Journal of Theoretical and Applied Information Technology
15th March 2022. Vol.100. No 5
2022 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INFORMATION SECURITY POLICY COMPLIANCE BEHAVIOR MODELS, THEORIES, AND INFLUENCING FACTORS: A SYSTEMATIC LITERATURE REVIEW

PUSPADEVI KUPPUSAMY[1], GANTHAN NARAYANA SAMY[1], NURAZEAN MAAROP[1], BHARANIDHARAN SHANMUGAM[2], SUNDRESAN PERUMAL[3]

[1]Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Malaysia

[2]School of Engineering and Information Technology, Casuarina, Charles Darwin University, Australia

[3]Faculty of Science and Technology, Universiti Sains Islam Malaysia, Negeri Sembilan, Malaysia

puspadevi_k@yahoo.com, ganthan.kl@utm.my, nurazean.kl@utm.my, Bharanidharan.Shanmugam@cdu.edu.au, sundresan.p@usim.edu.my

ABSTRACT

The paper aims to identify information security policy compliance behavior models, their respected theories, and influencing factors. This is the first and most current comprehensive systematic review of information security policy compliance models, theories, and influencing factors. A systematic review of empirical studies from twelve online databases was conducted. This review resulted in thirty-two (32) information security policy compliance behavior models proposed in different domains comprising various theories, concepts, and influencing factors. The results showed the importance of this issue among the researchers and a major limitation found was generalizability. Twenty (20) primary theories were extracted from the identified studies and found the theory of planned behavior and the protection motivation theory are the most trusted and reliable theories in information security policy compliance behavior models. Further analyses identified sixty (60) influencing factors and their alternative names and definitions. The most promising factors (high usage) of importance in descending orders are subjective norms, self-efficacy, attitudes, perceived benefits, threat vulnerability, threat severity, response efficacy, response cost, and experience. Besides that, factors such as self-efficacy, attitude, perceived benefit, threat severity, response efficacy, sanction severity, personal norms, experience, and training support were found and proved to be positively associated with the intention of compliance and considered robust for increasing information security compliance intention behavior. The results of this research can offer valuable information to fellow researchers in listing the models, their limitations, theories that are trustable, and influence factors that are critical for building a better model in the future.

Keywords: *Information Security Policy, Cybersecurity Policy; Security Compliance; Security Behavior; Systematic Literature Review*

1. INTRODUCTION

Organizations around the globe use their information security policies to safeguard their assets against information security breaches. Information security policies are defined as guidelines, requirements, and rules developed by management to guide employee's behaviors [1]. These policies commonly include the appropriate use of workstation resources, accountabilities concerning information security, and consequences of a security policy violation [2]. It is believed that information security policies provide a sufficient level of information security for an organization if the anticipated behavior mandated in policy is achieved in observance of the policy [2]–[4].

Employees should comply with these policies to protect their organization's resources and assets [5], [6]. Even though a good information security policy is in place, it does not guarantee that employees will comply it [7]. Hence, achieving information security policy compliance in an organization is far from trivial [8]. In reality, employee's noncompliance to information security policies certainly leads to greater

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

information security complications [9], [10]. Employee's compliance with the information security policy is, therefore, the biggest issue for organizations worldwide and continues to attract the attention of researchers [4]–[7], [9]–[13].

In the past, a variety of information security compliance models with their respective theoretical approaches and factors has been developed [14]. Different theories emphasized on different factors [14]. These factors however used different terms to describe similar concepts. Therefore, policymakers were unable to gain many advantages from the findings of these relative studies mainly because of such confusion.

A range of different systematic reviews has been undertaken on the problem so far, and mostly are a piece of a puzzle. Previous studies did not cover all the core aspect of information security policy compliance behavior models. Sommestad et al (2014) [8] performed a systematic literature review on variables alone mostly from papers in the year 2012 (period is not stated), Meanwhile, Wall et all (2014) [15] studied 24 papers from 2002 to 2011. Apart from these works from 2014, and Cram and Proudfoot (2017) [16] conducted a review, and identified core relationships solely among existing literature, and proposed research framework. In addition, Angraini et all (2019) [17] conducted literature review articles from 2014 to 2019 to find state of art and challenges in information security policy compliance studies. While Ali et all (2020) [18] conducted a literature review to identify the behavioral transformation process from non-compliance to compliance. Hence, it is evident that there have been no comprehensive systematic reviews covering information security policy compliance models, theories, and influencing factors published so far to the best of the author's knowledge. Hence there is a need to produce comprehensive systematic reviews covering information security policy compliance models, theories, and influencing factors in one single article. In terms of findings, this paper analyzed the models, their theories and their influencing factors in depth which is not visible in other such studies.

Hence, there is an essential need to investigate various information security compliance behavior models to expand the present knowledge in the field. Therefore, the purpose of this study is to provide an in-depth review of information security policy compliance behavior models, their theories, and influencing factors.

Information security policy compliance models from 1 January 2014 till 31 May 2021 is explored and analyzed in detail as well as their domains, limitations, applied theories, and influencing factors. This article is organized as follows: Section II defines the research method on the process of systematic literature review that was performed. Section III, IV and V present the steps in systematic literature review namely planning, execution and reporting. Section V contains the results of this study followed by Section V1 describes the findings of this study. The discussion and future works are highlighted in Section VII followed by the conclusion in Section VIII. Section IX is the acknowledgment segment.

2. RESEARCH METHOD

This section describes the systematic literature review (SLR) processes following the guidelines by [19] and [20]. These methods are suitable for information security compliance behavior studies. The SLR guidance consists of three main phases namely prepare, perform and report the review. The process of 'prepare the review' consists of five stages; a) defining the need for a review, b) commissioning a review (optional), c) outlining research questions, d) creating review protocol, and e) assessing the review protocol (optional). The second phase is 'perform the review' which includes five stages; (a) research identification; (b) primary studies selection; (c) quality assessment of the studies; (d) data retrieval and checking; and (e) data analysis. The last phase is 'report the review' consist of three stages: (a) the description of the distribution methods, (b) the formatting of the relevant report, and (c) the evaluations (optional). Figure 1 describe the phases and stages in detail.

Figure 1: Systematic literature review phases and stages

The research questions and the evaluation procedure were established during the planning process. The evaluation procedure contains the selection of data sources, search string, and study selection. In addition, the requirements for inclusion and exclusion, extraction of data, as well as the quality evaluation report, were also specified. Conducting the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

review phase means executing the research based on the review protocol in the selected repositories. The preliminary results from the search were examined according to the inclusion, exclusion, and quality criteria. When the finalized suitable studies are identified, the data is extracted to find answers for the identified research questions. Reporting in the review phase will provide the outcome based on the extracted data and report accordingly.

3. PHASE 1: PLANNING OF THE REVIEW

3.1 Define SLR Questions

The SLR questions were designed based on the criteria developed by Petticrew and Roberts [21]. Table 1 shows the requirements and scope of this SLR research question structure.

Table 1: Requirement and Scope of Research Question Structure

Requirement	Scope
Population	Information security policy compliance behavior models from both academics and industry
Intervention	Limitations of the identified Information security policy compliance behavior models
Comparison	Applicability of the models according to domains, theories, and influencing factors
Outcomes	List of information security policy compliance behavior models with their domains, limitations, their theories, and also their influencing factors
Context	Review of any studies on information security policy compliance behavior models

Based on the research question structure, the SLR questions are:

RQ1. What are the existing information security policy compliance behavior models?

RQ2. What are the limitations of the information security policy compliance behavior models?

RQ3. What are the underlying theories of each information security policy compliance behavior models?

RQ4. What are the influencing factors of information security policy compliance behavior models?

3.2 Define Data Sources, Search String, and Study Selection

The choice of online databases was based on the indexed databases about "information security policy compliance behavior models" studies from twelve online databases. Meanwhile, the data sources were derived from sources such as Academic search premier (EBSCO host), ACM digital library, Emerald Insight, IEEEXplore digital library, Springer link, Science direct, Scopus, Web of Science, Oxford academic journals, SAGE journals, Taylor & Francis and the Wiley online library. These repositories are subscribed by the library of University Technology Malaysia.

The search string included combinations of research related and synonymous phrases. The initial search strings are (information security policy compliance behavior), (cybersecurity policy compliance behavior), (model). The search string is then constructed using Boolean "AND" and Boolean "OR" to allow synonyms and word-class variants of each keyword used. The search string was calibrated and adjusted by following the source's particular syntax. In digital repositories, the search string will be executed based on titles, abstracts, and metadata to provide a clear and concise summary of the research.

The study ranks the source of research articles from highest to lowest priority in the following order: journals, conferences or proceedings, technical reports, thesis reports, books, and magazine articles.

3.3 Define Inclusion and Exclusion Criteria

Based on our research questions, the inclusion criteria are as follows:-

- Studies that wrote in English;
- Studies that originally proposed its own information security policy compliance behavior model;
- Peer-reviewed studies published between January 1st, 2014, and May 31st, 2021;
- Studies that clearly define information security policy compliance behavior model; and
- Studies that were tested empirically.

On the other hand, exclusion criteria are as follows:

- Studies that failed to produce the model;
- Studies that are on non-compliance only;
- Studies that contain only the framework and not the model; and
- Studies of the home user (out of scope).

In the event of any duplicate reports from the same research, the latest full report found is considered for evaluation.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. PHASE 2: CONDUCTING THE REVIEW

4.1 Search and Selection

The initial phase of the search process identified 43,453 studies using the defined search term. This was followed by 5,133 papers selected/checked to be reviewed. Only 382 of these were theoretically important based on the projection of titles and abstracts. Before being approved for data synthesis, each of these studies was screened according to the inclusion and exclusion criteria. When titles and abstracts were not adequate to determine a paper's importance, then the complete papers were searched. After a thorough review of the abstracts and full text and the exclusion of duplicates, Forty one (41) studies were then approved for synthesis.

4.2 Extraction of Data and Study Quality Assessment

In this process, a quality criteria checklist from [22] was used to ensure that the data extraction process met the quality criteria. Quality checklists for the study are shown in Table 2. The study checklist used three coded scales, which were given a score; Yes=1; Partially=0.5; No=0. Therefore, each study is given scores by answering 5 questions in Table II. Each paper will be given a summation of each of the items from the item checklist where the possible scores range is from 0.5 to 5. The fulfillment of the quality criteria was then used to assess the differences in quality and to understand the findings.

Table 2 :Item Study Checklist

Item	Answer
1. Was the article referred to?	Yes/No
2. Was the aim of the study is clearly stated?	Yes/No/Partially
3. Was the data collection were carried out well?	Yes/No/Partially
4. Were the study participants / respondents were described?	Yes/No/Partially
5. How generalizable are the findings of this study to the target population concerning the size and representativeness of the sample?	Yes/No/Partially

We identified 41 studies and then underwent a quality checklist. Twelve (12) articles scores 5 out of 5 points are from Alkalbani et al. (2015), Chen et al. (2018), Cheng et al (2014), Choi & Song (2018), Han et al (2017), Ifinedo (2014), Kim et al (2014), Kranz & Haeussinger (2014), Moody et al (2018), Safa et al (2015), Siponen et al (2014), and Sohrabi Safa et al (2016) [1], [3], [27], [28], [4], [9], [10], [14], [23]–[26].

Meanwhile, 5 articles scored 4.5 out of 5 points are from Amankwa, Loock, & Kritzinger (2018), Sommestad et al (2015), Lowry & Moody (2015), Dhillon, Talib, & Picoto (2020), Alanazi, Anbar, Ebad, Karuppayah, & Al-Ani (2020) [2], [5], [29]–[31].

Besides that, 15 articles scored 4 out of 5 points are from Rajab & Eydgahi (2019), Iriqat, Ahlan, & Molok (2019), Feng, Zhu, Wang, & Liang (2019), Ahmad, Ong, Liew, & Norhashim (2019), Sommestad (2018), Razilan et al (2016), Hofeditz, Nienaber, Dysvik, & Schewe (2017), D'Arcy & Lowry (2017), Yazdanmehr & Wang (2016), Humaidi, Balakrishnan, & Shahrom (2014), Onumo, Ullah-Awan, & Cullen (2021), Ali, Dominic, & Ali (2020), Liu, Wang, Wang, & Niu (2020), X. Wang & Xu (2021) and Carmi & Bouhnik (2020) [6], [32], [41]–[45], [33]–[40].

However, 9 articles from Alalwan (2018), Hina & Dominic (2017), Nasir et al (2017), Connolly, Lang, & Tygar (2015), Johnston, Warkentin, & Siponen (2015), Daud et al (2018), Box & Pottas (2014), Pham, El-Den, & Richardson, (2016), Stewart & Jurjens (2017) [11]–[13], [46]–[51] scored only 3 points and below.

Table 3 shows the quality scores for all 41 studies. Twenty studies (20) and twelve studies (12) were in the good and very good quality categories. Three (3) studies were rated as fair while three (3) studies are poor and three (3) more studies in very poor quality as they did not provide detailed results and methodology. Since this study only emphasizes the original, realistic, and clearly defined information security policy compliance behavior model, nine (9) studies have been excluded, with very poor, poor, and fair scores. Finally, only 32 studies were included for analysis.

Table 3 :Result of the Quality Checklist

Quality Scale	Very Poor (=1 or 1.5)	Poor (=2 or =2.5)	Fair (=3 or =3.5)	Good (=4 or =4.5)	Very Good (=5)	Total

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Number of Studies	3	3	3	20	12	41

Figure 2 provides a review of the selection phases of the study and their findings in the SLR guidelines as per [19].

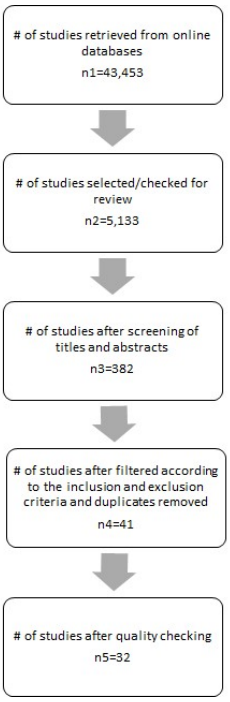

Figure 2: Summary of the stages of study selection

5. PHASE 3: REPORTING OF THE REVIEW

This section presents the data extracted from the studies according to the research questions defined in Section III.

5.1. RQ1: What are the Information Security Policy Compliance Behavior Models?

There are 32 studies available on information security policy compliance behavior models suitable for this review from January 2014 to May 2021. Table 4 shows that the models were given an article id accordingly and listed in descending order according to the year of publication. There were 6 studies in 2014, 4 studies in 2015, 2 studies in 2016, 4 studies in 2017, 5 studies in 2018, 4 studies in 2019, 5 studies in 2020, and 2 studies in 2021 (until May) respectively. There are a consistent number of papers published each year between 2014 to 2021. This indicates that the information security compliance behavior models still had unresolved gaps and room for improvement.

Some researchers produced complex models such as [6], [14], [38], [39] and others produced simpler solutions such as [37], [40]. However, the complexity of the model does not represent the effectiveness of the model to produce better results but the choices of the factors or variables that influence are more important.

Table 4 :Current Information Security Policy Compliance Behavior Models

Article Id	Year	Author	Title
A1 [44]	2021	X.Wang & Xu	Deterrence and leadership factors: Which are important for information security policy compliance in the hotel industry
A2 [41]	2021	Onumo et al	Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures
A3 [43]	2020	Liu et al	Influencing factors of employees' information systems security policy compliance: An empirical research in China
A4 [42]	2020	Ali et al	Organizational Governance, Social Bonds and Information Security Policy Compliance: A Perspective towards Oil and Gas Employees
A5 [30]	2020	Dhillon et al	The Mediating Role of Psychological Empowerment in Information Security Compliance Intentions
A6 [45]	2020	Carmi and Bouhnik	The Effect of Rational Based Beliefs and Awareness on Employee Compliance with Information Security Procedures: A Case Study of a Financial Corporation in Israel
A7 [31]	2020	Alanazi et al	Theory-Based Model and Prediction Analysis of Information Security Compliance Behavior in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

			the Saudi Healthcare Sector
A8 [32]	2019	Rajab, and Eydgahi	Evaluating the explanatory power of theoretical frameworks on the intention to comply with information security policies in higher education
A9 [33]	2019	Iriqat et al	Information security policy perceived compliance among staff in Palestine universities: An empirical pilot study
A10 [34]	2019	Feng et al	How paternalistic leadership influences IT security policy compliance: The mediating role of the social bond
A11 [35]	2019	Ahmad et al	Information security assurance behavior through information security monitoring and social learning factors
A12 [36]	2018	Teodor Sommestad	Information security compliance of work-related groups
A13 [23]	2018	Chen et al	Sanction severity and employees' information security policy compliance
A14 [24]	2018	Choi and Song	Social control through deterrence on the compliance with information security policy
A15 [14]	2018	Moody et al	Unified information security compliance model
A16 [29]	2018	Amankwa et al	Establishing information security policy compliance culture in organizations
A17 [37]	2017	Razilan et al	Information security policies compliance among employees in Cybersecurity Malaysia
A18 [9]	2017	Han et al	An integrative model of information security policy compliance with psychological contract
A19 [38].	2017	Hofeditz et al	Intrinsic and extrinsic motivators as predictors of compliance behavior intention
A20 [39]	2017	D'Arcy and Lowry	Information security compliance through cognitive-affective drivers
A21 [6]	2016	Adel Yazdanmehr, Jingguo Wang	Employees' information security policy compliance: A norm activation perspective
A22 [4]	2016	Sohrabi Safa et al	Information security policy compliance model in organizations
A23 [25]	2015 A18	Sohrabi Safa et al	Human aspects of information security in organizations
A24 [2]	2015 A19	Sommestad	The sufficiency of the theory of planned behavior for explaining information security policy compliance
A25 [26]	2015 A20	Alkalbani et al	Investigating the role of socio-organizational factors in the information security compliance in organizations
A26 [5]	2015	Lowry and Moody	Control-reactance compliance model (CRCM)
A27 [40]	2014	Humaidi et al	Exploring user's compliance behavior towards health information system security policies based on extended health belief model
A28 [1]	2014	Ifinedo	Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition
A29 [10]	2014	Siponen et al	Employees' adherence to information security policies: an exploratory field study
A30 [27]	2014	Cheng et al	Understanding personal use of the internet at work: An integrated model of neutralization techniques and general deterrence theory
A31 [28]	2014	Kranz and	The role of endogenous motivations on

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

		Haeussinger	employees' information security behavior
A32 [3]	2014	Kim et al	An integrative behavioral model of information security policy

Information security policy compliance behavior models have been developed and tested empirically in a variety of domains as in Table 5. These are classified as general, telecommunication/IT, university, public admin, health, industries, supply chain, research agency, hotel, oil and gas, and finance. The General domain includes also working professionals from (A15) [14] article, and generally titled employees (A21) [6] and workers from various organizations (A31) [28]. Besides that, sectors that could not fit into any other domain listed above have been put under the general domain too. Table V shows the application domains of the 32 information security compliance behavior models.

Table 5: Application Domains of the identified Models

	General	Telco/IT	University	Public Admin	Health	Industries	Supply chain	Research Agency	Hotel	Oil and Gas	Finance
A1									/		
A2				/							
A3				/							
A4										/	
A5			/								
A6											/
A7					/						
A8			/								
A9			/								
A10	/		/	/		/					
A11		/									
A12	/					/					
A13			/								
A14				/							
A15	/										
A16	/	/	/	/	/						
A17								/			
A18						/					
A19							/				
A20	/										
A21	/										
A22		/	/	/			/				
A23		/									
A24								/			
A25				/							
A26	/					/					
A27					/						
A28		/									
A29	/										
A30		/									
A31	/										
A32	/										

5.2. RQ2: What are the Limitations of Information Security Policy Compliance Behavior Models?

While numerous empirical studies have been undertaken to provide a complete understanding of the information security compliance phenomena, many limitations remain unanswered. Table 6 summarizes the list of limitations based on 32 articles chosen for this review. Seven (7) main limitations were identified, namely lack of generalizability, response biases, lack of theory consciousness, inappropriate sample size, criticality, and correlation versus causality problem.

Table 6: Limitation of the Information Security Policy Compliance Behavior Models

Article Id	Limitation
A1	Lack of generalizability as focus on four- and five-star hotels
A2	Small sample size (122) and only conducted in three key public sector information technology organizations in Nigeria
A3	Lack of theory consciousness as only one factor is focused on the main theory while ignoring the rest of the factors
A4	Data were collected from respondents whom both had formal ISPs implemented in their organizations and from those without formal ISPs, and this might have adverse effects on the results
A5	It employed a cross-sectional approach, which does not permit concluding causal direction and self-reporting biases
A6	Small sample population
A7	Lack of generalizability due to a single industry (governmental healthcare centers)
A8	Lack of generalizability due to a single industry (Higher education)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A9	Only concentrated on perceived factors
A10	An uneven sample size of organization from each group
A11	Self-reporting biases and lacks generalization due to single industry (Telecommunication)
A12	Comparison is based on uneven sample size from each group - bias
A13	Lack of generalizability and common method biases.
A14	Lack of generalization
A15	No theoretical analysis but only combines assumptions of theories
A16	Lack of generalizability due to environmental differences,
A17	No theory to support the ground
A18	Less critical industries
A19	Correlation versus causality problem because research is done at different time points
A20	Very small sample size respondent
A21	Lack of generalizability
A22	Lack of samples generalization and inability to control double responses by participants
A23	Lack of generalization because the respondents are only IT experts.
A24	Lack of generalizability – research agency
A25	Lack of generalizability –public organization in Oman
A26	Limited generalizability due to controlled laboratory experiment
A27	Lack of generalizability (health) and fewer factors explored
A28	Lack of generalizability because of a small sample size
A29	Response bias because of web-based survey
A30	Lack of generalization due to respondents only consist of young professionals and cultural differences among regions
A31	Lack of generalization due to cultural differences
A32	Problematic coordination of multiple theories

5.3. RQ3: What are the Underlying Theories and Concepts of Information Security Policy Compliance Behavior Models?

Literature analysis shows that a wide selection of theories and concepts were explored to measure information security compliance behavior. Table 7 list down the theories applied to each article in this review. It could be observed that each study emphasized the significance of a particular theory or theories or concepts while ignoring the rest.

Articles A11[35], A12[36], A13[23] and A18 [9], and A29 [10] used single theory while all other studies used more than one theory. It is interesting to note that the models presented in the studies used many combinations and extensions of theories. However, one study A17 [37] is not based on any particular theory.

Table 7: Theories and Concepts of the Identified Models

Article Id	Theory
A1	General deterrence theory
A2	Achievement motivation theory, Cultural value framework, Theory of planned behavior, Technology-organization and environment theory
A3	Information security climate, protection motivation theory
A4	Organizational governance and social bond theory
A5	Information security education, training, and awareness
A6	Theory of planned behavior, rational choice theory, information security awareness
A7	General deterrence theory, protection motivation theory, rational choice theory, theory of planned behavior, cognitive moral development theory
A8	Theory of planned behavior, Protection motivation theory, General deterrence theory and Organizational theory
A9	General deterrence theory, Protection motivation theory, Theory of planned behavior, and Information reinforcement
A10	Paternalistic leadership and social bond theory
A11	Social cognitive theory
A12	Theory of planned behavior
A13	General deterrence theory
A14	Social bond theory and General deterrence theory
A15	Theory of interpersonal behavior, Extended protection motivation theory, Neutralization theory, and Extended parallel processing model
A16	Involvement theory and Theory of organizational behavior policy
A17	No theory
A18	Rational choice theory
A19	Intrinsic and extrinsic motivators
A20	Rational choice theory, Theory of planned behavior, Cognitive and affective conditions
A21	Theory of norm activation, Social standards, and Ethical climate

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A22	Involvement theory and Social bond theory
A23	Theory of planned behavior and Protection motivation theory
A24	Protection motivation theory and Theory of planned behavior
A25	Socio-organizational factors
A26	Organizational control theory and Psychological reactance theory
A27	Health belief model
A28	Theory of planned behavior, Social bond theory, and Social cognitive theory
A29	Protection motivation theory, Theory of reasoned action, and Cognitive evaluation theory
A30	Neutralization theory and General deterrence theory
A31	Theory of planned behavior, Organismic integration theory (sub theory of the Self-determination theory)
A32	Planned action theory, Rational choice theory, Neutralization theory, and Protection motivation theory

Moving forward, we have listed the 20 theories used as a main/ground theory in the information security policy compliance behavior models. Table 8 shows the list of theories based on their original subject area/theory domains such as psychology, criminology, education, health, and management. They are theory of planned behavior by Ajzen (1985) [52], previously known theory of reasoned action by Fishbein and Ajzen (1975), protection motivation theory by Rogers (1975) [53], self-determination theory by Ryan and Deci (2000) [54], social cognitive theory by Bandura (1989) [55], theory of interpersonal behavior by Triandis (1977) [56], psychological reactance theory by Brehm (1966) [57], norm activation theory by Schwartz (1977) [58], cognitive evaluation theory by Deci and Cascio (1975) [59], Achievement Motivation Theory by Maslow, (1943) [60], Cognitive Moral Development Theory by Kohlberg & Hersh (1977) [61], general deterrence theory by Gibbs (1975) [62], neutralization theory by Sykes and Matza (1957) [63] , social bond theory also known as social control theory by Hirschi (1969) [64], rational choice theory by Becker (1974) [65], involvement theory by Astin (1999) [66], health belief model by Becker (1974) [67], extended parallel processing model by Witte (1992) [68], organizational control theory by Ouchi and Maguire (1975) [69], organizational behavior theory by Davis and Newstorm (1989) [70] and Technology-Organisation and Environment (TOE) by Tornatzky, Fleischer, and Chakrabarti, (1990) [71].

Besides that, alternative research concepts and approaches were also explored including intrinsic and extrinsic motivators by A19 [38], Socio-organizational factors by A27 [40], Cultural Value Framework by A2 [41], Information security climate by A3 [43], Organizational governance by A4 [42], security education, training, and awareness (SETA) by A5 [30], and information security awareness by A6 [45].

Table 8: Identified Theories According to Domains of the Theories

Psychology	• Theory of Planned Behavior [52] • Protection Motivation Theory [53] • Self Determination Theory [54] • Social Cognitive Theory [55] • Theory of Interpersonal Behavior [56] • Psychological Reactance Theory [57] • Norm Activation Theory [58] • Cognitive Evaluation Theory [59] • Achievement Motivation Theory [60] • Cognitive Moral Development Theory [61]
Criminology	• General Deterrence Theory [62] • Neutralization theory [63] • Social Bond Theory / Social Control Theory [64] • Rational Choice Theory [65]
Education	• Involvement Theory [66]
Health	• Health belief model [67] • Extended Parallel Processing Model [68]
Management -Organisation	• Organisational Control Theory [69] • Organizational Behaviour Theory [70] • Technology-Organisation and Environment (TOE) [71]

5.4. RQ4: What are the Influencing Factors of Information Security Policy Compliance Behavior Models

A total of 60 independent factors were identified from 32 selected models in this review. These factors were studied based on the motivation to comply with information security policy either directly or indirectly. However, it was discovered that each factor explained a small part of the variation in their behavior. Table 9 shows the list of 60 factors listed

with their alternative names, their pertinent theories, and definition.

We retrieved every factor and its definitions from each study. The definitions obtained were used to distinguish the same factors were examined. The definitions and measuring objects were used when studies adopted different names but represented the same concepts. A huge number of factors with different names but had the same content were merged. A detailed evaluation by comparing the definition of factors and was carried out until the factors were viewed as the same factor for conceptualizations.

Many factors had the same name and meanings and parts of different theories. For example, the variable 'Perceived Benefit' was found in the general deterrence theory, this was the same with the rational choice theory and health belief model too.

Ten (10) factors do not belong to any theories such as role values, psychological contract fulfillment, training support, moral beliefs, daily organizational citizenship behavior, organizational deviance, co-worker compliance, personal responsibility, security support, and anticipated regret. These are one-off factors suggested and tested by researchers based on their literature review or model verification or expert opinions.

Table 9: Influencing Factors from the Identified Studies

	Primary Factors	Relevant Theories	Definition
1.	Attitudes	• Theory of planned behavior	Attitude is defined as the individual's favorable or unfavorable feelings towards engaging in a specified behavior. [1], [25]
2.	Subjective Norms / Normative Belief/ Perceived Norm /Normative Faith	• Theory of planned behavior • Social cognitive theory	A person's interpretation of who is important to them such as the supervisor, colleague, and manager think about a given behavior [1], [3]
3.	Perceived Behavioural Control	• Theory of planned behavior	Perception of an activity or action that is easy or hard to execute [25]
4.	Threat Severity / Perceived Severity	• Protection motivation theory • Health belief model	A person's view of the seriousness of a security breach and the possible dangers that may result from the breaches [10]
5.	Threat Susceptibility / Perceived Susceptibility / Perceived Vulnerability	• Protection motivation theory • Health belief model	The people's assessment of their likelihood of being subjected to harmful threats such as how the person thinks a negative incident may occur if no action is taken to fix the problem [10]
6.	Response Efficacy	• Protection motivation theory	The employee's belief in whether the existing information security policies and procedures are capable of stopping potential information breaches [10]
7.	Self-Efficacy	• Protection motivation theory • Social cognitive theory	It is the confidence of a person in his or her skills and abilities [1], founded on optimism and reasoning capabilities and perhaps known a self-assessment[25]
8.	Response Cost	• Protection motivation theory	The individual's perception of external or intrinsic personal costs of carrying out the proposed adaptive actions [72]
9.	Outcome Expectation	• Social cognitive theory	A form of expectation relevant to a behavior based on observation in the workplace where employees analyze the significant actions of others and the implications of actions using their standards [35]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

10.	Information Security Monitoring	• Social cognitive theory	The action was taken by organizations to track the behaviors of employees thru the organization's IT facility [35].
11.	Perceived Inconvenience	• Social cognitive theory	Perception of troublesomeness
12.	Deterrence	• General deterrence theory	The effect of restrictions to prevent information security violations [24]
13.	Habit	• Theory of interpersonal behavior	The form of automatic response that builds as people repeat acts in stable conditions [73]
14.	Fear	• Extended parallel processing model	Negative emotional response to stimulations [14]
15.	Supportive organizational culture	• Organizational behavior theory	The employee's attitudes, perceptions, opinions, principles, and knowledge that in place when they communicate with the organization's processes and procedures at any moment [29]
16.	End-user involvement	• Involvement theory • Social bond theory (indirect to attitude)	The workers are engaged in the development or upgrading of security policies and it should be accepted and complied too. [29]
17.	Leadership	• Organizational behavior theory	The use of non - violent intervention to guide and organize the people towards goal fulfillment [29]
18.	Sanction Severity	• General deterrence theory	The degree of punishment if the user does not comply with the information security policy [37]
19.	Perceived Benefits	• General deterrence theory • Rational choice theory • Health belief model	The complete desirable outcomes expected in compliance with the cyber information security policy [9]
20.	Perceived cost	• Rational choice theory	An employees' expense of performing compliance action [9]
21.	Relatedness	• Self-determination theory	The intimate bonding a person has with his or her information [72]
22.	Competence	• Self-Determination Theory	The trust of the person in his or her capacity to study about and perform a range of work on a computer within a specific area, like security-focused activities. competency is synonymous with self-efficacy [72]
23.	Autonomy	• Self-determination theory	The availability of options open to respondents, as well as the right to select from certain options [72]
24.	Response Performance Motivation	• Self-determination theory	The motivation towards performing the recommended response [72]
25.	Experience	• Involvement Theory	Earlier experience of the person in coping with cyber threats could enable them to be conscious of similar threats and develop their skills in information security practice [4], [73].

26.	Personal Norms	• Social norms theory • Social bond theory	One's feelings on information security compliance with organizational information security policies [4], [6].
27.	Knowledge Sharing	• Involvement Theory	Exchanging information of a subject, fact, skill, knowledge, or competence theoretically or practically which was gained from education or experience to fix a problem, develop new ideas, or enforce policies and procedures [4], [74]
28.	Collaboration	• Involvement theory	Act together to accomplish a job or a mission [4].
29.	Attachment	• Social bond theory	A person's respect and love for their colleague, superior, and even their career and company. [4]
30.	Commitment	• Social bond theory	Dedication towards the organizational policy by safeguarding informational assets [4].
31.	Security Precautions	• Organizational control theory	To what extent a person perceives that they are taking measures to safeguard their computers to follow current information security policy [5], [75]
32.	Formal Control	• Organizational control theory	The existing organizational, formal information security policy controls [5]
33.	Mandatoriness	• Organizational control theory	The extent to which employees understand that they required to comply with established security policies and procedures as anticipated by management [5]
34.	Reactance	• Reactance theory	The adverse feelings reaction triggered by threats or deprivation of freedom of behavior and concentrating on retrieving the concerned freedom [5], [57]
35.	Perceived barrier	• Health belief model	Interpretations of the user regarding the complication in exercising computer security behavior [40], [76]
36.	Cues to action	• Health belief model	The views of employees on cybersecurity programs, media news, and social influences adopted in the corporation [40], [76]
37.	Locus of control	• Social cognitive theory	The extent that a person thinks he or she can influence things that affect them directly or indirectly [1]
38.	Awareness of Consequences	• Norm activation theory	The understanding that a worker has of how their actions of information security influence the wellbeing of their colleagues and the organization [6]
39.	Ascription of Personal Responsibility	• Norm activation theory	The employee feels responsible for the good or bad consequences of actions related to information security policies [6]
40.	Rewards	• Cognitive evaluation theory	What is offered in acknowledgment of someone's service, commitment, or

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

			accomplishment [10]
41.	Perceived Detection Certainty	• General deterrence theory	The probability of individual's belief that their deviant behavior will be caught [27]
42.	Internal perceived locus of causality	• Organismic integration theory	A person's assessment of his or her particular behavior as something that is meaningful [28]
43.	External perceived locus of causality	• Organismic integration theory	An individual perceives his or her behavior as being dominated by outside factors [28]
44.	Role Values	• Not from any theory	Compliance with the relevant information security policy action is necessary, justified, and reasonable, taking into account the nature of the job and the role the individual performs [14]
45.	Psychological Contract Fulfillment	• Not from any theory	A person assumption regarding the collective responsibilities that exist between a person and his or her organization [9]
46.	Training Support	• Not from any theory	Different training methods (according to research by [4]. The definition is not available
47.	Moral Beliefs	• Not from any theory	The degree to which the person finds the information security policy breach in the organization to be ethically wrong [39]
48.	Daily Organisational	• Not from any theory	The reflective of the worker's concern for the successful
	Citizenship Behaviour		operation of the organization, including encouraging and aiding others [39], [77]
49.	Organizational Deviance	• Not from any theory	Voluntary actions that breach key organizational guidelines and then jeopardize the organization and its members [39], [78]
50.	Co-Worker Compliance	• Not from any theory	Internal pressure caused by colleagues towards information security policy conformity [39]
51.	Personal Responsibility	• Not from any theory	The perception that measures should be taken to accomplish the expected results [79]
52.	Security Support	• Not from any theory	A person's capability to use external support tools that can help enforce preventive action [80]
53.	Anticipated Regret	• Not from any theory	The prediction of the unpleasant, cognitive-based feelings that we encountered when we discovered that perhaps the current situation might have been better if we had behaved differently. [2], [81]
54.	Perceived deterrent certainty	• General deterrence theory	Employees' perception of the probability of being punished associated with breaking information security policies [82]
55.	Leadership	• Achievement Motivation Theory of	The presence of an individual who influences a group of individuals to achieve a common goal

		Leadership	[83]
56.	Goal-Oriented Cultural Value	• Cultural Value Framework (CVF)	Values espoused by the employee in the belief that performance and appraisal are directly related to the attainment of organizational goals clearly defined by leadership [84]
57.	Rule Orientate Cultural Value	• Cultural Value Framework (CVF)	Espoused values by the employee in the belief that jobs and tasks are performed according to job specifications and clearly defines the procedure by everyone in the organization [84]
58.	Security Technologies	• Technology-Organisation and Environment (TOE) theory	Security mechanism deployed in establishing the requirement of organizational cybersecurity policies and standards in providing secured communication, protect IT assets [85]
59.	Workplace Capabilities (WPC)	• Organizational Governance	WPC include a set of sub-factors, such as the usability of systems, employee turnover, reliance on temporary employees, competency of employees, the effectiveness of monitoring procedures, job satisfaction, task pressure, task significance, security practices, disciplinary procedure, security monitoring, supervision, performance, and rewards. [84]
60.	Information security climate	• Not from any theory	Information security climate reflects a collection of norms, beliefs, values, and fundamental assumptions shared by organizational members on how information security matters [43]

6. FINDINGS

6.1. Model Domains

Information security policy compliance behavior models were largely developed for the general domain (23%). This may be due to information security compliance problem happens in every domain and the researchers feel that it can be addressed collectively. Moderately explored domains are namely university (16%) and public administration (16%), telecommunication/IT (13%), industries (9%), and health (5%). Meanwhile, domains that were least explored by researchers are supply chain (5%), research agency (5%), hotel (2%), oil and gas (2%), and finance (2%). Figure 3 shows the clustered column chart according to the domain in percentages.

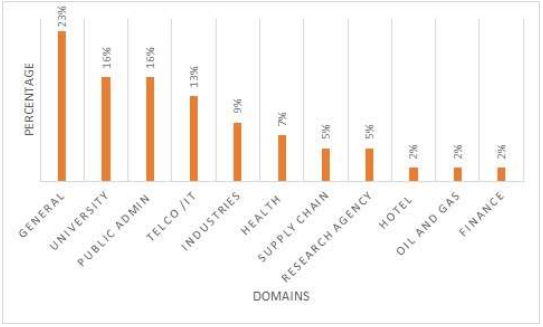

Figure 3: Information Security Policy Compliance Model's Domains in Percentage

This review discovered that researchers (around 16%) tend to test their models in different domains simultaneously such as A10 [34], A12[36], A16 [29], A22 [4], A30 [27], A31 [28] and A32 [3]. For example, A10 [34] respondents came from 13 companies, 4 government agencies, 10 master of bachelor administration (MBA) classes, and 4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Executive Development Programs (EDP) in China. Meanwhile A16 [29] population sample was from the banking, insurance, education, hospitality, IT/Telecommunications, essential services (medical, water, and electricity), and other sectors in Ghana. Besides that, Article A22 [4] tested their model in four different companies (retail/wholesale, telecommunication/it, education, government). Although this practice can increase generalizability it can lead to research frame biases because the diversity of the domains tested differed widely from each other and could not produce a reliable or consistent result. Alternately, researchers could have produced a comparison between those domains.

6.2. Limitations

This paper further calculated the frequency of the particular limitations and then highlighted the reasons behind the limitations found as in Table 10. The most prominent limitation in information security compliance behavior model studies is the lack of generalizability (about 40%) which is nearly half of the studies. This is mostly because the model was tested either in a single company in a single domain that did not consider environmental or cultural differences or focuses on a single group of people and so on. Because of this, researchers were unable to generalize their studies to a greater set of populations or common sets.

Lack of theory consciousness was found in 19% of studies. This occurs when researchers simply combine assumptions of theories without much proper theoretical analysis. None of the papers reported how or on what basis it could combine theories or factors from different theories. This problem is only realized and mentioned by A15 [14] and A32 [3]. Researcher Sommestad [2] identified this problem and studied the sufficiency of a single theory in his paper.

The inappropriate sample size or irrelevant sample was also found in 19% of studies. Most of these studies consist of a low sample size. A low sample size may produce inaccurate results. Yet, those researchers apply PLS-SEM technique to conduct their analysis where PLS-SEM software able to analyze with a low sample size. The irrelevant sample is referring to the extraneous respondents whose responses are taken into the sample population for analysis such as in A4 [42], A10 [34], A20 [39], and A28 [1].

Response biases also common limitations found in 16% of studies. That research collects data from web-based surveys or self-reporting. According to [86], respondents who believed that they demonstrate safe behaviors may think they complied with the policy, even if they do not, producing response biases. Besides that, criticality problem found in Article A18 [9] and correlation versus causality problem found in Article A19 [38].

Table 10: Frequency of limitations and their Reasons

Limitations	Frequency	Reasons for Limitations
Lack of generalizability	13	• Single industry • Environmental differences • Cultural differences among regions • A single group of people (IT experts, young professionals) • Controlled laboratory experiment
Response biases	5	• Self-reporting biases / common method biases • Web-based survey
Lack of theory consciousness	6	• No theoretical analysis and only combines assumptions of theories • No theory to support the ground • Fewer factors explored
Inappropriate sample Size and irrelevant Sample	6	• Very small sample size respondent • Inability to control double responses by participants • Comparison of an uneven sample size from each group
Criticality	1	• Less critical industries
Correlation versus causality problem	1	• Research is done at different time points

6.3. Theories

This review further made a theoretical analysis of information security policy compliance behavior models as in Figure 4, It was found that the theory of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

planned behavior is the most favored in information security compliance behaviour models, where 21% of studies applied it in their research. It is evident that the theory of planned behavior provided the most reliable findings and best described the behavioral intentions based on widely proven quantitative approaches. The theory of planned behavior is a revised version theory of reasoned action by Fishbein and Ajzen (1975) where they included the perceived behavioral control as an additional factor. The basic principle of this theory is intentions projected by the person's attitude to the behavior and any related subjective norms [87]. Therefore, the theory of planned behavior is considered to equip a consistent basis on understanding employees' security compliance decisions by academicians in recent years.

Besides that, the protection motivation theory was also widely considered as an important theory in explaining and predicting information security policy compliance behavior where 16% of studies in information security policy compliance applied protection motivation theory in their studies. Rogers (1975) proposed the protection motivation theory (PMT) to explain behaviors that are provoked when fear appeals to the present where fear is related to emotion rather than rational processing mind.

Meanwhile, the general deterrence theory was also used fairly as 12% of studies explored this theory. Social bond theory, rational choice theory, and neutralization theory were explored moderately with around 8%, 8%, and 5% each. Theories such as the involvement theory and social cognitive theory explored novice as only 3% of studies backed on these theories.

The least used theories are the Self Determination Theory, Theory of Interpersonal Behavior, Psychological Reactance Theory, Norm Activation Theory, Cognitive Evaluation Theory, Health Belief Model, Extended Parallel Processing Model, Organizational Control Theory, Organizational Behavior Theory, Achievement Motivation Theory, Technology-Organisation and Environment (TOE) Theory. These theories were only explored in 2% of studies in the information security policy compliance behavior field.

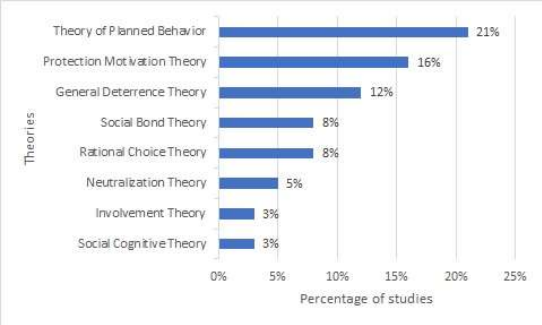

Figure 4: Theories in Information Security Policy Compliance Behavior Models

6.4. Factors

The most promising factors are shown in Table 11 arranged in descending order based on the total number of studies taking into consideration that the factor must be studied at least twice for better reliability and consistency. While the basic foundations of many studies are identical, there is a wide difference between the factors being studied where fifty (50) of the factors were only studied in a single study. The analysis of relevant factors revealed that many factors fall into the individual context except information security monitoring, deterrence, supportive organizational culture, formal control, mandatories, external perceived locus of causality, training support, organizational deviance, and security support which fall under organization context but surprisingly, one fall into the technological context which is security technologies. This was probably because these models were only intended to study employee's behavior without the technical assistance in combating cyber threats.

Table 11: Most Dominant Factors

Factors	Frequency
Normative belief/ subjective norms / perceived norm /normative faith	16
Self-efficacy	14
Attitudes	12
Perceived benefits	5
Threat susceptibility / perceived susceptibility/ Vulnerability	5
Threat severity / perceived severity	5
Response efficacy	5
Response cost	3
Experience	3
Sanction severity / Perceived deterrent severity	2

Moving forward, every factor that was identified explored further in terms of the path coefficient to determine whether that factor is positively, negatively

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

associated, or not associated with the intention to comply (directly or indirectly) in every article. Intention to comply is the dependent variable that was studied in all models in this review. Every path was measured by a number named a standardized path coefficient, which shows the direction and effects of the relationship between the exogenous factor and the endogenous factor [32]. The path coefficients often range between −1 and + 1. Closer values to + 1 indicated a strong positive association between the two constructs and values closer to −1 indicated a strong negative association. Values close to 0 represent a weak association between the constructs [32].

Factors such as Self-Efficacy, Attitude, Perceived Benefits, Response Efficacy, and Threat Severity are proved to be positively associated with intention of compliance in every study that it contains. Hence these factors are reliable factors to be used in the information security compliance model. Meanwhile, Training Support, Involvement, commitment, Beliefs, Experience, and Personal Norms directly have positive associations with some studies and indirectly have a positive association or positively mediates in some other studies. These indicate that these factors can be safely used to predict positive association to the intention of compliance. On the other hand, the subjective norms factor being the top-ranked in the most used factors was rendered positive association in more than 12 studies but was rendered no association in 2 studies A11 [35] and A20 [39]]. This might be caused by a measurement error and could be ignored.

However, factors such as Sanction Severity, have positive associations in two studies A17 [31] and A30 [27] and no association with another study A1 [44]. Other than that, factors such as perceived susceptibility vulnerability have positive association in one study, A29 [10], and no association in another study, A27 [40]. The same goes for the perceived behavioral control factor where it was found to have positive association in A24 [2] and also no association in another study A23 [25]. Moreover, the Attachment factor rendered positive association directly to intention to comply in A4 [42] and as a mediator in A10 [34] but rendered no association in A22 indirectly. The role values factor also inconsistent where it rendered indirect positive associated in A15 study and indirect negative associated in A19 study. This indicates factors such as Sanction Severity, perceived susceptibility vulnerability perceived behavioral control, attachment, and role value require more studies to evaluate further.

Fifty (50) other factors have only been investigated in a single study each and their outcome was extracted too. Factors such as outcome expectation, information security monitoring, perceived inconvenience, deterrence, supportive organizational culture, psychological contract fulfillment, co-worker compliance, the ascription of personal responsibility, anticipated regret, formal control, mandatories, cues to action, locus of control, and internal perceived locus of causality, perceived deterrent certainty, cybersecurity knowledge, perceived cost, information security climate, and leadership rendered positive association with intention of compliance while knowledge sharing and collaboration have an indirect positive association in their respective studies.

Factors such as response cost, habit, fear, perceived cost, organizational deviance, reactance, perceived barrier, rewards, and perceived detection certainty were rendered negative association in their respected studies thus far. For example, when fear increase, the information security policies compliance behavior intention decreases. As for rewards, the higher rewards do not guarantee compliance but incompliance. This seems to be very contradicting and in need of more data to confirm. Factors such as leadership, daily organizational citizenship behavior, awareness of consequences, security precautions, leadership, goal oriented cultural value, rule orientate cultural value, security technologies showed no association with any intention of compliance and thus could be a poor choice of factors for the information security policy compliance model.

The extracted data regarding factors associated with intention of compliance would offer great insights in building hypotheses in future studies. Hence, one of the main concerns here would be publication bias where the researcher generally tends to publish only significant or positive results more often than insignificant or negative results.

7. DISCUSSIONS AND FUTURE DIRECTIONS

Thirty-two (32) information security policy compliance behavior models analyzed in this review. A total of twenty (20) theories were extracted from those models and explored further. Then, a total of sixty (60) factors is studied with regards to information security policy compliance intention.

A consistent number of studies in recent years revealed that information security policy compliance behavior is niche and very much needed in even in tech-savvy organizations. However, a majority

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

number of models were developed for general reasons instead of field specific. This led to the generalizability error because the nature of business and environment differed in each domain or organization and may and may not suit the general model. Hence, the domain-specific or organization-specific models will enhance the adaptation of the models to increase information security compliance. Future studies should consider this besides improving methodology errors such as response biases and sample size.

In terms of theories, information security policy compliance behaviors studies included in this review derived factors and relationships from established theories from various domains, especially from Psychology and Criminology. This is because the researcher tends to study behavior in terms of psychology and compliance and noncompliance in terms of criminology. Even though the theory of planned behavior and protection motivation theory were considered excellent theories in information security compliance behavior dominance, other theories such as general deterrence theory, social bond theory, rational choice theory, neutralization theory, involvement theory, and social cognitive theory also offer interesting alternative perspectives. They however have yet to receive much empirical validation in this field.

In terms of factors, it was discovered that each factor described a small part of behavior. Factors such as self-efficacy, attitude, perceived benefit, threat severity, response efficacy, sanction severity, personal norms, experience, and training support factors have trustable ability to increase information security compliance behavior. This is because they are not only the most examined factors but were also able to predict information compliance intentions in a meaningful way.

However, it was discovered that most researchers combined factors from different theories in their models either entirely or partially. Therefore, the theory consciousness is very important to produce effective models and improve the current models.

Studies included in this review presented mixed results of information security policy compliance in terms of its significance from one study to another. Possible reasons behind the inconsistency results in findings are different measurement scales, the difference in the quality of the studies, different research methods, and different sample frames such as different domains, countries, industries, and so on. Future research should look into stricter testing of the theories with better sampling procedures and investigations of factors' relationship as well.

8. LIMITATIONS OF THE STUDY

This systematic literature review relied on a relatively limited number of databases which is twelve (12) databases namely Academic search premier (EBSCO host), ACM digital library, Emerald Insight, IEEEXplore digital library, Springer link, Science direct, Scopus, Web of Science, Oxford academic journals, SAGE journals, Taylor & Francis and the Wiley online library for the identification of potentially eligible studies. The inclusion of more databases especially google scholar certainly produce more eligible studies for this review.

Besides that, quality assessment methods were non-standardized. This limits the diagnostic of study included in this study. For example, Quadas which is a tool to assess the quality of diagnostic accuracy studies could have been included in this systematic review.

In addition, quality assessment in this review which excludes studies that are mainly on non-compliance or framework limited the identification of potentially eligible studies.

9. CONCLUSIONS

This SLR paper able to address core aspect of current information security compliance behavior models such as relevant theories and factors that influence the information security policy compliance behavior in previous studies. Important theories and factors emerged from this review. This review further detailed out each theory and factors that were not found in previous reviews.

From the review of information security policy compliance behavior models, it can be concluded that the importance of information security compliance behavior invited high interest among academic researchers in this research area. The vast number of new prediction models used to study security policy compliance indicates that none of the existing theories were suitable for the study of information security policy compliance on their own which requires the security community to produce new and improved models.

This systematic review of information security compliance literature provided an in-depth review of relevant models, theories, and influencing factors that have been adopted to study this information security policy compliance problem.The search strategy

resulted in 5,133 studies, of which 32 were identified as primary studies and a synthesise of twenty (20) theories and sixty (60) factors that are pertinent to this study is presented. In doing so, this study makes important contributions, namely (i) identification of limitations, (ii) domains (iii) reliable theories, and (iv) reliable factors of information security policy compliance behavior models. It would help fellow researchers to identify the merits of the most trustable theories and important factors and whether certain changes or considerations are relevant for behavior related to information security policy compliance. Such reviews must pave the way to new empirical studies addressing information security policy compliance.

Compliance is regarded as a complicated concept and should be discovered from a wide range of angles and realizing this gap, for future research the author will be in investigating information security compliance behavior through empirical research based on promising theoretical lenses. This would advance the current knowledge in the field.

10. ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewer who provided a discerning perspective on our work.

REFERENCES

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

[2] T. Sommestad, H. Karlzén, and J. Hallberg, "The sufficiency of the theory of planned behavior for explaining information security policy compliance," *Inf. Comput. Secur.*, vol. 23, no. 2, pp. 200–217, 2015.

[3] S. H. Kim, K. H. Yang, and S. Park, "An Integrative Behavioral Model of Information Security Policy Compliance," *Sci. World J.*, vol. 2014, pp. 1–12, 2014.

[4] N. Sohrabi Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Comput. Secur.*, vol. 56, pp. 1–13, 2016.

[5] P. B. Lowry and G. D. Moody, "Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies," *Inf. Syst. J.*, vol. 25, no. 5, pp. 433–463, 2015.

[6] A. Yazdanmehr and J. Wang, "Employees' information security policy compliance: A norm activation perspective," *Decis. Support Syst.*, vol. 92, pp. 36–46, 2016.

[7] P. Ifinedo, "Roles of Organizational Climate, Social Bonds, and Perceptions of Security Threats on IS Security Policy Compliance Intentions," *Inf. Resour. Manag. J.*, vol. 31, no. 1, pp. 53–82, 2018.

[8] T. Sommestad, J. Hallberg, K. Lundholm, and J. Bengtsson, "Variables influencing information security policy compliance: A systematic review of quantitative studies," *Inf. Manag. Comput. Secur.*, vol. 22, no. 1, pp. 42–75, 2014.

[9] J. Y. Han, Y. J. Kim, and H. Kim, "An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective," *Comput. Secur.*, vol. 66, pp. 52–65, 2017.

[10] M. Siponen, M. Adam Mahmood, and S. Pahnila, "Employees' adherence to information security policies: An exploratory field study," *Inf. Manag.*, vol. 51, no. 2, pp. 217–224, 2014.

[11] J. A. Alalwan, "Fear of Cybercrime and the Compliance with Information Security Policies : A Theoretical Study," no. 2008, pp. 85–87, 2018.

[12] M. Daud, R. Rasiah, M. George, D. Asirvatham, and G. Thangiah, "Bridging the gap between organisational practices and cyber security compliance: Can cooperation promote compliance in organisations?," *Int. J. Bus. Soc.*, vol. 19, no. 1, pp. 161–180, 2018.

[13] A. Nasir, M. Rashid, and A. Hamid, "Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture : A Conceptual Framework," pp. 56–60, 2017.

[14] G. D. Moody, M. Siponen, and S. Pahnila, *Toward a Unified Model of Information Security Policy Compliance*, vol. 42, no. 1. 2018, pp. 285–311.

[15] J. D. Wall, P. Palvia, and P. B. Lowry, "Control-related motivations and information security policy compliance: The role of autonomy and efficacy," *J. Inf. Priv. Secur.*, vol. 9, no. 4, pp. 52–79, 2013.

[16] W. A. Cram, J. G. Proudfoot, and J. D'Arcy, "Organizational information security policies: A review and research framework," *Eur. J. Inf. Syst.*, vol. 26, no. 6, pp. 605–641, 2017.

[17] Angraini, R. A. Alias, and Okfalisa,

"Information security policy compliance: Systematic literature review," *Procedia Comput. Sci.*, vol. 161, pp. 1216–1224, 2019.

[18] R. F. Ali, P. D. D. Dominic, S. E. A. Ali, M. Rehman, and A. Sohail, "Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance," *Appl. Sci.*, vol. 11, no. 8, p. 3383, 2021.

[19] B. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering Executive summary," 2007.

[20] C. Okoli and K. Schabram, "Working Papers on Information Systems - A Guide to Conducting a Systematic Literature Review of Information Systems Research A Guide to Conducting a Systematic Literature Review of Information Systems Research," *Sprouts*, vol. 10, no. 2010, p. 51, 2010.

[21] M. Petticrew and H. Roberts, *Systematic reviews in the social sciences: A practical guide*. John Wiley & Sons, 2008.

[22] N. Salleh, E. Mendes, and J. C. Grundy, "Empirical studies of pair programming for CS/SE teaching in higher education: A systematic literature review," *IEEE Trans. Softw. Eng.*, vol. 37, no. 4, pp. 509–525, 2011.

[23] X. Chen, D. Wu, L. Chen, and J. K. L. Teng, "Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables," *Inf. Manag.*, no. May, pp. 1–12, 2018.

[24] M. Choi and J. Song, "Social control through deterrence on the compliance with information security policy," *Soft Comput.*, no. 2009, 2018.

[25] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan, "Information security conscious care behaviour formation in organizations," *Comput. Secur.*, vol. 53, pp. 65–78, 2015.

[26] A. Alkalbani, H. Deng, and B. Kam, "Investigating the role of socio-organizational factors in the information security compliance in organizations," in *Australasian Conference on Information Systems*, 2015, no. 2010.

[27] L. Cheng, W. Li, Q. Zhai, and R. Smyth, "Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory," *Comput. Human Behav.*, vol. 38, pp. 220–228, 2014.

[28] J. Kranz and F. Haeussinger, "Why Deterrence is not enough : The Role of Endogenous Motivations on Employees ' Information Security Behavior," no. December, 2014.

[29] E. Amankwa, M. Loock, and E. Kritzinger, "Establishing information security policy compliance culture in organizations," in *Information & Computer Security*, 2018, vol. 26, no. 4, pp. 420–436.

[30] G. Dhillon, Y. Y. A. Talib, and W. N. Picoto, "The mediating role of psychological empowerment in information security compliance intentions," *J. Assoc. Inf. Syst.*, vol. 21, no. 1, pp. 152–174, 2020.

[31] S. T. Alanazi, M. Anbar, S. A. Ebad, S. Karuppayah, and H. A. Al-Ani, "Theory-based model and prediction analysis of information security compliance behavior in the Saudi healthcare sector," *Symmetry (Basel).*, vol. 12, no. 9, pp. 1–21, 2020.

[32] M. Rajab and A. Eydgahi, "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education," *Comput. Secur.*, vol. 80, pp. 211–223, 2019.

[33] Y. M. Iriqat, A. R. Ahlan, and N. N. A. Molok, "Information security policy perceived compliance among staff in palestine universities: An empirical pilot study," *2019 IEEE Jordan Int. Jt. Conf. Electr. Eng. Inf. Technol. JEEIT 2019 - Proc.*, pp. 580–585, 2019.

[34] G. Feng, J. Zhu, N. Wang, and H. Liang, "How Paternalistic Leadership Influences IT Security Policy Compliance : The Mediating Role of the Social Bond," vol. 20, pp. 1650–1691, 2019.

[35] Z. Ahmad, T. S. Ong, T. H. Liew, and M. Norhashim, "Security monitoring and information security assurance behaviour among employees," *Inf. Comput. Secur.*, vol. 27, no. 2, pp. 165–188, Jun. 2019.

[36] T. Sommestad, "Work-related groups and information security policy compliance," *Inf. Comput. Secur.*, vol. 26, no. 5, pp. 533–550, 2018.

[37] M. Razilan, A. Kadir, S. Norwahidah, S. Norman, S. A. Rahman, and A. Bunawan, "Information Security Policies Compliance among Employees in Cybersecurity Malaysia," in *Proceedings of the 28th International Business Information Management Association Conference*, 2016, no. November 2016.

[38] M. Hofeditz, A. M. Nienaber, A. Dysvik, and G. Schewe, "'Want to' Versus 'Have to': Intrinsic and Extrinsic Motivators as Predictors

of Compliance Behavior Intention," *Hum. Resour. Manage.*, vol. 56, no. 1, pp. 25–49, 2017.

[39] J. D'Arcy and P. B. Lowry, "Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study," *Inf. Syst. J.*, no. October, 2017.

[40] N. Humaidi, V. Balakrishnan, and M. Shahrom, "Exploring user's compliance behavior towards Health Information System security policies based on extended Health Belief Model," *2014 IEEE Conf. e-Learning, e-Management e-Services*, pp. 30–35, 2014.

[41] A. Onumo, I. Ullah-Awan, and A. Cullen, "Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures," *ACM Trans. Manag. Inf. Syst.*, vol. 12, no. 2, pp. 1–29, 2021.

[42] R. F. Ali, P. D. D. Dominic, and K. Ali, "Organizational governance, social bonds and information security policy compliance: a perspective towards oil and gas employees," *Sustain.*, vol. 12, no. 20, pp. 1–27, 2020.

[43] C. Liu, C. Wang, H. Wang, and B. Niu, "Influencing factors of employees' information systems security policy compliance: An empirical research in China," in *E3S Web of Conferences*, 2020, vol. 218.

[44] X. Wang and J. Xu, "Deterrence and leadership factors: Which are important for information security policy compliance in the hotel industry," *Tour. Manag.*, vol. 84, p. 104282, 2021.

[45] G. Carmi and D. Bouhnik, "The Effect of Rational Based Beliefs and Awareness on Employee Compliance with Information Security Procedures: A Case Study of a Financial Corporation in Israel," *Interdiscip. J. Information, Knowledge, Manag.*, vol. 15, pp. 109–125, 2020.

[46] S. Hina and D. D. Dominic, "Compliance : A Perspective in Higher Education Institutions," *Proc. 5th Int. Conf. Res. Innov. Inf. Syst.*, pp. 1–6, 2017.

[47] L. Connolly, M. Lang, and J. D. Tygar, "Investigation of Employee Security Behaviour: A Grounded Theory Approach," vol. 455, no. May, 2015.

[48] A. C. Johnston, M. Warkentin, and M. Siponen, "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric," *MIS Q.*, vol. 39, no. 1, pp. 113–134, 2015.

[49] D. Box and D. Pottas, "A Model for Information Security Compliant Behaviour in the Healthcare Context," *Procedia Technol.*, vol. 16, pp. 1462–1470, 2014.

[50] H. C. Pham, J. El-Den, and J. Richardson, "Stress-based security compliance model - An exploratory study," *Inf. Comput. Secur.*, vol. 24, no. 4, pp. 326–347, 2016.

[51] H. Stewart and J. Jurjens, "Information security management and the human aspect in organizations," *Inf. Comput. Secur.*, vol. 25, no. 5, pp. 494–534, 2017.

[52] I. Ajzen, "From Intentions to Actions: A Theory of Planned Behavior," *Action Control*, pp. 11–39, 1985.

[53] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *J. Psychol.*, vol. 91, no. 1, pp. 93–114, Sep. 1975.

[54] R. Ryan and E. Deci, "Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being.," *Am. Psychol.*, vol. 55, no. 1, pp. 68–78, 2000.

[55] A. Bandura, "Human agency in social cognitive theory.," *American Psychologist*, vol. 44, no. 9. American Psychological Association, US, pp. 1175–1184, 1989.

[56] H. C. Triandis, *Interpersonal behavior*. Brooks/Cole Pub. Co., 1977.

[57] J. W. Brehm, "A theory of psychological reactance.," 1966.

[58] S. H. Schwartz, "Normative Influences on Altruism '," no. September, 1977.

[59] K. J. Deci L, Cascio F, "Cognitive Evaluation Theory," *Personality and social psychology*, vol. 31, no. 1. pp. 81–85, 1975.

[60] A. H. Maslow, "A theory of human motivation.," *Psychol. Rev.*, vol. 50, no. 4, p. 370, 1943.

[61] L. Kohlberg and R. H. Hersh, "Moral development: A review of the theory," *Theory Pract.*, vol. 16, no. 2, pp. 53–59, 1977.

[62] J. P. Gibbs, *Crime, punishment, and deterrence*. Elsevier New York, 1975.

[63] G. M. Sykes and D. Matza, "Techniques of Nautralization: A Theory of Delinquency," *Am. Sociol. Rev.*, vol. 22, no. 6, pp. 664–670, 1957.

[64] T. Hirschi, "A control theory of delinquency," *Criminol. theory Sel. Class. readings*, vol. 1969, pp. 289–305, 1969.

[65] G. S. Becker, "A theory of social interactions," *NBER Work. Pap.*, vol. 42, no. 42, pp. 1–54,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1974.
[66] A. W. Astin, "Student involvement: A developmental theory for higher education.," 1999.
[67] M. H. Becker, "The health belief model and sick role behavior," *Health Educ. Monogr.*, vol. 2, no. 4, pp. 409–419, 1974.
[68] K. Witte, "Putting the fear back into fear appeals: The extended parallel process model," *Commun. Monogr.*, vol. 59, no. 4, pp. 329–349, Dec. 1992.
[69] W. G. Ouchi and M. A. Maguire, "Organizational control: Two functions," *Adm. Sci. Q.*, pp. 559–569, 1975.
[70] K. Davis and J. W. Newstrom, "Human behavior at work: Organizational behavior," 1989.
[71] L. G. Tornatzky, M. Fleischer, and A. K. Chakrabarti, *Processes of technological innovation*. Lexington books, 1990.
[72] P. Menard, G. J. Bott, and R. E. Crossler, "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory," *J. Manag. Inf. Syst.*, vol. 34, no. 4, pp. 1203–1230, 2017.
[73] H. Y. S. Tsai, M. Jiang, S. Alhabash, R. Larose, N. J. Rifon, and S. R. Cotten, "Understanding online safety behaviors: A protection motivation theory perspective," *Comput. Secur.*, vol. 59, no. 1318885, pp. 138–150, 2016.
[74] S. Wang and R. A. Noe, "Knowledge sharing: A review and directions for future research," *Hum. Resour. Manag. Rev.*, vol. 20, no. 2, pp. 115–131, 2010.
[75] S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler, and R. W. Boss, "If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security," *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 151–164, 2009.
[76] B. Y. Ng, A. Kankanhalli, and Y. (Calvin) Xu, "Studying users' computer security behavior: A health belief perspective," *Decis. Support Syst.*, vol. 46, no. 4, pp. 815–825, 2009.
[77] P. Organ, D. Podsakoff, and S. MacKenzie, "Organizational Citizenship Behaviour Its Nature Antecedents and Consequences." Sage Publications, 2006.
[78] R. J. Bennett and S. L. Robinson, "Development of a measure of workplace deviance," *J. Appl. Psychol.*, vol. 85, no. 3, pp. 349–360, 2000.
[79] R. Larose and N. Rifon, "Your privacy is assured of being disturbed: Websites with and without privacy seals," *New Media Soc.*, vol. 8, no. 6, pp. 1009–1029, 2006.
[80] P. Luarn and H.-H. Lin, "Toward an understanding of the behavioral intention to use mobile banking," *Comput. Human Behav.*, vol. 21, no. 6, pp. 873–891, 2005.
[81] T. Sandberg and M. Conner, "Anticipated regret as an additional predictor in the theory of planned behavior: A meta-analysis," *Br. J. Soc. Psychol.*, vol. 47, pp. 589–606, 2007.
[82] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Inf. Syst. Res.*, vol. 20, no. 1, pp. 79–98, 2009.
[83] D. C. McClelland and R. E. Boyatzis, "Leadership motive pattern and long-term success in management.," *J. Appl. Psychol.*, vol. 67, no. 6, p. 737, 1982.
[84] R. E. Quinn and J. Rohrbaugh, "A spatial model of effectiveness criteria: Towards a competing values approach to organizational analysis," *Manage. Sci.*, vol. 29, no. 3, pp. 363–377, 1983.
[85] R. Depietro, E. Wiarda, and M. Fleischer, "The context for change: Organization, technology and environment," *Process. Technol. Innov.*, vol. 199, no. 0, pp. 151–175, 1990.
[86] S. Kurowski, "Response biases in policy compliance research," *Inf. Comput. Secur.*, 2019.
[87] M. Fishbein and I. Ajzen, "Theory of Reasoned Action (TRA)." 1975.