cybersecurity.
Cram et al. (2017)	114	1990–2016	Focuses on security policy. This study creates a structure within the security policy domain that would facilitate theory building for future insights. This is conducted by looking into the inter-relationships among the key constructs.	Included qualitative studies. The time frame is too broad. The inclusion of studies prior to the new millennium may not be exhaustive and does not provide a comprehensive understanding of cybersecurity issues.
Sommestad et al. (2014)	29	2004–2012	60 variables have been studied concerning security policy compliance and incompliance.	Included from various sources (17 journals, 3 magazines, 4 conference proceedings, and 5 in book chapters or theses).
Lebek et al. (2014)	144	2000–2014	Theory-based studies.	Included conference papers. Included were eight methodology approaches rather than an empirical, quantitative study.
Karlsson et al. (2016)	64	1990–2014	interorganisational information security research.	Included conference papers.

2. Methodology

The methodology involves rigorous steps and procedures that examine the required papers within the scope of CIS behaviour. The articles included are from well-known sources, published in a Scopus-indexed journal, and based on reputable databases. Currently, Scopus and the Web of Science (WoS) are the only two reliable sources for citation data (Mongeon and Paul-Hus 2016); particularly, Scopus, whose coverage is interdisciplinary, represents a significant strength related to comparing different scientific fields. These databases included Sciencedirect, Emerald Insight, Taylor & Francis, Springer Link, Wiley-Blackwell, Inderscience, SAGE, and IEEE Explore. Apart from the 8 central databases, other journals included in the Scopus index are also acceptable. These include journals published by institutional publishers. The procedure for retrieving the articles is based on the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) method by including the exclusion and inclusion criteria for articles relevant to this review (Moher et al. 2015).

2.1. Inclusion and Exclusion Criteria

The only articles accepted were those using empirical data, excluding review articles. Conference proceedings and book chapters were excluded. Conference proceedings were omitted to ensure only peer-reviewed articles, thus determining the quality of the reviewed

publications (Mingers et al. 2012). Similar SLR studies have applied a similar approach by limiting sources to only journal publications (Galvão et al. 2018; Birkel and Müller 2021). Excluding conference proceedings has improved the quality of findings (Baashar et al. 2020). Furthermore, only English-language articles were included to minimise the potentially complicated process of understanding due to the need to translate. As for the duration, since the study of information and cybersecurity is relatively new in the social science context, only articles published between 2008 and 2020 (a thirteen-year time span) were accepted. As a result of the search, a total of 60 studies from reputable publishers were collected. Science Direct has the most extensive range of articles, comprising 35 studies. This is supported by multiple journals concerning information security and computer application journals, such as Computer & Security with 13 articles and Computers in Human Behaviour and Information & Management, which each produced 7 articles. Table 2 sets out the inclusion and exclusion criteria of this systematic review.

Table 2. Inclusion and exclusion criteria for the systematic review.

Inclusion	Exclusion
Journal indexed in Scopus	Journal not indexed in Scopus
Written in English	Conference proceedings, book chapters, and theses
Empirical and quantitative study	Conceptual study and literature review
Published between 2008 and 2020	Written in a language other than English

2.2. Search String

As CIS terminology varies in the literature, the authors searched for similar terminologies in dictionaries and thesauruses to ensure that essential terms were not missed. Information and cybersecurity overlap, as the latter precedes the former, including the human assets factor (Von Solms and Van Niekerk 2013). Information security is confined within the orbit of information resource protection and the role of humans in the security process. In contrast, cybersecurity includes humans as potential targets, sometimes participating in a cyber-attack without consciously knowing it. Cybersecurity terminology relates to protecting an individual's or organisation's virtual perimeter or environment (Althonayan and Andronache 2018). Van Schaik et al. (2017) define cybersecurity as cyberspace protection for personnel and organisations involved in cyberspace, as well as any of their assets.

Many organisations use these two terms interchangeably when relating them to their reputation, image, and compliance obligations (Althonayan and Andronache 2018). Among other terms used are "information assurance", "information technology security", or "electronic security". In another definition, Yoon and Kim (2013) define computer security as the "protection of information and computer assets" from computer attacks, theft, and other threats. General terminology such as "online safety behavior" (Boehmer et al. 2015) and "online security behavior" (Van Bavel et al. 2019) has also been adopted by several authors.

Due to these variations, the underlying crux of the term is based on managing software, hardware, assets, and humans in an organisation. Hence, this study uses cybersecurity and information security (CIS) terminology that reflects a holistic representation of protecting the cyber–physical aspects and the surrounding assets. This term also avoids confusion caused by variations in terminology that run the risk of researchers missing essential aspects of this field. The search string for the article search is as follows:

"Cyber Security" or "Information Security" or "Computer Security" or "internet security" or "digital security" and "behavior".

3. Results and Analysis

All the databases were searched one by one based on the specified search string. As a result, 60 studies were finalised. Table 3 presents the list of journals publishing the 60 studies. Computer and Security (Elsevier) produced 13 of the studies. This is followed

by Computers in Human Behavior (Elsevier) and Information and Management, with seven studies each. Other journals had four or fewer studies. (All 60 studies were marked with an "*" in the references).

Table 3. List of journals.

Journal Name	No. of Studies
Computer and security	13
Computers in Human Behavior	7
Information & Management	7
Decision Support system	4
MIS Quarterly	4
Information System Journal	2
European Journal of Information System	2
Information Management & Computer Science	2
Journal of Management Information System	2
Information and Computer Security	2
International Journal of Information Management	2
Others *	13
Total	60

* Others are journals with one publication.

Table 4 shows the list of theories adapted in all the 60 studies. PMT was the most frequently used, with 14 studies, followed by PMT + TPB/TRA and GDT with five studies each. PMT, the Health Belief Model (HBM), and GDT + Neutralisation Theory comprised three studies each. The rest of the theories were applied in at least one or two studies.

Table 4. Theories adapted in the review.

Theory/Theories	No of Studies	Studies
Protection Motivation Theory	14	Boss et al. (2015), Chou and Chou (2016), Dang-Pham and Pittayachawan (2015), Hanus and Wu (2016), Hina et al. (2019), Johnston and Warkentin (2010), Li et al. (2019), Meso et al. (2013), Posey et al. (2015), Torten et al. (2018), Tsai et al. (2016), Van Bavel et al. (2019), Warkentin et al. (2016), and Workman et al. (2008).
GDT	6	Chen et al. (2018), Dinev et al. (2009), Guo and Yuan (2012), Hovav and D'Arcy (2012), Safa et al. (2019), Son (2011), and Siponen and Vance (2010).
PMT + TPB/TRA	4	Cox (2012), Ifinedo (2012), Safa et al. (2015), and Siponen et al. (2014)
GDT+ Neutralisation Theory	3	Alshare et al. (2018), Barlow et al. (2013), and Silic et al. (2017).
PMT + HBM	2	Anwar et al. (2017) and Hwang et al. (2017).
HBM	2	Dodel and Mesch (2019) and Ng et al. (2009).
TPB/TRA	2	Hu et al. (2012) and Zhang et al. (2009).
TTAT	2	Gillam and Foster (2020) and Liang and Xue (2010).
Big Five Personality	2	Gratian et al. (2018) and McCormac et al. (2017).
Others	21	Al-Mukahal and Alshare (2015), Barton et al. (2016), Boehmer et al. (2015), Bulgurcu et al. (2010), Burns et al. (2017), Cheng et al. (2013), Choi and Song (2018), D'Arcy and Greene (2014), Donalds and Osei-Bryson (2019), Herath and Rao (2009), Humaidi and Balakrishnan (2015), Ifinedo (2014), Johnston et al. (2016), Lee et al. (2016), Li et al. (2010), Lowry and Moody (2015), Menard et al. (2017), Shropshire et al. (2015), Vance and Siponen (2012), Yazdanmehr and Wang (2016), and Yoon and Kim (2013).
Total	60	

4. Discussion

This systematic review provides an insight into how several theories were adapted in CIS studies. This review is not the first to review theoretical perspectives, as Lebek et al. (2014) have already provided this, but it provides a more in-depth focus on the adapted theories and, especially, theory integration. This review is more converged and exclusive by limiting sources to only journal publications, as compared to Lebek's study, which includes conference proceedings, books, book chapters, and editorials that had not undergone an extensive peer-review process. This review discovered that one of the many theories discussed in their study, the Technology Acceptance Model (TAM), was not applied in any of the 60 studies, except for Dinev et al. (2009), which applied TAM as a supporting and complementary theory in support of PMT. This shows that TAM did not sufficiently explain the user's CIS behaviour, as the constructs did not relate to any cognitive evaluation of security or the psychological domain involving a threat and coping appraisal. The following discussion of this paper is presented in the form of theories adopted/adapted from previous studies.

4.1. Protection Motivation Theory (PMT)

PMT first evolved in the 1980s from the Theory of Fear Appeal (Maddux and Rogers 1983). It has been proposed in the health and medical fields to predict individual engagement in disease prevention (Torten et al. 2018). Within the preventive medicine field, PMT was formulated to predict protective responses among individuals through the health threat of fear appeals (Posey et al. 2015). The theory has developed as a general motivation theory that explains human behaviour based on threats to their actions. Subjectively, the primary purpose of fear appeals is not to frighten people, but to inspire protective behaviours (Herath and Rao 2009; Meso et al. 2013; Boss et al. 2015). Fear is induced when an individual values the cost–benefit analysis in a state of perceived danger or when facing a threat (Workman et al. 2008). It is negatively associated with one affective state that represents a response that arises from a perceived threat, such as worry, negative arousal, discomfort, concern, or a particularly negative mood (Boehmer et al. 2015).

Safa et al. (2015) explain why PMT is one of the best theories to explain individual protective actions. It is central to information technology for users to comply with and perform actions related to cyber protection (Torten et al. 2018). On the other hand, security awareness as a critical role in PMT can also be designed from PMT developed through cognitive responses to security in the form of perceived severity, perceived vulnerability, response cost, response efficacy, and self-efficacy (Hanus and Wu 2016). The danger process controls the primary cognitive function by inducing stress and coping appraisals (Workman et al. 2008). This cognitive coping appraisal is engaged when an individual confronts a situation under pressure, which then leads to appraising the threat vulnerability. This could entail motivational consideration in facing such a threat based on the perception of vulnerability's existence (Herath and Rao 2009). PMT has been adapted in various studies, including in complying with the policy on security, data backup, protection of home and network computers, employing antivirus and antimalware software (Menard et al. 2017), desktop security behaviour (Hanus and Wu 2016), the omission of information security measures (Workman et al. 2008), and general security compliance behaviour (Herath and Rao 2009; Meso et al. 2013; Yoon and Kim 2013; Siponen et al. 2014).

4.1.1. Extension of PMT

PMT has been used as the most fundamental theory in the field of CIS in the past decade. As organisations seek to protect their assets and valuable intangible property, understanding employees' "protection" actions and reactions to threats is the most practical insight for organisations. Given that the majority of the studies adapt PMT, notable studies have adapted and integrated PMT well with other theories and variables. TPB, within the scope of cybersecurity, has been seen to be compatible with PMT (Safa et al. 2015). Five of the studies integrated PMT and TPB/TRA. Four studies integrated PMT and TPB

(Ifinedo 2012; Cox 2012; Safa et al. 2015; Hina et al. 2019) and one study integrated PMT and TRA (Yoon and Kim 2013). Ifinedo (2012) suggest that PMT and TPB, when combined, provide a better understanding of the factors that affect an employee's cybersecurity compliance. As organisations comprise various psychological aspects, a combination of different domains within two or more theories will deepen the fundamental knowledge of employee compliance and violation in CIS.

Dang-Pham and Pittayachawan (2015) proposed an extended PMT model. This model is deemed to be viable in the context of a personal mobile device or the "bring your own device" (BYOD) context that involves corporate and public places. One of the variables included in the extended PMT is the reward. Reward was found to be affected by response efficacy based on the user's intention. The suggested link is different from other studies, as the relationship was proposed as an endogenous relationship, rather than both serving as an exogenous variable to compliance intention. Findings emphasised that the extent of the cyber-threat critically influences the user's intention to perform malware avoidance. Users are not prepared to avoid malware even though they are not working while online. This extended PMT utilises the user's cognitive factors to provoke a considerable change in their intention to avoid threat.

Burns et al. (2017) proposed a relationship between psychological capacities (hope, optimism, self-efficacy, and resilience) and PMT variables. Psychological capacities encompass critical resources for work-related motivation. This integration provides a broad understanding of an employee's compliance with cybersecurity policies through motivational determinants that complement PMT. Furthermore, the model includes maladaptive rewards and fear; these two extra variables within the model help to explain employee-protective security actions.

Another construct integrated with PMT is perceived extraneous circumstances, defined as the user's inability to take control due to unforeseen circumstances that prevent one from engaging in intended actions (Warkentin et al. 2016). Similar to facilitating conditions as a factor that makes an action easier, the perceived extraneous circumstance is a hindrance factor based on events beyond one's control. It may be in the form of family emergencies, work duties, or travel restrictions. Within the scope of cybersecurity, this variable can be viewed as employees failing to comply with cybersecurity policies, perceiving that their workload is high, being busy with assignments, and/or focusing on other necessary job scopes (Siponen et al. 2014). Safa et al. (2015) linked PMT with the TPB variable with a precedent-dependable construct. This includes information security awareness of attitude and organisation policy on the subjective norm and experience and involvement in perceived behavioural control.

The Health Belief Model (HBM) is considered the predecessor of PMT. PMT and HBM have been integrated in two studies (Anwar et al. 2017; Hwang et al. 2017). As an extension of HBM, PMT has been able to predict individual cybersecurity behaviour. One particular focus of the integration of PMT and HBM is the way these two theories are integrated. While many of the PMT and HBM studies acted as two underlying precedent theories to predict cybersecurity behaviour, Li et al. (2019) presented HBM variables as the exogenous variables to PMT. The model refers to peer behaviour that influences cues to action and, subsequently, to prior experience with security practice. It was constructed in such a way that a link was established between the employees' experience of having security breaches and how they would make them less vulnerable to future cyber-attacks.

Tsai et al. (2016) tested the prior experience of safety hazards on the user's online behaviour. The study included perceived security support, personal responsibility, and safety habits. The new coping appraisal examines cognitive capability in connection to taking protective security actions. This coping variable is opted for more frequently than the threat appraisal due to its desirability in identifying user education interventions that can develop the motivation to acquire cybersecurity habits that can fend off online threats.

4.1.2. General Deterrence Theory (GDT)

GDT is the second most adapted theory in CIS studies (Alshare et al. 2018; Johnston et al. 2016; Cheng et al. 2013; Guo and Yuan 2012; Hovav and D'Arcy 2012; Son 2011; and Herath and Rao 2009). Studies applying Single Deterrence Theory include Son (2011), Hovav and D'Arcy (2012), and Guo and Yuan (2012). Studies that apply a single GDT to CIS typically investigate the aspect of negative encouragement in engaging in cybercrime. As studies of CIS are categorised in terms of compliance and violation, all the studies that apply GDT have both compliance (five studies) and violation (seven studies). This shows that GDT is the most suitable theory to be applied to understand employees' violations of behaviour as compared to compliance.

Deterrence Theory suggests that humans will refrain from engaging in undesirable behaviours (violation, crime, and abusive behaviour) if they believe that adverse consequences such as punishment and sanctions might occur (Johnston et al. 2016). Consequently, GDT was found to establish a relationship with humans engaging in deviant behaviours (Cheng et al. 2013). Human behaviour is based on an individual level of rationality that can be influenced by incentives in a particular negative way. Two main domains are laid out in this theory: sanction severity and sanction certainty. Certainty is defined as a belief that their criminal behaviour will be detected. Severity, on the other hand, refers to the degree of punishment once they are caught. It is posited that the higher the degree of certainty and severity of sanctions for a particular act, the more the individual will be deterred from acting in a negative way (Wenzel 2004). Another critical aspect of GDT is the celerity of sanctions, or the swiftness of sanction implementation. People will avoid criminal behaviour if the punishment for such behaviour is carried out with severity, swiftness, and a degree conviction (Alshare et al. 2018). People who are rational in terms of their actions are unlikely to commit a criminal act if their perception of the certainty, celerity, and severity of the sanctions resulting from their actions are more significant than the benefits of the crime (Dinev et al. 2009).

GDT has the highest instances of theory integration. A review shows that it is integrated with PMT + TPB (Herath and Rao 2009), Neutralisation Theory (Siponen and Vance 2010; Barlow et al. 2013; Silic et al. 2017), Social Capital Theory (Cheng et al. 2013), Neutralisation Theory + TPB (Al-Mukahal and Alshare 2015), PMT (Johnston et al. 2016), and Neutralisation Theory + Justice Theory (Alshare et al. 2018). GDT is effective and efficient due to its deterrence in relation to abiding by security policies. Deviant human behaviour can be explained in terms of punishment and sanctions to obtain compliance, as most people weigh up benefits and risks before engaging in any action. Future studies should always include factors within GDT in order to understand the implicit actions related to compliance with CIS.

4.1.3. Theory of Planned Behaviour (TPB)

TPB is a theory that explains how three predictors (attitude, subjective norm, and perceived behavioural control) influence an intention. The intention, in turn, affects individual behaviour. TPB is an extension of the Theory of Reasoned Action (TRA). Both theories are regarded as having the same theoretical underpinning in this review. The former has the added variable of perceived behavioural control. These two theories explain that attitude refers to positive personal feelings toward a behaviour either positively or negatively. The subjective norm is other people's perceptions and views of individuals engaging in a particular behaviour, while perceived behavioural control is one's perception that one can influence such behaviour (Fauzi et al. 2019).

Ten studies applied TPB/TRA (eight of the studies applied TPB) (Dinev et al. 2009; Bulgurcu et al. 2010; Hu et al. 2012; Ifinedo 2012; Cox 2012; Ifinedo 2014; Safa et al. 2015; Humaidi and Balakrishnan 2015), while two studies applied TRA (Yoon and Kim 2013; Siponen et al. 2014). Studies that applied TPB with other theories included PMT (Ifinedo 2014; Cox 2012; Safa et al. 2015) and HBM (Humaidi and Balakrishnan 2015). Humaidi and Balakrishnan (2015) adopted TPB and HBM when assessing employees' security policies

and compliance behaviour. This behaviour was linked with the HBM factors inherent in information security awareness (perceived severity, perceived susceptibility, and perceived benefits). Within the model, management support plays a vital role in information security when managing, for example, a public hospital. The study shows that hospital management is directly connected to decision making by dint of having the authority to solve problems related to human errors before proceeding to develop any information security policies. Another variable perceived to be important is trust. Trust is embedded in the TPB and HBM models. Trust is a critical factor for employees to believe in top management. Instilling confidence in employees to take on board security policy practises and implementation is highly dependent on the role of top management.

Dinev et al. (2009) proposed a model comprising TPB and elements of the Technology Acceptance Model (TAM). The two domains of TAM, i.e., perceived ease of use and perceived usefulness, were posited as the antecedents of attitude, subjective norm, and perceived behavioural control. The model was further complemented by Hofstede's (1980) cultural domain of uncertainty avoidance, power distance, masculinity, individualism, and long-term orientation. The study assesses an organisation's employees' antispyware technology adoption to protect information technology in two different cultures, the U.S. and South Korea. Hofstede believes that cultural differences have a considerable impact on an employee's intentions and behaviour. The practical implication of Hofstede's cultural contention provides an in-depth understanding of different cultural practises and compliance to cybersecurity protocols in the organisation. As this study was conducted in 2009, an early stage in digital technology, it is probably one of the few studies that adapted TAM in its study. Interestingly, TAM was not found in any of the recent studies other than in that of Dinev et al. (2009).

Top management has a strong influence on employees' norms, values, and beliefs concerning security policies. Subordinates would be more willing to participate in cybersecurity practises if they believed that top management participated in related initiatives and programs. Top management is the party responsible for establishing and enforcing such policies. Perceived management participation was studied by Hu et al. (2012), based on the TPB model. Apart from that, perceived goal orientation and perceived rule-oriented findings show that top management in the study impacted subjective norms and perceived behavioural control, but not attitude. This is because attitude is derived from an individual's cognitive evaluation of compliance within their inner self-belief. Top management provides the extrinsic motivation or pressure on employees' compliance intentions, which encourages employees to conform to CIS security policies.

5. Integration of Three Theories

Considering the depth and critical impact of CIS on organisational safety and livelihoods, it is acceptable that a combination of more than two theories is sufficient to answer the fundamental issue in today's organisational context. Very few studies combine more than two theories due to considerable difficulty in explaining the reason for these theories concerning CIS studies. This review discovered that six studies integrated three theories to explain the CIS phenomenon.

5.1. PMT + TPB + GDT

PMT and TPB are the two most adapted theories in CIS studies, with five studies. Herath and Rao (2009) extended the model by incorporating it with GDT. The model is viewed as an Integrated Protection Motivation and Deterrence Model of Security Policy Compliance under Taylor–Todd's Decomposed TRA. Even though the study is considered to pass the current perspective in CIS, it could provide valuable insights for future researchers reviewing the possibility of drawing together the theoretical perspectives of threat and coping appraisal that can determine the attitude of security policies among employees. The model is claimed to be holistic, as it comprises the organisational commitment of employees and the intention to comply, as well as environmental factors in

the deterrence of facilitating conditions and social influence. Social influence is measured in the context of subjective and descriptive norms. This was one of the earliest studies to provide a theoretical focus on employees' policy compliance intentions. The findings provide a foundation for other scholars studying employee compliance behaviour. The study found that an employee's certainty around security breaches has little impact on security concerns. Employees were found to have low security-breach perceptions. When this study was conducted in the late 2000s, CIS breaches and threats were not as prevalent as they are now. Employees complied with security policies because they perceived that it was not a hindrance to their daily lives. Furthermore, organisations were not as conscious of, and had very little idea of, the severity of CIS threats and their implications for their systems and organisations as a whole.

5.2. PMT, TRA, and CET

PMT, the Theory of Reasoned Action, and Cognitive Evaluation Theory, were studied by Siponen et al. (2014). The model consists of several components of the theories, including attitude (TRA), threat and coping appraisal (PMT), and rewards (CET). CET is a theory that estimates the negative outcome of rewards on intrinsic motivation, particularly for tangible rewards such as prizes or awards (Siponen et al. 2014). CET posits that rewards are a negative element in the context of their acting as a tool for behavioural control. This is due to recipients feeling controlled, resulting in decreased feelings of self-determination and autonomy. It was believed that CET rewards would be directly linked to positive behaviour such as security compliance, but attitudes toward compliance with security policies are needed, as employees' affection toward the policy as well as regulated rules is highly associated with their attitude. Rewards, on the other hand, predict the detrimental effect of intrinsic motivation on individuals based on actual remuneration.

5.3. GDT + Neutralisation Theory + TPB

GDT successfully explains an employee's compliance, integrated with Neutralisation and TPB. A study of three theories (GDT, Neutralisation, and TPB), with the added inclusion of Hofstede's cultural value, was studied by Al-Mukahal and Alshare (2015) in relation to employees in Qatar. The integration of the cultural factors of Hofstede's uncertainty avoidance and collectivism delineated the CIS behaviour in a developing country. Uncertainty avoidance moderates the scope of policy and the violation of information security in the case of a country having high uncertainty avoidance. On the other hand, collectivism shows that in a society where trust influences the violation of information security, it correlates negatively with a society with high collectivism. The clarity of the CIS policy predicts employees' violations. An individual who does not understand or who has a different understanding of the management's views does not comprehend the need to comply with security policies. Policy violations, work environments, and policy scope are all moderated by the cultural dimensions of uncertainty avoidance and collectivism.

5.4. TPB + SCT + SBT

Ifinedo (2014) proposed a recomposed TPB model. It was integrated with Social Capital Theory and Social Bond Theory (SBT). The SCT consists of locus of control and self-efficacy, which are based on perceived behavioural control. The study tends to link socialisation and group influence through SBT, personal beliefs, and self-efficacy through TPB and SCT, and cognition through TPB. SBT describes the bonding of the social aspect within a group. Bonding involves commitment, attachment, personal norms, and involvement (Hirschi 2002). The theory explains that individuals who have built their relationships upon such bonding could reduce their antisocial behaviour. Ifinedo (2014) believes that attachment is inherent in SBT and reflects individual identification with organisational values. Commitment refers to the effort and energy to uphold organisational CIS policy, while involvement reflects the employee's relationship with subordinates. Personal norms are the views and values of employees in relation to CIS policy. It was found that the

socio-organisational element was critical in explaining an individual's security compliance behaviour. Socio-organisational factors predict individual intention positively through the attitude and subjective norms of CIS compliance. On the other hand, social influence and the perception of individuals of their competence and control in conforming to such compliance have a dominant impact on their compliance behaviour.

5.5. GDT, TPB, and Situational Crime Prevention Theory (SCPT)

One study combined GDT, TPB, and situational crime prevention factors. Situational crime prevention encourages employees to prevent misconduct within information security (Safa et al. 2019). Both theories have a positive impact on individual attitudes, albeit an outcome proven slightly different in its role. GDT focuses on perception and attitude, while Situational Crime Prevention Theory emphasises environmental restrictions that allow the organisation to mitigate the insider threat. The integration has tended to decrease insider threats to the organisation. SCPT is believed to have the same effect on individuals' attitudes. Altogether, the three theories are claimed to complete a "chain of behaviour change" in relation to violating the CIS. The study by Safa et al. (2019) conceptualised the scope of deterrence and prevention based on insider threats. The deterrence factors of employees can be examined through the lens of managerial aspects. The security breaches and violations within organisations can be managed by technology. More importantly, psychological factors should be subjected to substantial managerial action. The role of values and culture also has a considerable influence on employees' violations in CIS (Wiley et al. 2020).

5.6. GDT, Neutralisation, and Justice Theory

A comprehensive study by Alshare et al. (2018) integrated three theories (GDT, Neutralisation, and Justice Theory). Within Justice Theory, procedural and distributive justice were significant factors in employee violations of CIS in higher education in the United States. On the other hand, interactional justice was not significant. While the importance of sanction severity and certainty is undeniable, sanctions' celerity has not been seen as influential. This is crucial in managing CIS in organisations, as threats and risks can happen very quickly. As violations or compliance in an organisation are implemented, the issue of justice arises. An employee might be compliant and rewarded for their loyalty, while other employees who violate the protocols might not be sufficiently punished for their actions. This form of justice involves various dimensions and magnitudes that warrant further empirical investigation within the organisation. This could provide interesting findings in relation to whether justice prevails among employees through the implementation of cybersecurity practises in an organisation.

5.7. Other Theories

Other relevant theories adapted in these studies include the Health Belief Model (HBM) (Bonar and Rosenberg 2011; Dodel and Mesch 2019), Rational Choice Theory (Li et al. 2010; Vance and Siponen 2012), Social Bond Theory (Choi and Song 2018), Social Exchange Theory (D'Arcy and Greene 2014), Control Theory and Reactance Theory (Lowry and Moody 2015), Compensation Theory (Zhang et al. 2009), Personality (Shropshire et al. 2015; McCormac et al. 2017), and Norm Activation Theory (Yazdanmehr and Wang 2016). All these theories are relevant based on their contextual studies. The findings could provide considerable insights for practitioners based on the findings and the inferred justifications provided. The use of any of these theories has a justification for employing them. For example, in the case of using HBM, the context of the study should be to answer the organisation's perceived "health" on the verge of the CIS attack. As for the use of personality, it could be used to determine the relationship between personality and the individual traits that organisations perceive would be a risk to CIS.

6. Suggestions for Future Research

Based on this review, the directions for future studies are many. The frequency of cybersecurity and information breaches has become a norm; compliance with policies should be the number one policy goal in an organisation. Therefore, the organisation should make sure employees understand policy implementation and the reason it is being regulated. PMT predicted that employees who felt that security policies were inconvenient and believed that the cost of compliance was too high would be more likely to not comply (Vance and Siponen 2012). Gaps are discussed and provide possibilities for relevant future studies in the scope of CIS.

When deciphering the geographical context of CIS studies conducted, one of the main gaps is the locality of studies. Based on a geographical context, the majority of the studies (31) were conducted in the United States, representing more than half of all the studies reviewed. Within the magnitude of studies in the United States, it is well-accepted that organisations in the United States are aware of the need to study the role of cybersecurity issues in the country's organisations. They are acutely aware of safeguarding their assets and information and their vulnerability to cyber-attacks. Other countries have a high concentration of studies, including Canada (four studies), South Korea (four studies), Finland (three studies), and Malaysia (three studies). Of these four countries, Malaysia is considered the only developing country among the top four countries undertaking CIS-behaviour studies; this indicates that the CIS issue is a serious issue for the country's cybersecurity. European countries, on the other hand, have not displayed as much interest in the CIS field, with only a handful of studies. Except for Finland with three studies, other countries have only one study (the UK and Israel) and only two studies have been conducted across multiple European countries (Van Bavel et al. 2019; Silic et al. 2017). European countries do not focus as much on CIS studies, possibly for two main reasons. Firstly, security systems are well-coordinated in Europe; or secondly, the people in Europe are law-abiding citizens who do not see the need to conduct an in-depth CIS study.

Security policies should include the domain of reward and penalty, as suggested by Safa et al. (2015). Abiding by policies is not easy for some individuals due to their personalities. Hence, customising reward and penalty schemes would enhance the regulatory aspect of cybersecurity. Apart from that, intervention by the management in terms of knowledge sharing by experts and industrial partners conducting technical training on how to avoid and identify threats could serve as a new research avenue (Fauzi et al. 2018). Knowledge sharing by experts skilled in the area of cybersecurity coming from industry or academia would be able to develop individual susceptibility and resistance towards cyber threats and reduce the risk of cyber-attacks.

To date, the role of responsibility in relation to cybersecurity is still understudied; this includes personal responsibility and group responsibility. Personal responsibility is a normative belief of personal action that is required for an individual to achieve a desirable outcome (Boehmer et al. 2015). As studies employing personal responsibility are still scarce, future studies should employ this variable on personal grounds. One should take responsibility for taking care of one's cyber welfare, similar to health (Gaston and Prapavessis 2014). In a cybersecurity context, users should believe that they have the responsibility to fend off possible malicious threats via the internet and become more vigilant. Employees should also update their spyware protection and make sure that their security software is a programme that is reliable in preventing malware and spam.

Another critical issue of interest is the effect of gender on cybersecurity in the organisation. Due to biological and physiological differences, each gender perceives risk and threat differently; hence, there would be different dependent variables for cybersecurity practices. In a significant study by Anwar et al. (2017), it was revealed that men have more self-reported cybersecurity behaviour compared to women. Men tend to take risks, while women have a higher level of risk concern. Women are significantly impacted by perceived control and risk of privacy when using social networking sites when sharing information

(Hajli and Lin 2016). The impact of gender on CIS should be further investigated to mitigate the CIS issue in an organisation.

The underlying concern of this study is that the integration of theories serves to explain employee compliance and violations in CIS. Well-established and -adopted theories should be tested thoroughly before being extended or integrated, as suggested by Sommestad et al. (2014). The main issue of integrating different theories in studying the user's CIS is the effect size. Combining effect sizes from different adapted models may lead to a distortion of variables and an overlap of each other, as they can measure similar aspects from different theories. This causes one variable to have the effect size of other variables in the same model (Fauzi 2019). This issue is also apparent when researchers remove certain variables, as it will cause an increase in effect size. Hence, from a statistical point of view, each theory's adaptation should be carefully taken from well-proven theories, having been empirically tested individually in relation to information and cybersecurity practises such as PMT, TPB, and GDT. Other nonextensive theories should be adapted individually or as complementary theories.

7. Conclusions

The escalation of cyber and information usage in today's world warrants the need for a systematic implementation of security policies in an organisation. Despite having sophisticated security systems in organisations, humans will always be the most vulnerable point of attack and threat to an organisation's CIS system. In light of cybersecurity studies, this paper reviewed 60 recent adoptions of CIS in the last 13 years. Three theories have been extensively used to study employee compliance and violation behaviour in the organisational context. Empirical justifications are crucial in explaining the CIS phenomenon. PMT, TPB, and GDT were found to be of the most relevance and served as the basis of future underpinning theories. A review of these theories, together with other relevant theories in CIS studies, provides compelling insight for practitioners, particularly to mitigating the severity of security compliance as well as violation. Several gaps and mis-steps were identified in CIS studies, including the geographical context of studies conducted, the role of gender in complying with CIS, the role of responsibility, and the issue of theory integration. Related studies to understand the user's adoption of cyber-related regulations are reviewed in this paper. This review has proven that CIS is imperative for an organisation to stay relevant in this challenging digital age. Threat and risk are ever present when the human factor is included in the equation.

Author Contributions: Conceptualization, N.S.S. and M.A.F.; methodology, N.S.S. and M.A.F.; software, N.S.S. and M.A.F.; validation, N.S.S. and M.A.F.; formal analysis, N.S.S. and M.A.F.; investigation, N.S.S. and M.A.F.; resources, N.S.S. and M.A.F.; data curation, N.S.S.; writing—original draft preparation, N.S.S.; writing—review and editing, M.A.F., W.W., J.R., S.H., S.A.H.; visualization, N.S.S. and M.A.F.; supervision, M.A.F.; project administration, N.S.S.; funding acquisition, M.A.F. All authors have read and agreed to the published version of the manuscript.

Funding: This study received funding from Ministry of Higher Education Malaysia under the Fundamental Research Grant Scheme FRGS RACER/1/2019/SS03/UMP/1 (University Grant no. RDU192619).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

Al-Mukahal, Hasan M., and Khaled Alshare. 2015. An examination of factors that influence the number of information security policy violations in Qatari organisations. *Information & Computer Security* 22: 410–30.

Alshare, Khaled A., Peggy L. Lane, and Michael R. Lane. 2018. Information security policy compliance: A higher education case study. *Information & Computer Security* 26: 91–108.

Althonayan, A., and A. Andronache. 2018. Shifting from information security towards a cybersecurity paradigm. Paper presented at 2018 10th International Conference on Information Management and Engineering, Manchester, UK, September 22–24, pp. 68–79.

Anwar, Mohd, Wu He, Ivan Ash, Xiaohong Yuan, Ling Li, and Li Xu. 2017. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior* 69: 437–43. [CrossRef]

Baashar, Yahia, Hitham Alhussian, Ahmed Patel, Gamal Alkawsi, Ahmed Ibrahim Alzahrani, Osama Alfarraj, and Gasim Hayder. 2020. Customer relationship management systems (CRMS) in the healthcare environment: A systematic literature review. *Computer Standards & Interfaces* 71: 103442.

Barlow, Jordan B., Merrill Warkentin, Dustin Ormond, and Alan R. Dennis. 2013. Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security* 39: 145–59.

Barton, Kevin A., Gurvirender Tejay, Michael Lane, and Steve Terrell. 2016. Information system security commitment: A study of external influences on senior management. *Computers & Security* 59: 9–25.

Birkel, Hendrik, and Julian M. Müller. 2021. Potentials of industry 4.0 for supply chain management within the triple bottom line of sustainability–A systematic literature review. *Journal of Cleaner Production* 289: 125612. [CrossRef]

Boehmer, Jan, Robert LaRose, Nora Rifon, Saleem Alhabash, and Shelia Cotten. 2015. Determinants of online safety behavior: Towards an intervention strategy for college students. *Behavior & Information Technology* 34: 1022–35.

Bonar, Erin E., and Harold Rosenberg. 2011. Using the health belief model to predict injecting drug users' intentions to employ harm reduction strategies. *Addictive Behaviors* 36: 1038–44. [CrossRef]

Bongiovanni, I. 2019. The least secure places in the universe? A systematic literature review on information security management in higher education. *Computers & Security* 86: 350–57.

Boss, Scott R., Dennis F. Galletta, Paul Benjamin Lowry, Gregory D. Moody, and Peter Polak. 2015. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly (MISQ)* 39: 837–64. [CrossRef]

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* 34: 523–48. [CrossRef]

Burns, A. J., Clay Posey, Tom L. Roberts, and Paul Benjamin Lowry. 2017. Examining the relationship of organisational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior* 68: 190–209. [CrossRef]

Chen, Xiaofeng, Dazhong Wu, Liqiang Chen, and Joe K. L. Teng. 2018. Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management* 55: 1049–60.

Cheng, Lijiao, Ying Li, Wenli Li, Eric Holm, and Qingguo Zhai. 2013. Understanding the violation of IS security policy in organisations: An integrated model based on social control and deterrence theory. *Computers & Security* 39: 447–59.

Choi, Myeonggil, and Jeongseok Song. 2018. Social control through deterrence on the compliance with information security policy. *Soft Computing* 22: 6765–72. [CrossRef]

Chou, Hui-Lien, and Chien Chou. 2016. An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior* 65: 334–45. [CrossRef]

Cox, James. 2012. Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior* 28: 1849–58. [CrossRef]

Cram, W. Alec, Jeffrey G. Proudfoot, and John D'arcy. 2017. Organisational information security policies: A review and research framework. *European Journal of Information Systems* 26: 605–41. [CrossRef]

D'Arcy, John, and Gwen Greene. 2014. Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security* 22: 474–89.

Dang-Pham, Duy, and Siddhi Pittayachawan. 2015. Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security* 48: 281–97.

Dinev, Tamara, Jahyun Goo, Qing Hu, and Kichan Nam. 2009. User behavior towards protective information technologies: The role of national cultural differences. *Information Systems Journal* 19: 391–412. [CrossRef]

Dodel, Matias, and Gustavo Mesch. 2019. An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. *Computers & Security* 86: 75–91.

Donalds, Charlette, and Kweku-Muata Osei-Bryson. 2019. Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management* 51: 102056. [CrossRef]

Fauzi, Muhammad Ashraf. 2019. Knowledge sharing in Asia Pacific via virtual community platform: A systematic review. *International Journal of Web Based Communities* 15: 368–94. [CrossRef]

Fauzi, Muhammad Ashraf, Christine Nya-Ling Tan, and T. Ramayah. 2018. Knowledge sharing intention at Malaysian higher learning institutions: The academics' viewpoint. *Knowledge Management & E-Learning: An International Journal* 10: 163–76.

Fauzi, Muhammad Ashraf, Christine Tan Nya-Ling, Ramayah Thurasamy, Adedapo Oluwaseyi Ojo, and Ibrahim Shogar. 2019. Muslim academics' knowledge sharing in Malaysian higher learning institutions. *Journal of Islamic Marketing* 10: 378–93. [CrossRef]

Galvão, Anderson, Joao J. Ferreira, and Carla Marques. 2018. Entrepreneurship education and training as facilitators of regional development: A systematic literature review. *Journal of Small Business and Enterprise Development* 25: 17–40. [CrossRef]
Gaston, Anca, and Harry Prapavessis. 2014. Using a combined protection motivation theory and health action process approach intervention to promote exercise during pregnancy. *Journal of Behavioral Medicine* 37: 173–84. [CrossRef]
Gillam, Andrew R., and W. Tad Foster. 2020. Factors affecting risky cybersecurity behaviors by US workers: An exploratory study. *Computers in Human Behavior* 108: 106319. [CrossRef]
Gratian, Margaret, Sruthi Bandi, Michel Cukier, Josiah Dykstra, and Amy Ginther. 2018. Correlating human traits and cyber security behavior intentions. *Computers & Security* 73: 345–58.
Guo, Ken H., and Yufei Yuan. 2012. The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management* 49: 320–26.
Hajli, Nick, and Xiaolin Lin. 2016. Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics* 133: 111–23. [CrossRef]
Hanus, Bartlomiej, and Yu Andy Wu. 2016. Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management* 33: 2–16. [CrossRef]
Herath, Tejaswini, and H. Raghav Rao. 2009. Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems* 18: 106–25. [CrossRef]
Hina, Sadaf, Dhanapal Durai Dominic Panneer Selvam, and Paul Benjamin Lowry. 2019. Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security* 87: 101594.
Hirschi, Travis. 2002. *Causes of Delinquency*. New Brunswick: Transaction publishers.
Hofstede, Geert. 1980. Culture and organisations. *International Studies of Management & Organisation* 10: 15–41.
Hovav, Anat, and John D'Arcy. 2012. Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management* 49: 99–110.
Hu, Qing, Tamara Dinev, Paul Hart, and Donna Cooke. 2012. Managing employee compliance with information security policies: The critical role of top management and organisational culture. *Decision Sciences* 43: 615–60. [CrossRef]
Humaidi, Norshima, and Vimala Balakrishnan. 2015. The Moderating effect of working experience on health information system security policies compliance behavior. *Malaysian Journal of Computer Science* 28: 70–92.
Hwang, Inho, Daejin Kim, Taeha Kim, and Sanghyun Kim. 2017. Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review* 41: 2–18. [CrossRef]
Ifinedo, Princely. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security* 31: 83–95.
Ifinedo, Princely. 2014. Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management* 51: 69–79.
Johnston, Allen C., and Merrill Warkentin. 2010. Fear appeals and information security behaviors: An empirical study. *MIS Quarterly* 34: 549–66. [CrossRef]
Johnston, Allen C., Merrill Warkentin, Maranda McBride, and Lemuria Carter. 2016. Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems* 25: 231–51. [CrossRef]
Kabanda, Salah, Maureen Tanner, and Cameron Kent. 2018. Exploring SME cybersecurity practices in developing countries. *Journal of Organisational Computing and Electronic Commerce* 28: 269–82. [CrossRef]
Karlsson, Fredrik, Ella Kolkowska, and Frans Prenkert. 2016. Inter-organisational information security: A systematic literature review. Information & Computer Security. *Information & Computer Security* 24: 418–51.
Lebek, Benedikt, Jörg Uffen, Markus Neumann, Bernd Hohler, and Michael H. Breitner. 2014. Information security awareness and behavior: A theory-based literature review. *Management Research Review* 37: 1049–92. [CrossRef]
Lee, Chunghun, Choong C. Lee, and Suhyun Kim. 2016. Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security* 59: 60–70.
Li, Han, Jie Zhang, and Rathindra Sarathy. 2010. Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems* 48: 635–45. [CrossRef]
Li, Ling, Wu He, Li Xu, Ivan Ash, Mohd Anwar, and Xiaohong Yuan. 2019. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management* 45: 13–24. [CrossRef]
Liang, Huigang, and Yajiong Lucky Xue. 2010. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems* 11: 394–413. [CrossRef]
Lowry, Paul Benjamin, and Gregory D. Moody. 2015. Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal* 25: 433–63. [CrossRef]
Maddux, James E., and Ronald W. Rogers. 1983. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology* 19: 469–79. [CrossRef]
McCormac, Agata, Tara Zwaans, Kathryn Parsons, Dragana Calic, Marcus Butavicius, and Malcolm Pattinson. 2017. Individual differences and information security awareness. *Computers in Human Behavior* 69: 151–56.
Menard, Philip, Gregory J. Bott, and Robert E. Crossler. 2017. User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems* 34: 1203–30.

Meso, Peter, Yi Ding, and Shuting Xu. 2013. Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security* 9: 47–67. [CrossRef]
Mingers, John, Frederico Macri, and Dan Petrovici. 2012. Using the h-index to measure the quality of journals in the field of business and management. *Information Processing & Management* 48: 234–41.
Moher, David, Larissa Shamseer, Mike Clarke, Davina Ghersi, Alessandro Liberati, Mark Petticrew, Paul Shekelle, and Lesley A. Stewart. 2015. Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. *Systematic Reviews* 4: 1–9. [CrossRef]
Mongeon, Philippe, and Adèle Paul-Hus. 2016. The journal coverage of Web of Science and Scopus: A comparative analysis. *Scientometrics* 106: 213–28. [CrossRef]
Nasir, Akhyari, Ruzaini Abdullah Arshah, Mohd Rashid Ab Hamid, and Syahrul Fahmy. 2019. An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications* 44: 12–22.
Ng, Boon-Yuen, Atreyi Kankanhalli, and Yunjie Calvin Xu. 2009. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems* 46: 815–25.
Posey, Clay, Tom L. Roberts, and Paul Benjamin Lowry. 2015. The impact of organisational commitment on insiders' motivation to protect organisational information assets. *Journal of Management Information Systems* 32: 179–214.
Safa, Nader Sohrabi, Carsten Maple, Steve Furnell, Muhammad Ajmal Azad, Charith Perera, Mohammad Dabbagh, and Mehdi Sookhak. 2019. Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems* 97: 587–97.
Safa, Nader Sohrabi, Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani, and Tutut Herawan. 2015. Information security conscious care behavior formation in organisations. *Computers & Security* 53: 65–78.
Shropshire, Jordan, Merrill Warkentin, and Shwadhin Sharma. 2015. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security* 49: 177–91.
Silic, Mario, Jordan B. Barlow, and Andrea Back. 2017. A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information & Management* 54: 1023–37.
Siponen, Mikko, and Anthony Vance. 2010. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly* 34: 487–502. [CrossRef]
Siponen, Mikko, M. Adam Mahmood, and Seppo Pahnila. 2014. Employees' adherence to information security policies: An exploratory field study. *Information & Management* 51: 217–24.
Sommestad, Teodor, Jonas Hallberg, Kristoffer Lundholm, and Johan Bengtsson. 2014. Variables influencing information security policy compliance. *Information Management & Computer Security* 22: 42–75.
Son, Jai-Yeol. 2011. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management* 48: 296–302.
Soomro, Zahoor Ahmed, Mahmood Hussain Shah, and Javed Ahmed. 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management* 36: 215–25.
Torten, Ron, Carmen Reaiche, and Stephen Boyle. 2018. The impact of security awarness on information technology professionals' behavior. *Computers & Security* 79: 68–79.
Tsai, Hsin-yi Sandy, Mengtian Jiang, Saleem Alhabash, Robert LaRose, Nora J. Rifon, and Shelia R. Cotten. 2016. Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security* 59: 138–50.
Van Bavel, René, Nuria Rodríguez-Priego, José Vila, and Pam Briggs. 2019. Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies* 123: 29–39.
Van Schaik, Paul, Debora Jeske, Joseph Onibokun, Lynne Coventry, Jurjen Jansen, and Petko Kusev. 2017. Risk perceptions of cyber-security and precautionary behavior. *Computers in Human Behavior* 75: 547–59.
Vance, Anthony, and Mikko T. Siponen. 2012. IS security policy violations: A rational choice perspective. *Journal of Organisational and End User Computing* 24: 21–41.
Von Solms, Rossouw, and Johan Van Niekerk. 2013. From information security to cyber security. *Computers & Security* 38: 97–102.
Warkentin, Merrill, Allen C. Johnston, Jordan Shropshire, and William D. Barnett. 2016. Continuance of protective security behavior: A longitudinal study. *Decision Support Systems* 92: 25–35.
Wenzel, Michael. 2004. The social side of sanctions: Personal and social norms as moderators of deterrence. *Law and Human Behavior* 28: 547–67.
Wiley, Ashleigh, Agata McCormac, and Dragana Calic. 2020. More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security* 88: 101640.
Workman, Michael, William H. Bommer, and Detmar Straub. 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior* 24: 2799–816.
Yazdanmehr, Adel, and Jingguo Wang. 2016. Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems* 92: 36–46.
Yoon, C., and H. Kim. 2013. Understanding computer security behavioral intention in the workplace. *Information Technology & People.* 26: 401–19.
Zhang, Jie, Brian J. Reithel, and Han Li. 2009. Impact of perceived technical protection on security behaviors. *Information Management & Computer Security* 17: 330–40.