IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 18, 2021, accepted November 30, 2021, date of publication December 3, 2021,
date of current version December 16, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3132574

Exploring the Influence of Direct and Indirect Factors on Information Security Policy Compliance: A Systematic Literature Review

MADA ALASSAF AND ALI ALKHALIFAH
Department of Information Technology, College of Computer, Qassim University, Buraydah 51921, Saudi Arabia
Corresponding author: Ali Alkhalifah (a.alkhalifah@qu.edu.sa)

ABSTRACT Information systems security is considered one of the key issues concerning organizations' management. Despite the massive investment that organizations make to safeguard their systems, there are still many internal security breaches. The increase in insider threats to information systems can be related to the employees' compliance toward information security policy. Several review papers were conducted to explore information security policy compliance behavior research. However, the literature lacks insight into the positive and negative (direct or indirect) influence of human and organizational theories and their factors influencing information security policy compliance behavior. Therefore, this paper provides a systematic literature review synthesizing the psychological theories, organizational theories, and other internal and external factors on information security policy compliance researches. The results analysis of 87 studies showed that the general deterrence theory, theory of planned behavior, and protection motivation theory are the most frequently used. The influencing factors of theories are mostly similar in the results. Furthermore, information security education, training and awareness, trust, and leadership, among many other internal and external factors, are highly used. This study is one of the first researches that explores the relationship types among the influencing factors; emphasizing the direct and indirect effect, and information security policy compliance behavior. This paper also identifies some gaps in information security policy compliance behavior research and proposes future works. In addition, it provides a theoretical contribution and practical insight in the context of information security policy compliance.

INDEX TERMS Compliance behavior, information security policy, information security policy compliance, systematic literature review.

I. INTRODUCTION

Due to globalization and interconnection, organizations rely heavily on information systems (IS) in their business processes [1]. Securing IS from potential threats and controlling the risk that relates to these systems must be an essential priority for organization management [2], [3]. To safeguard IS assets, multi-dimensional solutions can be applied; these are the technical, and non-technical solutions. The technical solutions that can be used to protect IS are installing a firewall, using data backup, downloading an antivirus program and implementing frequent system checks against threats. Non-technical solutions relate to the behavioral solutions to employee and organization issues [4], [5]. Many organizations realize that technology solutions alone were rarely sufficient to minimize the security threat because all the solutions were employed and managed by individuals [6], [7]. Studies confirmed that human behavior should be a focus when considering security solutions alongside technology, since individuals are considered the weakest link in the organization's security [8], [9]. An example can be seen in, the 2019 IBM X-Force Threat Intelligence Index which revealed that internal error was accountable for most of the incidents within the organization [10]. A study conducted in Britain found that 58% of attacks in organizations resulted from insider threats. 33% of these attacks resulted from non-compliance with information security policies [11].

To reduce organizational security threats, several organizations have applied various security standards and guidelines. Examples of these standards are the International Organization for Standardization (ISO), and International Electro-technical Commission (IEC) (ISO/IEC 27001); and

The associate editor coordinating the review of this manuscript and approving it for publication was Sathish Kumar.

Control Objectives for Information and Related Technologies (COBIT). These guidelines and standards provide best practices for IS security [12]. Therefore, to help individuals to improve their security activities, organizations should integrate these regulations into a document called Information Security Policy (ISP); this policy assists to shape their employees' behavior towards IS security [3]. ISP is defined as ''a set of formalized procedures, guidelines, roles and responsibilities to which employees are required to adhere to safeguard and use properly the information and technology resources of their organizations'' [13]. Furthermore, ISP is described as a document that states the employee's roles and duties to function in a manner that safeguards their organizations' information and technology assets [14]. Enforcing ISP increases the high level of security within the organization [15].

However, developing an ISP is not sufficient to ensure the security of the organization's assets; the employees must comply with their organization's ISP. Studies indicate that employees are not always complying with ISP, and this non-compliance is considered one of the most significant factors affecting security breaches [16], [17]. Non-compliance with ISP leads to an interruption of the organization's operations [18]. Information security policy compliance (ISPC) is the degree to which employees safeguard their organization's information and technology assets against security threats by following ISP. Yazdanmehr and Wang [19] argues that the effectiveness of ISP depends on compliance with this policy, and a comprehensive policy will be insufficient as a countermeasure to security threats without compliance and observance thereof. ISPC is considered an issue of human behavior. Improving compliance behavior among employees will reduce security threats for the organizations and their employees [8].

Several studies have focused on ISPC and exploring the psychological and organizational theories that explain compliance behavior [3], [20]–[23]. Numerous articles examine several internal and external factors and theoretical constructs that motivate human behavior toward ISP [17], [24], [25]. While there are extensive studies on ISPC, it was noted that none of the reviewing studies classify the positive and negative (direct or indirect) influence of the human and organizational theories and their influencing factors toward ISPC behavior. This study investigates this issue as a research gap in the literature. We bridge this gap by exploring the literature published from 2012 - 2020 to shed light on the need for synthesizing the psychological theories, organizational theories, and other factors on ISPC researches. In addition, this paper examines the positive and negative (direct or indirect) impact of the human and organizational theories and their influencing factors toward ISPC behavior. This paper provides an investigation into relation between these theories and ISPC. This paper engages in a systemic review of current studies that address the theories and factors that contribute significantly to ISPC for practice and research as described in section VIII.

The remainder of the paper is organized as follows: a presentation of the related research and motivations for the current study (section II) followed by the research methodology (section III), results and discussion of the study (section IV). Next, the moderation and mediation analyses are presented in (section VI). The paper concludes with the identified gaps (section VII), implications (section VIII), and conclusion (section VX).

II. MOTIVATIONS FOR THE CURRENT STUDY

The systematic literature review (SLR) is based on the information security policy compliance reviewing studies. The available studies focus on determining the behavioral and organizational theories that are used (i.e. theory of planned behavior, deterrence theory, etc.) [3], [8]. Moreover, several studies were conducted to discover the influencing factors that affect information security policy compliance behavior (i.e. information security awareness, rewards, etc) [22], [25].

One of the earliest studies performed by Sommestad [26] covered 16 articles related to the theory of planned behavior.

In a later study, Sommestad *et al.* [27] analyze more than 60 factors from 29 articles that significantly contribute to the information security policy compliance behavior. Similarly, Cram *et al.* [28] classify the influence factors into 17 categories by conducting a meta-analysis covering 25 quantitative studies. Furthermore, SLR based on 51 articles was performed by Hina and Dominic [29] to explain the information security culture, awareness, and management issues within ISPC. A meta-analysis of 35 articles was conducted by Trang and Brendel [30] to explain the effect of deterrence theory towards ISPC. Angraini *et al.* [31] conducted a study covering 59 articles to evaluate the existing theories in ISPC research. Kuppusamy *et al.* [32] also identified several theories using 29 relevant articles. Recently, an SLR study based on 80 articles was performed by Ali *et al.* [33] to identify the behavioral transformation process from ISP noncompliance to compliance. The results and limitations obtained from the previous studies of ISPC researches are shown in Table 1.

In examining the literature, it was noted that none of the reviewing studies classify the positive and negative (direct or indirect) influence of the human and organizational theories and their influencing factors toward ISPC behavior. Considering the studies mentioned above, a systematic literature review was conducted to analyze the human behavior and organizational theories used in the ISPC researches. This study explores the factors that are related to these theories and their relation to ISPC behavior. Furthermore, the factors that are used in ISPC researches are reviewed. The study contributes to the research stream and will provide insight for other researchers to further investigate ISCP behavior.

III. RESEARCH METHODOLOGY

Based on the Okoli *et al.* [34] method, a systematic literature review was performed to cover the research topic. The process

TABLE 1. The existing reviewing studies in the ISPC context.

Study	Sample Size	Results	Limitations
[29]	51 articles	- An association between information security awareness, culture, and management with information security policy compliance behavior was found.	- Performed in the education field only. - Three concepts were studied.
[28]	25 articles	- Personal attitudes, norms, and beliefs have an important impact on ISPC, meanwhile, rewards and punishment have a weak effect.	- Variables based analysis. - Small dataset
[31]	59 Articles	- Multiple human and organizational theories were identified. - general deterrence theory, theory of planned behavior and protection - motivation theory was widely used in the literature.	- The study only mentions the number of theories, and most common, without more details.
[27]	29 Articles	- No clear result for the affective factors towards the compliance and misuse of ISP.	- Variable based analysis. - Small dataset
[30]	35 Articles	- There is an influence of deterrence theory on ISP compliance. - Deterrence has different effects on diverse cultures.	- The study only targets the deterrence theory and its influencing factors.
[32]	29 Articles	- Several behavioral theories have been identified, and their applied domain. - Three classifications for these theories according to their frequent usage.	- The study is limited to human behavior theories. - The study doesn't discuss the influencing factors related to the theories. - Small dataset.
[26]	16 Articles	- Theory of planned behavior can explain the ISPC behavior as other behaviors.	- The study only targets the theory of planned behavior and its influencing factors.
[33]	80 Articles	- Value conflicts, security-related stress, and neutralization significantly influence ISP noncompliance. - Internal/external and protection motivations positively affect the ISPC. - The transformation process from noncompliance into compliance is may controlled by deterrence techniques, management behaviors, culture, and information security awareness.	- The classification of compliance and noncompliance factors were ambiguous.

includes four phases; planning, selection, extraction, and execution. The planning phase includes identifying the research purpose and questions, in addition to the protocol that will be used in the literature. The purpose of the systematic literature review is to identify and classify the current body of research literature, that either quantitatively or qualitatively used theories in the information security policy compliance context in a given organizational setting. The following questions were formulated to expand the investigation.

RQ1- What are the theories used in the information security policies compliance context?

RQ2- What is the kind of relation of influencing factors and information security policies compliance behavior?

RQ3- What are the factors concluded in studies that influence information security policy compliance?

This process was performed using multiple keywords applied to the online database. The online databases of AIS library, Emerald insight, IEEE Xplore, Google Scholar, ProQuest, and ScienceDirect were used to identify the current researches of information security policy compliance. The search strategy was based on the following strings and combination of keywords: Information security policy/policies, compliance, comply, non-compliance, adherence, and compliance behavior. These keywords were combined in multiple ways, by using ''and'' and ''or'' operators and both, these strings were applied to the titles of the publications.

TABLE 2. Inclusion and exclusion criteria.

Inclusion criteria	-Written in English -Publication from 2012 to 2020 -Studies that explore the field using theoretical or empirical data. -Studies that examine employees' compliance behavior towards information security policy in the organizations. -Studies distributed in Journal, Conference Proceedings, Book\Book section.
Exclusion criteria	-Studies from organization reports, guidelines, technical opinion reports. -Studies that explain non-compliance behavior. -Studies that explain the organizational security culture, compliance and security behavior.

The selection phase includes specifying the inclusion and exclusion criteria for the eligibility of the retrieved researches which is shown in Table 2.

Kitchenham and Charters [35] claim that quality assessment of the selected review paper determines the significance of the individual publication when the results are

being synthesized. Quality assessment was applied to assure the reliability of the selected publications [36]. Several guidelines and metrics were suggested in multiple studies to make such assessments effective [37]. Therefore, in addition to the inclusion and exclusion criteria determined previously, this study applied the assessment of individual publications quality through other criteria. Articles from indexed impact factor journals were included. For conference papers, three quality assessments criteria were assessed. First, papers published in high reputable IS and Computer Science conference proceedings that are indexed in google scholar metrics, by ''h-index'' in the latest five-year window [37]. Second, conference papers that are cited in articles published in leading journals [38]. Third, papers published in conferences that have high-rank Scopus's CiteScore. Scopus's CiteScore calculates the citation impact of conferences, journals, book series, and trade journals included in the Scopus database [39].

In the extraction phase, the researches that met one of the exclusion criteria were eliminated, and classified by the eliminating reasons. The result of the search strategy produced 127 studies from different databases, in addition to 24 studies through forward and backward searches, two studies were excluded for non-English language. After records screening, nine studies were duplicated, and thus eliminated from the process. Also, five studies additional studies were excluded for the following reasons; one study cannot be accessed, and four studies were guideline reports. Afterward, a title and abstract screening were performed, and an additional 25 studies did not

meet the criteria. Then, a full-text screening for the remaining studies was conducted, and 23 studies were out of the research scope, that is the employees' compliance behavior towards information security policy in the organizations. Finally, a total of 87 published studies were included for detailed analysis. The result of the literature search strategy and evaluation for inclusion is shown in Fig 1. Finally, the execution phase includes analyzing the findings, which are discussed in further detail in section IV and V.

IV. RESULTS AND DISCUSSION RELATED TO THE MAJOR CLASSIFICATION

In this section, the finding and state of art analysis of the systematic literature review were reported based on the process that described above. The search strategy produced a total of 87 studies used for detailed analysis, which are shown in Appendix Table 1. The research was analyzed based on patterns in the nature of the research, empirical methods used, the classification of the applied theories, and research target sectors, in relation to the information security policy compliance context.

Fig 2 highlights the rapid growth of information security policy context researches and the increasing academic interest in this field. The number of papers has increased over the last three years, peaking 2018- 2019, and decreasing in 2020. The 2020 decrease is due to the suspension of research in the

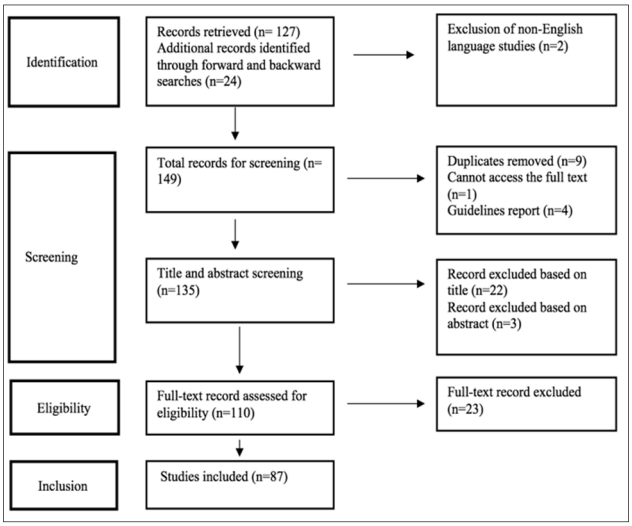

FIGURE 1. Flowchart of research strategy.

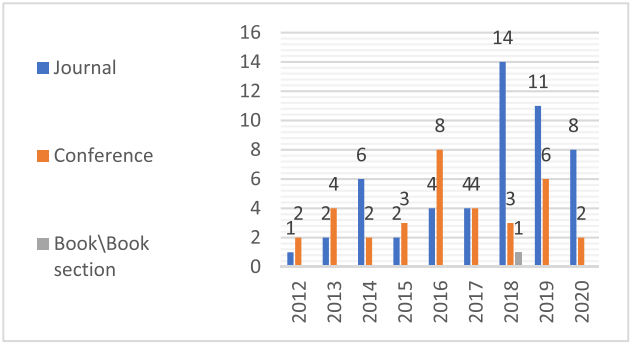

FIGURE 2. Year-wise analysis of the selected studies per type of publication.

middle of the year possibly due to the global epidemic situation. Fig 2 illustrates the year-wise analysis of the selected studies per type of publication.

A. THE NATURE OF RESEARCH

To determine the research nature, Kothari [40] classification was used for the selected studies. The categorizing is based on whether the study is conceptual or empirical research. Conceptual research relates to an abstract idea or theory, and is also used to develop new concepts or reinterpret present concepts. Empirical research depends on experience or observation, and is based on primary or secondary data. The empirical research concludes with results that can be proved by observation or experiments. In our study, the literature review paper that concluded with a new result was classified as empirical research, while that study with unclear results was categorized as conceptual research. Empirical research was used in most of the publications, 73 studies (84%), as shown in Fig. 3. More than half of the empirical publications were quantitative, 67 studies (77%), and the rest were qualitative (7%). Only 14 studies (16%) were classified as conceptual research.

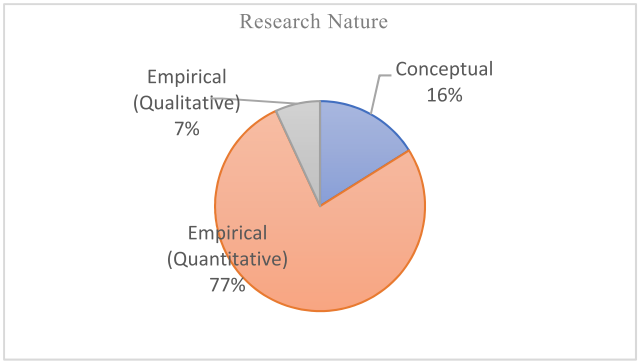

FIGURE 3. Classification of the research nature.

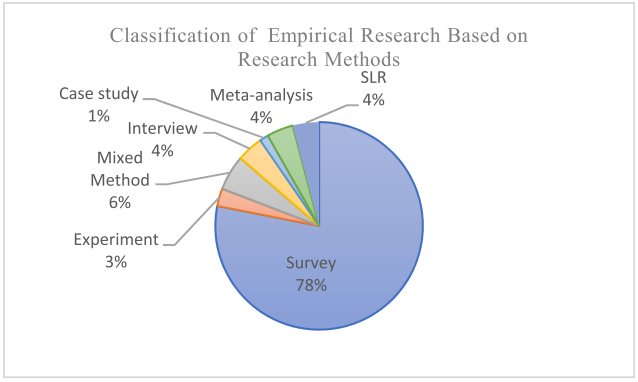

FIGURE 4. Classification of empirical research based on research methods.

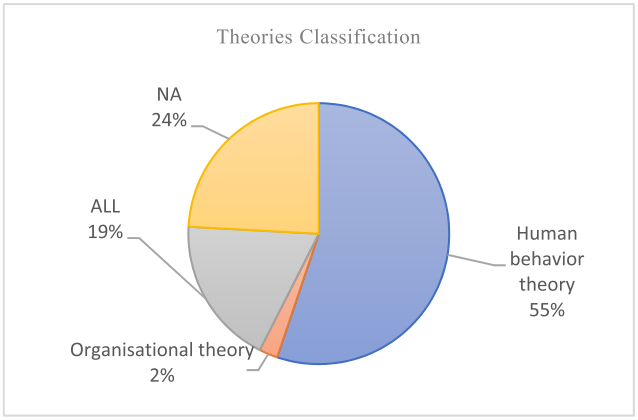

FIGURE 5. The classification of the used theories.

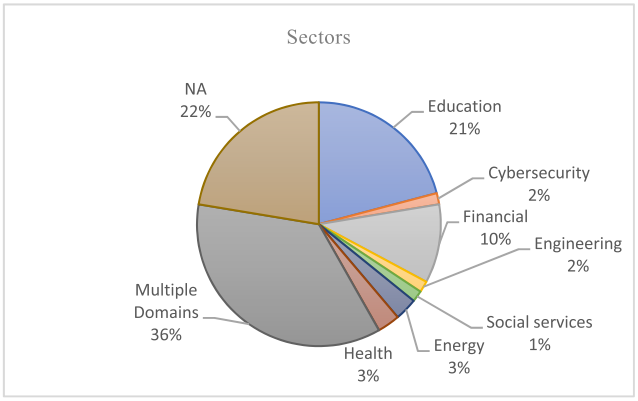

FIGURE 6. The classification of the target sectors.

As earlier noted, 84% of studies were empirical research. Most (78%) of the studies used a survey method [17], [41], [42], and (6%) used a mixed method approach [8], [20], [23]. In addition, 9 studies (12%) used interviews, meta-analysis, and systematic literature review [43]–[45]. While (3%) of studies applied experiments [46], [47], and one study (1%) used a case study method [48] as illustrated in Fig 4.

B. THEORIES CLASSIFICATION

Among the 87 selected studies, 48 studies (55%) applied a human behavior theory [3], [49], [45]. Moreover, 16 studies (17%) used human behavior and organizational theories together [8], [21], and 2 studies utilized an organizational theory [1], while 21 studies (24%) were classified as 'not applicable' for not using any kind of theories as shown in Fig 5.

C. TARGET SECTORS

The sector specific distribution of the studies is shown in Fig 6. Eight sectors have been identified from the researches analysis. The highest percentage of the studies (35%) were applied to multiple domains ex banking, insurance, manufacturing, retail, and government organization, etc. [1], [21], followed by the education field with (21%) [25], [49]. The financial sector followed with (10%) of studies [43], [51]. While (6%) of the studies targeted the health and energy sectors [52], [53]. Cybersecurity, and engineering, as the target sectors, accounted for 4% in all studies [54]. Only (1%) of studies targeted the social services field [55]. However (22%) of studies do not identify the sectors related to the research [22], [42]. Notably, the reviewed studies were unbalanced in terms of target sectors.

V. RESULTS AND DISCUSSION RELATED TO THEORIES AND FACTORS

RQ1- What are the theories used in the information security policies compliance context?

RQ2- What is the kind of relation of influencing factors and information security policies compliance behavior?

This section outlines the theories and factors that are consistently used within the reviewed ISPC research. Across 85 publications, 35 human behavior and organizational theories were analyzed. Studies may have used constructs from theories or the whole theory to demonstrate as much result variance as possible. All the constructs studied the dependent variable (DVs), which are (intent to comply and actual compliance behavior). In this research, the relation to ISPC is classified as direct, indirect, partial, and no effect. The constructs that affect the DV directly. positively or negatively are classified as a direct effect (D+, D−). Indirect

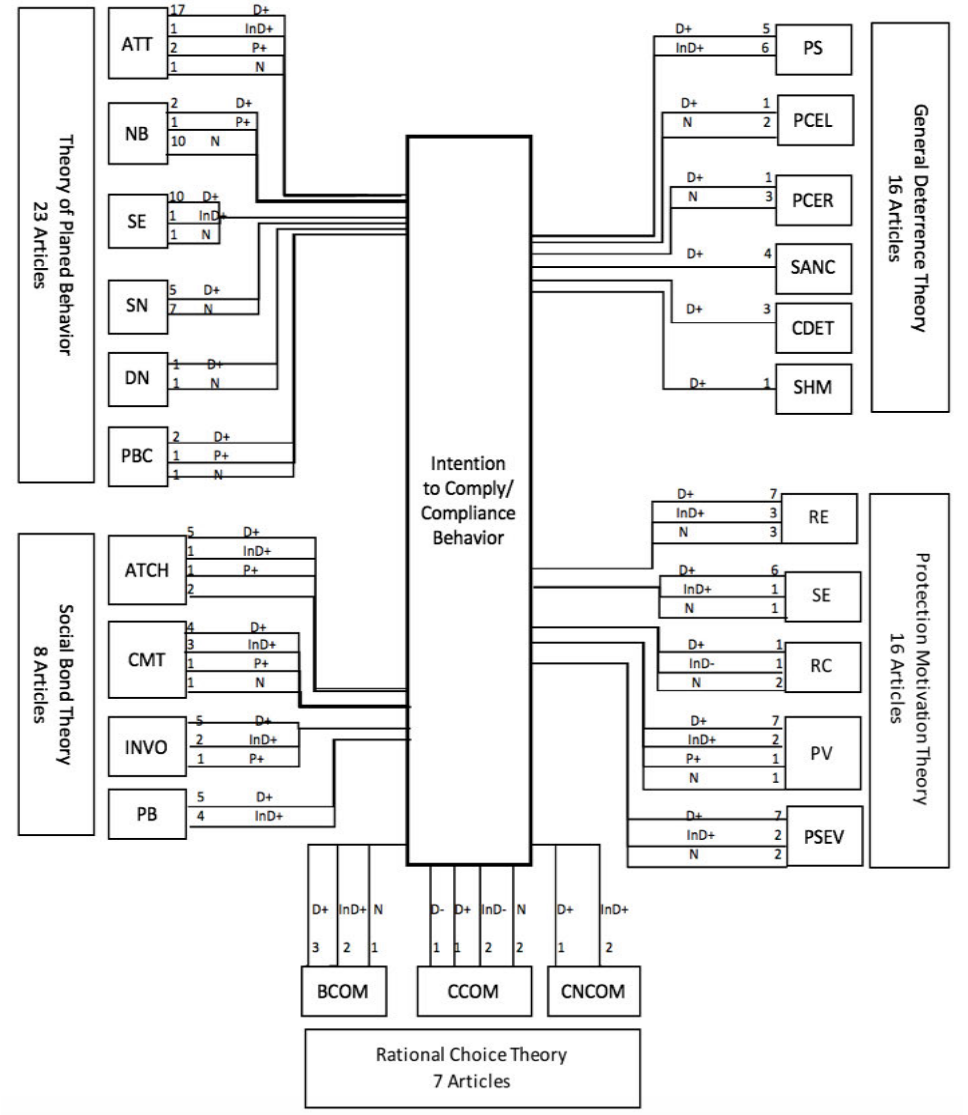

FIGURE 7. Map of theories and kind of relation toward ISPC.

effect is noted when there is a moderator or mediator to indicate the relation, or when the construct effect on a variable, in turn affects the DV (InD+, InD−). In the case of measuring multiple aspects of the construct, in which the result supports some of them, they classified as a partial effect (P+, P−). Finally, no or weak effect demonstrates the lack of effect for DV (N). Fig 7 and 8 show the most common theories and their influencing factors related to information security policy compliance, which are listed in Appendix Table 5 in detail. Less explored theories which used in one or two studies are listed in Appendix Table 6.

[Abbreviation for Fig 7 and 8. ATT: Attitude; NB: Normative Belief; SE: Self-Efficacy; DN: Descriptive Norms; SN: Subjective Norms; PBC: Perceived Behavioral Control; ATCH: Attachment; CMT: Commitment; INVO: Involvement; PB: Personal Belief; PS: Punishment Severity; PCEL: Punishment Celerity; PCER: Punishment Certainty; SANC: Sanctions; CDET: Certainty of Detection; SHM: Shame; RE: Response Efficacy; RC: Response Cost; PV: Perceived Vulnerability; PSEV: Perceived Severity; BCOM: Perceived Benefit of Compliance; CCOM: Perceived cost of compliance; CNCOM: Perceived Cost of non-Compliance; SSG: Supervisor-Subordinate Guanxi; OC: Organizational Commitment; DOA: Developmental-Oriented Appraisal; RWD: Reward; SS: Selective Staffing; TCD: Training for Career Development; RO: Role; HBT: Habit; TMS: Top Management Support; PP: Peer Pressure; ORC: Organizational Climate; SD: Self-Determination; CMP: Competence; ATN: Autonomy; RTD: Relatedness; LC: Locus of Control]

The studies are drawn from diverse theories including human behavior theories and organizational theories.

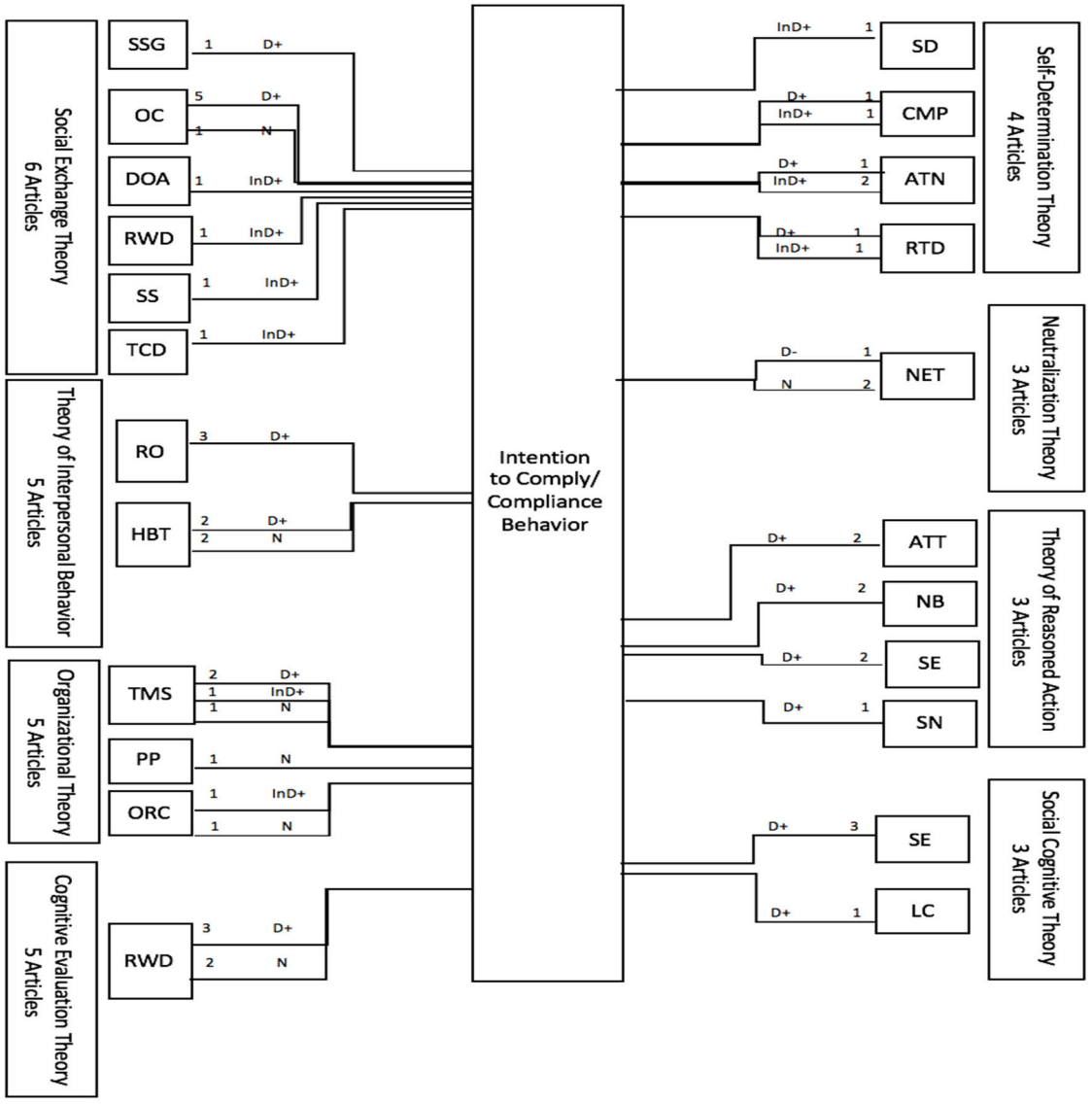

FIGURE 8. Map of theories and kind of relation toward ISPC cont.
Notes: The numbers listed in the figures indicate the number of studies that used the factors.
D+; positive direct effect, InD+; positive indirect effect; P+; positive partially effect; D-; negative direct effect, InD-; negative indirect effect; P-; negative partially effect; N; no or week effect.

Examples of these theories are the theory of planned behavior, the theory of protection motivation, general deterrence theory, social bond theory, neo-institutional theory, and organizational control theory, which include variables that impact ISP compliance. The results showed that the general deterrence theory, theory of planned behavior (TPB) and protection motivation theory are the most frequently used in the field which concurs with [31], [32]. The following paragraphs discuss the five most common theories in the studies; other theories are listed in Appendix Table 5 in detail.

As presented in Fig 7 and 8, drawing from the TBP, attitude, normative belief, self-efficacy, descriptive norms, subjective norms, perceived behavioral were examined in 23 articles to find out about employees' ISPC. While compliance is human behavior, the TPB was explored commonly. The studies were similar in results as shown in the figures. ATT and SE are positively significant to ISPC, while NB and SN have weak strength in predicting ISPC. However, DN and PBC have not been given extensive attention in the studies. The protection motivation theory constructs which are response efficacy, self-efficacy, response cost, perceived vulnerability, and perceived incision were analyzed through 16 articles. Most of the studies showed a positive effect on ISPC. RE, PV, and PSEV are considered strong positive predictors for ISPC. In addition, SE has a positive direct influence on ISPC. Ryutov *et al.* [56] proved a

negative indirect association between RC and ISPC, while Rajab *et al.* [57] found a positive relation. Ifinedo [4], Nasir *et al.* [58] also found that RC is not a significant predictor for ISPC. Furthermore, the general deterrence theory explained the punishment severity, punishment celerity, punishment certainty, sanctions, certainty of detection, and shame in 16 articles. Most of the results show positive influence on ISPC. PS was analyzed frequently in the studies, and the results support the positive direct and indirect impacts on ISPC. The studies show the weak strength of PCER in predicting ISPC. Other constructs received less attention in the context.

Drawing from the social bond theory, attachment, commitment, involvement, and personal belief were studied in 8 articles to examine employees' ISPC. The studies were similar in the results as shown in the Fig 7. All the constructs are either directly or indirectly positively significant to ISPC. Whilst Safa *et al.* [2], Choi *et al.* [59], Ifinedo, [60] found a weak impact of attachment and commitment to the employees' ISPC. Rational choice theory is based on the cost and benefit of a given action. Seven articles explained the benefit of compliance; cost of compliance and non-compliance. There was a variance in the results, where Han *et al.* [61], Kim *et al.* [62], Arage *et al.* [63], D'Arcy and Lowry [41], Kim *et al.* [7] found a positive direct and indirect influence of BCOM and CNCOM on ISPC. The exception was found in the studies of D'Arcy and Lowry [41], Kim *et al.* [7], Ifinedo [64], they found a negative relation between CCOM and ISPC behavior.

RQ3- What are the factors concluded in studies that influence information security policy compliance?

Among 85 studies, 38 factors from different concepts were analyzed. All the factors studied toward the dependent variable that was used in the studies, which are (intention to comply and actual compliance behavior). These factors can be categorized as both internal and external to the individuals. Examples of internal factors are trust, information security awareness, organizational citizenship behaviors, and demographics. Moreover, the external factors could be a SETA program, corporate social responsibility, supportive organizational culture, and compliance audit. The results indicate that internal factors play more of a role in motivating the ISPC behavior than external factors. The most commonly noted factors, discussed in the next sections, are information security education, training and awareness, trust, and leadership. Table 3 lists the factors that influence ISPC.

A. INFORMATION SECURITY EDUCATION, TRAINING, AWARENESS

Studies confirm that information security awareness education and training is a powerful predictor of ISP compliance. Researchers argue that ISP awareness is associated with positive attitudes among organizations' employees [18], [25]. Hina *et al.* [65] argue that security education, training, and awareness (SETA) programs improve the information security culture in organizations. Similarly, the information security education, training, and awareness factor was commonly analyzed in current researches. Koohang *et al.* [25] analyzed four predictors for ISPC within 237 university employees; their results confirmed that information security awareness is essential for ISPC. Abed *et al.* [66] proposed an ISP continuous model, and found security awareness directly influences continuous ISPC behavior among 270 banking employees. Chongrui *et al.* [67] examined the role of security climate and training on employee's ISPC. Their study was conducted on 525 civil servants in China and results show a significant direct effect of security training on ISPC. Dhillon *et al.* [17] study the mediation role of psychological empowerment in ISPC intention. They found that SETA, participation in information security decision-making, and access to ISP influence the ISPC intention.

The above mentioned studies explain the direct effect of SETA on ISPC behavior. However, Koohang et al [18] build an awareness-centered ISPC model; their study was applied among 285 non-management employees, and results show the indirect impact of ISP awareness through the understanding of resource vulnerability and self-efficacy which lead employees to comply with ISP requirements. Alomari *et al.* [68] proved that information security and technologies awareness shape employees' attitude toward the ISPC among 878 financial organization employees. Arage *et al.* [63] explored the role of norms in compliance toward ISP within 201 employees from different organizations. Their findings show that ISP-related awareness of consequences shapes the personal norms, which in turn guide ISPC behavior. Furthermore, Stafford *et al.* [46] confirmed that an effective training program for users is more crucial than other prevention protocols in ISPC behavior. Among 301 employees working in higher education institutions in Malaysia, Hina *et al.* [65] considered the SETA program to play a vital role in motivating employees to embrace protective behavior for compliance with ISP. The study of Burns *et al.* [69] explores the role of employee awareness of the SETA program toward two different intentions among 411 participants. The result shows that the SETA program indirectly affects ISPC intention and protection of organization information assets. Likewise, Ali *et al.* [23] study three organizational factors to explore the social bound theory constructs with a survey of 254 managers in oil and gas organizations. They found that a SETA program was one of the factors which play an essential role in developing ISPC behavior among the employees. However, the studies of Kretzer *et al.* [70], Abdul Kadir *et al.* [54] concluded that information security training has a weak positive association with ISP compliance behavior.

B. TRUST

Studies realized that users' perception of the security characteristics for their information systems leads to trust in the system. The high level of IS trust leads to improve the security decisions that performed by employees [25]. This is also supported by Bahtiyar *et al.* [71] who confirm that individuals' high trust level in the security system guides to using

TABLE 3. Factors influencing ISPC.

Influencing Factors	Description	Relation to ISPC			
		Direct effect	Indirect effect	Partially effect	No/weak effect
Leadership	The roles of the leaders in protecting the organization's information assets, through formulating well-established security strategies and objectives to ensure the effectiveness of ISP.	[25,73]	[18,73]		[21]
Trust	The employees' expectations or beliefs like (competence, benevolence, and integrity) that explain the trustworthiness regarding all the ISP requirements.	[25,52, 72]	[18,42]		
Information Security Awareness	The employee's knowledge and understanding of the rules and responsibilities related to information security and its requirements.	[25,66, 74]	[18,63,68, 75]		
Security-Related Stress	A stress resulted from the internal and external security requirements, which are beyond the employee's energy and capabilities.		[22]		
Understanding Resource Vulnerability	Understanding the weakness in the organization's resources and assets, which may utilize through a threat source.	[18]			
Information Security Training	The organization programs to communicate with their employees about the organization's information security issues.	[67,74]	[46]		[54,70]
Moral Beliefs	The level where the employee considers the violation as unacceptable behavior.	[41,63, 76]			
Organizational Citizenship Behaviors	Discretional actions that can develop the organization's effective performance like engaging in extra-role behaviors, that are not required by the organization.				[41]
Organizational Deviance	A behavior breach of the essential organization rules, which can influence the organization's reputation and well-being.	[41]			
Perceived Organizational Formalization	Formalize the organization's rules, instructions, and communications to manage the employees' behaviors.			[8]	
Work-Related Groups	The individuals associated with others under the same circumstances.				[77]
Ethical Climate	Describing the moral atmosphere of the organization and its members.		[19]		
Organization's Information Security Strategy Access	Employee opportunities given by the management, to reach and understand their organization's information security strategic objectives.	[17]			
Position Level	An employee position within the organization, that addresses the individual's required liabilities and job expectations.	[78]			
Information Security Climate	The policies, practices, and procedures that enhance the employees' perception about the information security value in their organizations.	[67,79]			
Satisfaction	The positive feeling about the information security policy that motivates compliance.	[66]			
Confirmation	An individual's confirmation of expectations about the ISPC.		[66]		
Security Avoidance	Deliberately avoiding the information security policy, despite employee knowledge of its need and importance.	[79]			
Participation in Decision-Making	Grant the employee the right to participate in their organization's information security goals, by requesting input.	[17]			

TABLE 3. *(Continued.)* **Factors influencing ISPC.**

Demographic	A population statistical study, which can include multiple criteria like age, ethnicity, education level, and work experience.			[24]	
Corporate Social Responsibility	Engaging in social goals and practices to provide a high financial return to shareholders.		[62]		
SETA programs	Sharing knowledge about information security issues with the employees, in addition to the required security practices to do their job.	[17]	[23,53,65, 69,75]		
Psychological Empowerment	Intrinsic motivation factors which derive from the task, that reflect on the individual's work and involvement	[78]	[17]		
Religiosity	Religiosity level in a social context impact the compliance and deviance behavior.	[80]			
Supportive Organizational Culture	A set of common suppositions and conceptions relating to the organization's work environment.	[76]	[21]		
Internal Audit	Examining the preventive system quality, and figuring the vulnerabilities of security solutions against security policy violations.		[46]		
Behavioral Monitoring	The employees' behavior observation at work to identify how they deal with technologies, systems, and assets.				[45]
Provision of Policy	The existence of ISP and its role in improving the security behavior within the organization employees		[65]		
Negative Experience	The negative incident related to information system security that remains in the employee experience when dealing with future issues.			[65]	
Security Agents	The consultant and trainer responsible to perform security-related tasks whether a full or part time security agent.			[70]	
Informational Materials	Tangible and non-tangible resources that explain the employees' compliance behavior, and common mistakes within the organization.			[70]	
Compliance Audit	Checking the information security policy compliance through an internal and external auditor.		[70]		
National Culture	The impact of the society's culture on the individual's values, and the relationship between these values and their behavior.	[63]			
Worries about Cybercrime	The fear that may have functional and dysfunctional effects, and the individuals are different in nature; so, their level of worry varies.	[81]			
Working Experience	Abilities, knowledge, and skills can be gained through education or participation in specific events.				[72]
Self-Regulatory Approach	The approach that considers the major drivers of behavior are intrinsic desires.	[82]			
Psychological Ownership	The sense of possession of the information related to their work.				[83]
Organizational Injustice	The organization's actions that impact the employee conception of justice and injustice, which are divided into distributive, procedural and interactional justice.			[47]	

this system consistently, which might decrease the security threat in the organization. Therefore, the organization should build trust in their security systems, and that trust-based information security has a positive effect in safeguard the organizations from security incidents [25].

Several empirical studies confirmed that trust is a powerful predictor of an employee's intention to comply with the ISP requirements. Koohang *et al.* [25] study the trust beliefs impact among 237 university employees, they found a prediction association for trust toward employees' ISP compliance. Humaidi *et al.* [72] implement multidisciplinary theories to evaluate the correlation between the and compliance behavior and integrated social-technical values towards ISP among 454 health professionals. Their study was performed on two sub-group which are a high and low experience groups. They revealed that perceived trust is the most

important predictor of ISPC in both sub-groups. The study of Humaidi *et al.* [52] explored the Indirect effect of management support on users' ISPC within 454 healthcare professionals. Their finding supports the effect of management support through both self-efficacy and the trust factor. In addition, a direct influence was found between trust and ISPC behavior. While Paliszkiewicz, [42], Koohang *et al.* [18] confirmed the indirect impact of trust toward the organization's ISP compliance through the leadership factor.

C. LEADERSHIP

Studies argue that information security should be considered a top management priority and that effective leadership from top management encourages ISP enforcement [18]. Leaders should develop a strong information security culture to enhance compliance with ISP requirements in the organizations, and preserve the organization's assets from security incidents. Leaders should motivate their employees to follow the ISP procedures [25]. Researchers propose that employees might comply with ISP because of reliance on their leader, or in regard to their leader's morals. Employees' beliefs, attitudes, and intention to ISP compliance can heavily depend on their leader's opinions [21], [73].

Koohang *et al.* [25] study the leadership influence among 237 university employees, and they found a direct positive association for leadership toward employees' ISP compliance. Feng *et al.* [73] examined the relationship between paternalistic leadership and employees' ISPC. Their study was conducted among 314 employees and their supervisors in organizations. The findings supported that all three dimensions of paternalistic leadership which are benevolence, morality, and authoritarianism directly affect employees' ISPC. Koohang *et al.* [18] found an indirect positive impact of effective leadership which guides employees to comply with ISP requirements among 285 non-management staff. However, the study of Amankwa *et al.* [21] which was performed on 424 employees in different organization, argues that leaders have a weak impact on employees' compliance toward ISP.

VI. MODERATION AND MEDIATION ANALYSIS

Among existing studies, ten articles used moderation and mediation analysis to enhance the result. Humaidi *et al.* [72] study the employees' work experience as moderator for the relationship between (management support, information security awareness, perceived barrier, self-efficacy, perceived trust) and ISPC behavior. Their results confirmed the effect of work experience on management support and information security awareness, while they did not support the other constructs. Yazdanmehr *et al.* [82] argue that the rule-oriented ethical climate and susceptibility to interpersonal influence negatively moderated both the effect of the command-and-control approach and the effect of the self-regulatory approach on ISPC. Liu *et al.* [84] suggest that organizational commitment could be a significant moderator in threat avoidance behavior. They proved that organizational commitment weakens the negative effect of perceived costs and the positive effect of self-efficacy on ISPC behavior. They also found a weak effect of organizational commitment on the perceived threat, perceived effectiveness and ISPC behavior. Yazdanmehr and Wang [19] propose that the ISP awareness of consequence and ISP ascription of personal responsibility positively moderates the impact of ISP-related personal norms on ISPC. Their results confirmed the effect of ISP ascription of personal responsibility, while they did not confirm the ISP awareness of consequence.

For the mediation analysis, Feng *et al.* [73] proved that the social bond mediates the effect of moral leadership and benevolent leadership on ISPC intentions; however, social bond did not mediate the effect the authoritarian leadership on ISPC. Moreover, Dhillon *et al.* [17] confirm the argument that psychological empowerment mediates the association between (SETA, access to information, participation in decision- making) and ISPC intention. Kim [85] found that compliance knowledge mediates the correlations between (social pressure,and compliance behavioral belief) and compliance intention. Overall, this kind of analysis is helpful because it explains the relationships and the variables' impact on these relationships. There was variety in the moderators and mediators, individuals' factors (such as psychological empowerment, and employees experience), and environmental factors (such as ethical climate). Also, several factors were studied frequently (such as leadership, rewards, SETA, response cost), which may produce a valuable result when they are utilized as moderators and mediators.

VII. IDENTIFIED GAPS

The analysis of the current studies provides some of research gaps that could be investigated. First, the role of organizational theories needs further deep investigation. Second, there is a noted paucity in studies implementing technology-related behavior theories, such as the technology acceptance model, technology threat avoidance theory, and task technology fit model. The technology-related behavior theories should be a priority in future ISPC research because the understanding of these theories will reflect on the security countermeasures that are used in organizations [86]. Third, the moderation and mediation analysis have received less attention within the current studies. The potential mediation and moderation effect could help gain better understanding of the underlying factors and theories. Future research could be carried out on empirical work and a meta-analysis considering the effect of mediator and moderator variables. Fourth, the studies were unbalanced in related to the target sectors. For example, there is a general lack of research targeting the health sector, where, according to a report by Bitglass [87], the average cost of security breaches is still higher than that of every other industry in 2020. There were approximately 600 healthcare data breaches in 2020, increasing 55% from 2019. Therefore, more attention should be paid to the health sector. Fifth, very few studies have applied diverse research methods such as lab experiments and interviews, and using such

TABLE 4. A description of the studies identified in the selection phase of ISPC literature review.

Study	Year	Publication Type	Nature of Study	Method	Data Analysis Technique	Sector	Used Theories
[68]	2012	Conference	Empirical- QNT	Survey	PLS-SEM	Financial	Human Behavior
[4]	2012	Journal	Empirical- QNT	Survey	PLS	Multiple domains	Human Behavior
[75]	2012	Conference	Empirical- QNT	Survey	PLS	Financial	Human Behavior
[91]	2013	Journal	Empirical- QNT	Experiment	EFA	Financial	Human Behavior
[55]	2013	Journal	Empirical- QUAL	Interviews	-	Social Services	NA
[80]	2013	Conference	Empirical- QNT	Survey	PLS-SEM	Education	Human Behavior
[92]	2013	Conference	Empirical- QNT	Survey	PLS	Financial	Human Behavior
[93]	2013	Conference	Empirical- QNT	Survey	PLS	Education	Organizational
[94]	2013	Conference	Empirical- QNT	Survey	PLS-SEM	Multiple domains	Human Behavior
[95]	2014	Conference	Conceptual	-	-	-	Human Behavior
[5]	2014	Journal	Empirical- QNT	Survey	PLS-SEM	Multiple domains	Human Behavior
[7]	2014	Journal	Empirical- QNT	Survey	PLS-SEM	Multiple domains	Human Behavior
[90]	2014	Journal	Empirical- QNT	Survey	SEM	Multiple domains	Human Behavior
[96]	2014	Journal	Empirical- QNT	Survey	PLS	NA	Human Behavior
[74]	2014	Conference	Conceptual	-	-	-	Human Behavior
[79]	2014	Journal	Empirical- QNT	Survey	PLS	Multiple domains	ALL
[27]	2014	Journal	Empirical- QNT	SLR	-	-	NA
[13]	2015	Journal	Empirical- QNT	Mixed Method	PLS regression analysis	Multiple domains	ALL
[86]	2015	Conference	Conceptual	-	-	-	NA
[70]	2015	Conference	Empirical- QNT	Survey	NA	Engineering	Human Behavior
[63]	2015	Conference	Conceptual	-	-	-	Human Behavior
[72]	2015	Journal	Empirical- QNT	Survey	PLS-SEM	Health	ALL
[2]	2016	Journal	Empirical- QNT	Survey	SEM	Multiple domains	Human Behavior
[54]	2016	Conference	Empirical- QNT	Survey	NA	Cybersecurity	Human Behavior
[19]	2016	Journal	Empirical- QNT	Survey	PLS	NA	Human Behavior
[50]	2016	Journal	Empirical- QNT	Survey	PLS	Education	Human Behavior
[97]	2016	Conference	Empirical- QNT	Survey	NA	Education	Human Behavior
[66]	2016	Conference	Empirical- QNT	Survey	SEM	Financial	Human Behavior
[64]	2016	Journal	Empirical- QNT	Survey	PLS-SEM	Multiple domains	ALL
[48]	2016	Conference	Empirical- QUAL	Case study	NA	Education	NA
[78]	2016	Conference	Empirical- QNT	Survey	PLS-SEM	NA	NA
[15]	2016	Conference	Conceptual	-	-	-	NA
[98]	2016	Conference	Empirical- QNT	Survey	SEM	Education	Human Behavior
[83]	2016	Conference	Empirical- QNT	Survey	PLS	Multiple domains	Human Behavior
[99]	2017	Journal	Empirical- QNT	Survey	NA	Multiple domains	Human Behavior
[61]	2017	Journal	Empirical- QNT	Survey	PLS	Multiple domains	ALL
[100]	2017	Conference	Empirical- QNT	Survey	NA	Education	Human Behavior
[51]	2017	Journal	Empirical- QNT	Survey	CB-SEM	Financial	ALL
[101]	2017	Conference	Empirical- QNT	Meta-analysis	NA	-	NA

TABLE 4. *(Continued.)* **A description of the studies identified in the selection phase of ISPC literature review.**

[28]	2017	Conference	Empirical- QNT	Meta-analysis	NA	-	NA
[43]	2017	Journal	Empirical- QUAL	Interviews	-	Financial	NA
[102]	2017	Conference	Conceptual	-	-	-	NA
[21]	2018	Journal	Empirical- QNT	Survey	PLS-SEM	Multiple domains	ALL
[103]	2018	Conference	Empirical- QNT	Survey	PLS-SEM	NA	Human Behavior
[20]	2018	Journal	Empirical- QNT	Mixed method	CFA	Multiple domains	Human Behavior
[24]	2018	Journal	Empirical- QNT	Survey	ALM	Multiple domains	NA
[62]	2018	Journal	Empirical- QNT	Survey	PLS	Multiple domains	ALL
[49]	2018	Journal	Empirical- QNT	Survey	PLS	Education	Human Behavior
[56]	2018	Journal	Empirical- QNT	Survey	PLS	NA	ALL
[58]	2018	Journal	Conceptual	-	-	-	Human Behavior
[104]	2018	Book	Conceptual	-	-	-	NA
[77]	2018	Journal	Empirical- QNT	Survey	OLS	Multiple domains	Human Behavior
[46]	2018	Journal	Empirical- QUAL	Interviews	-	NA	NA
[44]	2018	Journal	Empirical- QUAL	SLR	-	-	NA
[59]	2018	Journal	Empirical- QNT	Survey	PLS-SEM	NA	Human Behavior
[60]	2018	Journal	Empirical- QNT	Survey	PLS-SEM	Multiple domains	ALL
[81]	2018	Conference	Conceptual	-	-	-	NA
[105]	2018	Conference	Empirical- QNT	Survey	EFA	Multiple domains	Human Behavior
[52]	2018	Journal	Empirical- QNT	Survey	PLS-SEM	Health	Human Behavior
[69]	2018	Journal	Empirical- QNT	Survey	CB-SEM	Multiple domains	Human Behavior
[42]	2019	Journal	Empirical- QNT	Survey	MRA	NA	NA
[73]	2019	Journal	Empirical- QNT	Survey	CB-SEM	Multiple domains	Human Behavior
[22]	2019	Journal	Empirical- QNT	Survey	HLM	NA	Human Behavior
[18]	2019	Journal	Empirical- QNT	Survey	PLS-SEM	NA	Human Behavior
[1]	2019	Journal	Empirical- QNT	Survey	PLS	Multiple domains	Organizational
[41]	2019	Journal	Empirical- QNT	Survey	HLM	NA	Human Behavior
[8]	2019	Journal	Empirical- QNT	Mixed Method	SEM	Multiple domains	ALL
[57]	2019	Journal	Empirical- QNT	Survey	PLS-SEM	Education	ALL
[47]	2019	Journal	Empirical- QNT	Experiment	SEM	Education	ALL
[106]	2019	Conference	Empirical- QNT	Survey	PLS-SEM	NA	Human Behavior
[107]	2019	Conference	Conceptual	-	-	-	Human Behavior
[108]	2019	Journal	Conceptual	-	-	-	NA
[31]	2019	Conference	Empirical- QUAL	SLR	-	-	N
[109]	2019	Conference	Conceptual	-	-	-	NA
[110]	2019	Conference	Conceptual	-	-	-	Human Behavior
[45]	2019	Conference	Empirical- QNT	Meta-analysis	NA	-	Human Behavior
[65]	2019	Journal	Empirical- QNT	Survey	SEM	Education	Human Behavior
[25]	2020	Journal	Empirical- QNT	Survey	MRA	Education	NA
[111]	2020	Journal	Empirical- QNT	Survey	PLS-SEM	Education	Human Behavior

TABLE 4. *(Continued.)* **A description of the studies identified in the selection phase of ISPC literature review.**

[76]	2020	Conference	Conceptual	-	-	-	ALL
[17]	2020	Journal	Empirical- QNT	Survey	SEM	NA	NA
[3]	2020	Journal	Empirical- QNT	Survey	PLS-SEM	Education	Human Behavior
[84]	2020	Journal	Empirical- QNT	Survey	PLS	NA	ALL
[82]	2020	Journal	Empirical- QNT	Survey	SEM	Multiple domains	Human Behavior
[53]	2020	Journal	Empirical- QNT	Survey	EFA	Energy	Human Behavior
[67]	2020	Conference	Empirical- QNT	Survey	PLS	NA	Human Behavior
[23]	2020	Journal	Empirical- QNT	Mixed Method	PLS	Energy	ALL

Notes: NA, Not Available; QUAL, Qualitative; QNT, Quantitative; SLR, Systematic Literature Review; ALL, Human and organizational theories ;PLS-SEM, Partial Least Squares Structural Equation Modeling; PLS, Partial Least Squares Technique; SEM, Structural Equation Modeling; CB-SEM, Covariance-Based Structural Equation Modeling; CFA, Confirmatory Factor Analysis; ALM, Automatic Linear Modelling; OLS, Ordinary Least Squares; MRA, Multiple Regression Analysis; HLM, Hierarchical Linear Modeling; EFA, Exploratory Factor Analyses.

methods may obtain new results in the field. Finally, the data analysis techniques were mostly similar using the structural equation modeling (see Appendix Table 4); therefore, there was an absence of techniques such as artificial intelligence techniques. Liébana-Cabanillas *et al.* [88], Alwabel and Zeng [89] confirm that using artificial neural networks, which is an important artificial intelligence technique, can provide greater prediction accuracy than linear models, and it is better than the traditional statistical techniques in predicting technology adoption. Therefore, it would be interesting to focus more intensely on these gaps to investigate ISPC behavior.

VIII. IMPLICATIONS FOR PRACTICE AND RESEARCH

This paper has several contributions and implications for information security research. The paper seeks to offer an overview of information on security policy compliance current research. From the research perspective, one of the most important contributions is the synthesizing of the human behavior theories and organizational theories, and other factors that motivate the compliance behavior. Another significant contribution to the academic field is that it is one of the first researches to determine the relationship types among the influencing factors; emphasizing the direct and indirect effect, and information security policy compliance behavior provided from current researches. Furthermore, the paper also enhances the growing body of research that study the current theories in information security behavior, highlighting the need for organizational theories that specify compliance behavior. It also emphasizes the importance of implementing more technology-related behavior theories such as the technology acceptance model. Moreover, the study draws attention to the need to revisit neglected theories and models in this field; for instance, the task technology fit model which may provide new insight into the field. It also identified some research gaps that should be addressed in future researches. The study findings will provide guidelines for future studies that concentrate on ISPC behavior in the organizations.

This systematic literature review has provided several practical contributions for information security behavioral research. In light of the huge impact of attitude and self-efficacy found on ISPC behavior, managers could implement several strategies to shape their employees' behavior, such as frequent awareness and training programs, and facilitation of information security procedures and practices, so that employees can take responsibility for basic issues of information security. Given that punishment severity could engender compliance, the management should foster suitable sanctions within the organization. The studies confirmed the effect of perceived severity and perceived vulnerability in ISPC behavior; therefore, management should constantly remind employees of information security threats; and the extent of the damage caused by these threats [90]. Several studies indicate that better social bonding among the employees positively impacts ISPC behavior [45], [73]; therefore information security policymakers should take this information into account to improve compliance behavior [33]. Furthermore, the study proved that compliance behavior may be circumscribed by the employees' rational choices. Ifinedo [64] urges managers to clarify the advantages and benefits for the employees associated with compliance.

This study's findings show the important impact of SETA, leadership, and trust as compliance factors. Thus, the organization should provide an education and training program, and make it consistently available and easy to reach until the employees ultimately adopt security behavior. Leadership should guaranty employee knowledge about the ISP requirements, and leaders should adjust their behavior to impact the employees' behavior. Moreover, trust among the employees and their management must be enhanced, as this could effectively leverage the compliance behavior. This study also provides the main compliance factors that can assist security

TABLE 5. Overview of f theories influencing ISPC.

Theory	No of articles	Constructs	Relation to ISPC			
			Direct effect	Indirect effect	Partially effect	No/Week effect
Theory of Planned Behavior	23	Attuite	[3][41],[8],[5],[56],[80],[58],[100],[92],[68],[4],[65],[47],[21],[76],[60], [53]	[3]	[54],[77]	[57]
		Normative Belief	[58],[66]		[77]	[54]
		Self-Efficacy	[41], [50],[80],[58], [92],[68],[4],[76],[72], [52]	[75]		[7]
		Subjective Norms	[5],[100],[92],[68],[4]			[41],[8],[57],[56],[80],[65],[3]
		Descriptive Norms	[56]			[3]
		Perceived Behavioral Control	[8],[53]		[77]	[57]
General Deterrence Theory	16	Punishment Severity	[91],[56],[64],[106],[70]	[57],[54],[50],[49],[58],[45]		
		Punishment Celerity	[106]			[57],[45]
		Punishment Certainty	[8]			[106],[58],[45]
		Sanctions	[59],[74],[63],[82]			
		Certainty of Detection	[57],[56]			
		Shame	[63]			
Protection Motivation Theory	16	Response Efficacy	[57],[7],[97],[94],[58],[98],[67]	[20],[100],[56]		[90],[65],[111]
		Self-Efficacy	[50],[97],[90],[56],[65],[58]	[100]		[98]
		Response Cost	[57]	[56]		[4],[58]
		Perceived Vulnerability	[57],[97],[90],[65],[59],[60],[67]	[100],[56]	[94]	[98]
		Perceived Severity	[97],[65],[90],[94],[58],[70],[67]	[100],[56]		[4],[98]
Social Bond Theory	8	Attachment	[45],[73],[60],[53],[23]	[73]	[5]	[2],[59]
		Commitment	[45],[73],[23],[53]	[2],[73],[59]	[5]	[60]
		Involvement	[45],[73],[69],[23],[53]	[2],[73]	[5]	
		Personal Belief	[45],[73],[60],[23],[53]	[2],[73],[5],[59]		
Rational Choice Theory	7	Perceived Benefit of Compliance	[61],[62],[63]	[41],[7]		[54]
		Perceived Cost of Compliance	[64],[76]	[41],[7]		[61],[7]
		Perceived Cost of non Compliance	[62]	[41],[7]		
Social Exchange Theory	6	Supervisor-subordinate guanxi	[84]			
		Organizational commitment	[1],[51],[84],[79], [76]			[56]
		Developmental-oriented appraisal		[51]		
		Reward		[51]		
		Selective staffing		[51]		
		Training for career development		[51]		
Theory of Interpersonal Behavior	5	Roles	[20],[111],[25]			
		Habit	[20],[76]			[111],[8]
Organizational Theory	5	Top Management Support	[64],[72]	[52]		[57]
		Peer Pressure				[57]
		Organizational Climate		[60]		[57]

TABLE 5. *(Continued.)* **Overview of f theories influencing ISPC.**

Cognitive Evaluation Theory	5	Reward	[91],[76],[82]			[90],[45]
Self-Determination Theory	4	Self-determination		[95]		
		Competence	[103]	[107]		
		Autonomy	[103]	[96],[107]		
		Relatedness	[103]	[107]		
Neutralization Theory	3	Neutralization	[7]			[20],[111]
Theory of Reasoned Action	3	Attitude	[7],[90]			
		Normative Belief	[7],[90]			
		self-efficacy	[7],[63]			
		Subjective Norm	[75]			
Social Cognitive Theory	3	Self-efficacy	[18],[83],[5]			
		Locus of Control	[5]			

TABLE 6. **Less explored theories used in ISPC studies.**

Study	Theory Name	Study	Theory Name
[22],[47]	Affective Events Theory	[72]	Health belief Model
[111],[20]	Extended Parallel Processing Model	[105]	Social Influence Theory
[21],[2]	Involvement Theory	[69]	Expectancy Theory
[13],[96]	Psychological Reactance Theory	[106]	Social Learning Theory
[66],[75]	Technology Acceptance Model	[92]	Deontological Theory
[80],[110]	Theory of Personal Value Types	[92]	Teleological Theory
[13]	Organizational Control Theory	[95]	Self-Regulation Theory
[61]	Psychological Contract Theory	[1]	Organizational Support Theory
[19]	Social Norms Theory	[1]	Dual Labor Market Theory
[19]	Norm Activation Theory	[84]	Technology Threat Avoidance Theory
[93]	Neo-Institutional Theory	[22]	Coping Theory

managers and IT professionals to design their information security policies.

IX. CONCLUSION

This systematic literature review aimed to investigate existing studies that explore information security policy compliance. The main objective of this study was to examine the positive and negative (direct or indirect) impact of the human and organizational theories and their influencing factors toward ISPC behavior. The study attempted to answer three research questions by reviewing a total of 87 articles that examine the ISPC context. Comprehensively, this paper answered the following questions: What are the theories used in the information security policies compliance context? What is the kind of relation of influencing factors and information security policies compliance behavior? What are the factors concluded in studies that influence information security policy compliance?

This paper highlights the human behavior theories and organizational theories that are applied in existing articles. Moreover, it provides an investigation into relation between these theories and ISPC, and reviews several internal and external factors in relation to the ISPC. The results determine 35 applied human behavior theories and organizational theories, and 38 factors that could affect the ISPC. The results also showed that the theory of planned behavior, the general deterrence theory, and the protection motivation theory are the most frequently used. The most noteworthy finding revealed through this study is that most of the theories shape positively (direct or indirect) ISPC behavior. While the cost of compliance and naturalization are found in four studies to have a negative influence on ISPC behavior. Furthermore, a large number of internal and external factors have been monitored as affecting the ISPC. The findings indicate that internal factors play more of a role in motivating the ISPC behavior than external factors. Information security education, training and awareness, trust, and leadership, among many other internal and external factors, are highly used.

This study presents some limitations and provides recommendations for future research. First, although a comprehensive manual online search process was performed to select the studies, the remaining missing literature was

considered as a study limitation. This literature could improve the study results, therefore, future research should implement an automated search process to gain as much as possible of targeted studies. Second, the selected inclusion and exclusion criteria could be a limitation (e.g, including only theoretical and empirical articles, excluding technical reports and guidelines), therefore, considering these issues in future research could be significant. Third, this study was conducted with a range of nine years until the end of 2020 (the close of the research project), therefore, similar SLR about ISP compliance behavior in shorter periods produce more accurate results, and concentrate the recent interest of research. Finally, the identified gaps previously described in section VII are considered a valuable direction for future research. This paper contributes to information security research, and can assist other researchers in future investigation.

APPENDIX

See Tables 4–6.

ACKNOWLEDGMENT

The authors would like to thank Qassim University and the Deanship of Scientific Research for their support and funding the publication for this project.

REFERENCES

[1] S. Sharma and M. Warkentin, "Do i really belong?: Impact of employment status on information security policy compliance," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101397.
[2] N. S. Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Comput. Secur.*, vol. 56, pp. 70–82, Feb. 2016.
[3] I. Wiafe, F. N. Koranteng, A. Wiafe, E. N. Obeng, and W. Yaokumah, "The role of norms in information security policy compliance," *Inf. Comput. Secur.*, vol. 28, no. 5, pp. 743–761, Jun. 2020.
[4] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Comput. Secur.*, vol. 31, no. 1, pp. 83–95, Feb. 2012.
[5] P. Ifinedo, "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," *Inf. Manage.*, vol. 51, no. 1, pp. 69–79, Jan. 2014.
[6] S. E. Chang and C. Lin, "Exploring organizational culture for information security management," *Ind. Manage. Data Syst.*, vol. 107, no. 3, pp. 438–458, Apr. 2007.
[7] 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, Jan. 2014.
[8] Y. Hong and S. Furnell, "Motivating information security policy compliance: Insights from perceived organizational formalization," *J. Comput. Inf. Syst.*, vol. 59, pp. 1–10, Nov. 2019.
[9] J. Zhang, B. J. Reithel, and H. Li, "Impact of perceived technical protection on security behaviors," *Inf. Manage. Comput. Secur.*, vol. 17, no. 4, pp. 330–340, Oct. 2009.
[10] *FPO Headline X-Force Threat Intelligence Index*, Int. Bus. Mach., New York, NY, USA, 2019, pp. 1–36.
[11] *UK Organisations Still Failing to Prepare Effectively for Cyber Attack*. Accessed: Sep. 5, 2021. [Online]. Available: https://www.pwc.co.uk/press-room/press-releases/global-state-information-security-survey-2018-uk.html
[12] J.-Y. Son, "Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies," *Inf. Manage.*, vol. 48, no. 7, pp. 296–302, Oct. 2011.
[13] 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, Sep. 2015.
[14] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quart.*, vol. 34, no. 3, pp. 523–548, 2010.
[15] M. Alotaibi, S. Furnell, and N. Clarke, "Information security policies: A review of challenges and influencing factors," in *Proc. 11th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2016, pp. 352–358.
[16] S. Cuganesan, C. Steele, and A. Hart, "How senior management and workplace norms influence information security attitudes and self-efficacy," *Behav. Inf. Technol.*, vol. 37, no. 1, pp. 50–65, Jan. 2018.
[17] 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.
[18] A. Koohang, J. Anderson, J. H. Nord, and J. Paliszkiewicz, "Building an awareness-centered information security policy compliance model," *Ind. Manage. Data Syst.*, vol. 120, no. 1, pp. 231–247, Dec. 2019.
[19] A. Yazdanmehr and J. Wang, "Employees' information security policy compliance: A norm activation perspective," *Decis. Support Syst.*, vol. 92, pp. 36–46, Dec. 2016.
[20] G. D. Moody, M. Siponen, and S. Pahnil, "Toward a unified model of information security policy compliance," *MIS Quart.*, vol. 42, no. 1, pp. 285–311, Jan. 2018.
[21] E. Amankwa, M. Loock, and K. Elmarie, "Establishing information security policy compliance culture in organizations," *Inf. Comput. Secur.*, vol. 23, no. 3, pp. 1–29, 2018.
[22] J. D'Arcy and P.-L. Teh, "Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization," *Inf. Manage.*, vol. 56, no. 7, Nov. 2019, Art. no. 103151.
[23] 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.
[24] H. N. Chua, S. F. Wong, Y. C. Low, and Y. Chang, "Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations," *Telematics Informat.*, vol. 35, no. 6, pp. 1770–1780, Sep. 2018.
[25] A. Koohang, A. Nowak, J. Paliszkiewicz, and J. H. Nord, "Information security policy compliance: Leadership, trust, role values, and awareness," *J. Comput. Inf. Syst.*, vol. 60, no. 1, pp. 1–8, Jan. 2020.
[26] T. Sommestad and J. Hallberg, "A review of the theory of planned behaviour in the context of information security policy compliance," *IFIP Adv. Inf. Commun. Technol.*, vol. 405, pp. 257–271, Jul. 2013.
[27] T. Sommestad, J. Hallberg, K. Lundholm, and J. Bengtsson, "Variables influencing information security policy compliance: A systematic review of quantitative studies," *Inf. Manage. Comput. Secur.*, vol. 22, no. 1, pp. 42–75, Mar. 2014.
[28] W. A. Cram, J. Proudfoot, and J. D'Arcy, "Seeing the forest and the trees: A meta-analysis of information security policy compliance literature," in *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, 2017, pp. 4051–4060.
[29] S. Hina and P. D. D. Dominic, "Information security policies' compliance: A perspective for higher education institutions," *J. Comput. Inf. Syst.*, vol. 60, no. 3, pp. 201–211, 2020.
[30] S. Trang and B. Brendel, "A meta-analysis of deterrence theory in information security policy compliance research," *Inf. Syst. Frontiers*, vol. 21, no. 6, pp. 1265–1284, Dec. 2019.
[31] R. A. Alias, "Information security policy compliance: Systematic literature review," *Proc. Comput. Sci.*, vol. 161, pp. 1216–1224, Jan. 2019.
[32] P. Kuppusamy, G. N. Samy, N. Maarop, P. Magalingam, N. Kamaruddin, B. Shanmugam, and S. Perumal, "Systematic literature review of information security compliance behaviour theories," *J. Phys., Conf. Ser.*, vol. 1551, no. 1, May 2020, Art. no. 012005.
[33] 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, Apr. 2021.
[34] C. Okoli and K. Schabram, "A guide to conducting a systematic literature review of information systems research," *SSRN Electron. J.*, vol. 10, no. 26, pp. 1–49, 2010.
[35] S. Keele, "Guidelines for performing systematic literature reviews in software engineering, version 2.3," Dept. Comput. Sci., School Comput. Sci. Math., Softw. Eng. Group, Keele Univ., Keele, U.K., Tech. Rep. EBSE- 2007-01, 2007.
[36] U. A. Bukar, M. A. Jabar, F. Sidi, R. N. H. B. Nor, S. Abdullah, and M. Othman, "Crisis informatics in the context of social media crisis communication: Theoretical models, taxonomy, and open issues," *IEEE Access*, vol. 8, pp. 185842–185869, 2020.

[37] S. Vahdati, S. Fathalla, C. Lange, A. Behrend, A. Say, Z. Say, and S. Auer, "A comprehensive quality assessment framework for scientific events," *Scientometrics*, vol. 126, no. 1, pp. 641–682, 2021.
[38] E. R. T. Chiware and D. Becker, "Citation patterns of conference proceedings in Master's and doctoral studies: A case study of information technology and systems," *SAGE Open*, vol. 8, no. 2, Apr. 2018, Art. no. 215824401877049.
[39] L. I. Meho, "Using Scopus's CiteScore for assessing the quality of computer science conferences," *J. Informetrics*, vol. 13, no. 1, pp. 419–433, Feb. 2019.
[40] C. R. Kothari, *Research Methodology Methods & Techniques*, vol. 148. New Delhi, India: New Age Int. Publishers, 1990.
[41] 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.*, vol. 29, no. 1, pp. 43–69, Jan. 2019.
[42] J. Paliszkiewicz, "Information security policy compliance: Leadership and trust," *J. Comput. Inf. Syst.*, vol. 59, no. 3, pp. 211–217, May 2019.
[43] S. Bauer, E. W. N. Bernroider, and K. Chudzikowski, "Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks," *Comput. Secur.*, vol. 68, pp. 145–159, Jul. 2017.
[44] A. Tsohou and P. Holtkamp, "Are users competent to comply with information security policies? An analysis of professional competence models," *Inf. Technol. People*, vol. 31, no. 5, pp. 1047–1068, Sep. 2018.
[45] J. Liu, J. Zhang, and J. Zhang, "Validating a control-based model of information security policy compliance—A meta-analysis," in *Proc. 40th Int. Conf. Inf. Syst. (ICIS)*, 2020, pp. 1–17.
[46] T. Stafford, G. Deitz, and Y. Li, "The role of internal audit and user training in information security policy compliance," *Managerial Auditing J.*, vol. 33, no. 4, pp. 410–424, Jun. 2018.
[47] D. Ormond, M. Warkentin, and R. E. Crossler, "Integrating cognition with an affective lens to better understand information security policy compliance," *J. Assoc. Inf. Syst.*, vol. 20, no. 12, pp. 1794–1843, 2019.
[48] M. P. Buthelezi, J. A. Van Der Poll, and E. O. Ochola, "Ambiguity as a barrier to information security policy compliance: A content analysis," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2016, pp. 1360–1367.
[49] 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. Manage.*, vol. 55, no. 8, pp. 1049–1060, Dec. 2018.
[50] X. Chen, L. Chen, and D. Wu, "Factors that influence employees' security policy compliance: An awareness-motivation-capability perspective," *J. Comput. Inf. Syst.*, vol. 58, no. 4, pp. 312–324, Oct. 2018.
[51] Y. Choi, "Human resource management and security policy compliance," *Int. J. Hum. Capital Inf. Technol. Prof.*, vol. 8, no. 3, pp. 68–81, Jul. 2017.
[52] N. Humaidi and V. Balakrishnan, "Indirect effect of management support on users' compliance behaviour towards information security policies," *Health Inf. Manage. J.*, vol. 47, no. 1, pp. 17–27, Jan. 2018.
[53] R. F. Ali, P. D. D. Dominic, and P. K. Karunakaran, "Information security policy and compliance in oil and gas organizations—A pilot study," *Solid State Technol.*, vol. 63, pp. 1275–1282, Oct. 2020.
[54] M. R. A. Kadir, S. N. S. Norman, S. A. Rahman, A. R. Ahmad, and A. A. Bunawan, "Information security policies compliance among employees in cybersecurity Malaysia," in *Proc. 28th Int. Bus. Inf. Manag. Assoc. Conf. Vis. Innov. Manag. Dev. Sustain. Compet. Econ. Growth*, Nov. 2016, pp. 2419–2430.
[55] E. Kolkowska and G. Dhillon, "Organizational power and information security rule compliance," *Comput. Secur.*, vol. 33, pp. 3–11, Mar. 2013.
[56] T. Ryutov, N. Sintov, M. Zhao, and R. S. John, "Predicting information security policy compliance intentions and behavior for six employee-based risks," *J. Inf. Priv. Secur.*, vol. 13, no. 4, pp. 260–281, 2018.
[57] 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, Jan. 2019.
[58] A. Nasir, R. A. Arshah, and M. R. A. Hamid, "The significance of main constructs of theory of planned behavior in recent information security policy compliance behavior study: A comparison among top three behavioral theories," *Int. J. Eng. Technol.*, vol. 7, no. 2.29, p. 737, May 2018.
[59] M. Choi and J. Song, "Social control through deterrence on the compliance with information security policy," *Soft Comput.*, vol. 22, no. 20, pp. 6765–6772, Oct. 2018.
[60] P. Ifinedo, "Roles of organizational climate, social bonds, and perceptions of security threats on IS security policy compliance intentions," *Inf. Resour. Manage. J.*, vol. 31, no. 1, pp. 53–82, Jan. 2018.
[61] J. 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, May 2017.
[62] H. L. Kim and J. Han, "Do employees in a 'good' company comply better with information security policy? A corporate social responsibility perspective," *Inf. Technol. People*, vol. 32, no. 4, pp. 858–875, Aug. 2019.
[63] T. M. Arage, F. Bélanger, and T. B. Tesema, "Influence of national culture on employees' compliance with information systems security (ISS) policies: Towards ISS culture in Ethiopian companies," in *Proc. Amer. Conf. Inf. Syst. (AMCIS)*, 2015, pp. 1–7.
[64] P. Ifinedo, "Critical times for organizations: What should be done to curb Workers' noncompliance with IS security policy guidelines?" *Inf. Syst. Manage.*, vol. 33, no. 1, pp. 30–41, Jan. 2016.
[65] S. Hina, D. D. D. P. Selvam, and P. B. Lowry, "Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101594.
[66] J. Abed, G. Dhillon, and S. Ozkan, "Investigating continuous security compliance behavior: Insights from information systems continuance model," in *Proc. AMCIS Surfing IT Innov. Wave 22nd Amer. Conf. Inf. Syst.*, 2016, pp. 1–10.
[67] C. Liu, C. Wang, H. Wang, and B. Niu, "Influencing factors of employees' information systems security police compliance: An empirical research in China," in *Proc. E3S Web Conf.*, vol. 218, 2020, Art. no. 04032.
[68] A. Al-Omari, O. El-Gayar, and A. Deokar, "Information security policy compliance: The role of information security awareness," in *Proc. 18th Amer. Conf. Inf. Syst. (AMCIS)* vol. 2, Dec. 2015, pp. 1633–1640.
[69] A. J. Burns, T. L. Roberts, C. Posey, R. J. Bennett, and J. F. Courtney, "Intentions to comply versus intentions to protect: A VIE theory approach to understanding the influence of Insiders' awareness of organizational SETA efforts," *Decis. Sci.*, vol. 49, no. 6, pp. 1187–1228, Dec. 2018.
[70] M. Kretzer and A. Maedche, "Which are the most effective measures for improving employees' security compliance? Designing user assistance view project designing conversational requirements elicitation systems view project," in *Proc. 36th Int. Conf. Inf. Syst (ICIS)*, Dec. 2015.
[71] S. Bahtiyar and M. U. Çaglayan, "Trust assessment of security for e-health systems," *Electron. Commerce Res. Appl.*, vol. 13, no. 3, pp. 164–177, May/Jun. 2014.
[72] N. Humaidi and V. Balakrishnan, "The Moderating effect of working experience on health information system security policies compliance behaviour," *Malaysian J. Comput. Sci.*, vol. 28, no. 2, pp. 70–92, 2015.
[73] G. Feng, J. Zhu, N. Wang, and H. Liang, "How paternalistic leadership influences it security policy compliance: The mediating role of the social bond," *J. Assoc. Inf. Syst.*, vol. 20, no. 11, pp. 1650–1691, 2019.
[74] D. Sikolia, M. Mason, D. Biros, and M. Weiser, "A theory of employee compliance with information security," in *Proc. MWAIS*, 2014, pp. 1–6.
[75] A. Al-Omari, O. El-Gayar, and A. Deokar, "Security policy compliance: User acceptance perspective," in *Proc. 45th Hawaii Int. Conf. Syst. Sci.*, Jan. 2012, pp. 3317–3326.
[76] R. A. Alias, "A model of information security policy compliance for public universities: A conceptual model," *Adv. Intell. Syst. Comput.*, vol. 1073, pp. 810–818, Sep. 2020.
[77] T. Sommestad, "Work-related groups and information security policy compliance," *Inf. Comput. Secur.*, vol. 26, pp. 1–18, Nov. 2018.
[78] H. Lee, S. Jeon, and A. Zeelim-Hovav, "Impact of psychological empowerment, position and awareness of audit on information security policy compliance intention," in *Proc. Pacific Asia Conf. Inf. Syst. (PACIS)*, 2016.
[79] J. Goo, M. S. Yim, and D. J. Kim, "A path to successful management of employee security compliance: An empirical study of information security climate," *IEEE Trans. Prof. Commun.*, vol. 57, no. 4, pp. 286–308, Dec. 2014.
[80] B. Borena and F. Bélanger, "Religiosity and information security policy compliance," in *Proc. 19th Amer. Conf. Inf. Syst. (AMCIS) Hyperconnected World Anything, Anywhere, Anytime*, vol. 4, 2013, pp. 2848–2855.
[81] J. A. Alalwan, "Fear of cybercrime and the compliance with information security policies: A theoretical study," in *Proc. ACM Int. Conf. Proc. Ser.*, 2018, pp. 85–87.
[82] A. Yazdanmehr, J. Wang, and Z. Yang, "Peers matter: The moderating role of social influence on information security policy compliance," *Inf. Syst. J.*, vol. 30, no. 5, pp. 791–844, Sep. 2020.
[83] H. W. Huang, N. Parolia, and K. T. Cheng, "Willingness and ability to perform Information security compliance behavior: Psychological ownership and self-efficacy perspective," in *Proc. Pacific Asia Conf. Inf. Syst. (PACIS)*, 2016, p. 57.

[84] C. Liu, N. Wang, and H. Liang, "Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment," *Int. J. Inf. Manage.*, vol. 54, Oct. 2020, Art. no. 102152.
[85] S. S. Kim and Y. J. Kim, "The effect of compliance knowledge and compliance support systems on information security compliance behavior," *J. Knowl. Manage.*, vol. 21, no. 4, pp. 986–1010, Jul. 2017.
[86] I. Topa and M. Karyda, "Identifying factors that influence employees' security behavior for enhancing ISP compliance," in *Proc. Int. Conf. Trust Privacy Digit. Bus.*, vol. 9264. Cham, Switzerland: Springer, 2015, pp. 169–179.
[87] *Healthcare Breach Report 2021 Hacking and IT Incidents on the Rise*, Bitglass, Campbell, CA, USA, 2021, p. 9.
[88] F. Liébana-Cabanillas, V. Marinkovic, I. Ramos de Luna, and Z. Kalinic, "Predicting the determinants of mobile payment acceptance: A hybrid SEM-neural network approach," *Technol. Forecasting Social Change*, vol. 129, pp. 117–130, Apr. 2018.
[89] A. S. A. Alwabel and X.-J. Zeng, "Data-driven modeling of technology acceptance: A machine learning perspective," *Expert Syst. Appl.*, vol. 185, Dec. 2021, Art. no. 115584.
[90] M. Siponen, M. A. Mahmood, and S. Pahnila, "Employees' adherence to information security policies: An exploratory field study," *Inf. Manage.*, vol. 51, no. 2, pp. 217–224, Mar. 2014.
[91] Y. Chen, K. Ramamurthy, and K.-W. Wen, "Organizations' information security policy compliance: Stick or carrot approach?" *J. Manage. Inf. Syst.*, vol. 29, no. 3, pp. 157–188, Dec. 2012.
[92] A. Al-Omari, A. Deokar, O. El-Gayar, J. Walters, and H. Aleassa, "Information security policy compliance: An empirical study of ethical ideology," in *Proc. 46th Hawaii Int. Conf. Syst. Sci.*, Jan. 2013, pp. 3018–3027.
[93] H. J. Kam, P. Katerattanakul, G. Gogolin, and S. Hong, "Information security policy compliance in higher education: A neo-institutional perspective," in *Proc. Pacific Asia Conf. Inf. Syst. (PACIS)*, 2013, p. 106.
[94] S. Pahnila, M. Karjalainen, and M. Siponen, "Information security behavior: Towards multistage models," in *Proc. Pacific Asia Conf. Inf. Syst. (PACIS)*, 2013, p. 102.
[95] M. Luecke and J. Simon, "A self-regulatory approach to behavioral compliance with is security policies—'Come on, baby, do the locomotion,'" in *Proc. 20th Amer. Conf. Inf. Syst. (AMCIS)*, 2014, pp. 1–11.
[96] 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. Privacy Secur.*, vol. 9, no. 4, pp. 52–79, Oct. 2013.
[97] S. Hina and D. D. Dominic, "Information security policies: Investigation of compliance in universities," in *Proc. 3rd Int. Conf. Comput. Inf. Sci. (ICCOINS)*, Aug. 2016, pp. 564–569.
[98] D. Sikolia, D. Twitchell, and G. Sagers, "Employees' adherence to information security policies: A partial replication," in *Proc. AMCIS Surfing IT Innov. Wave 22nd Amer. Conf. Inf. Syst.*, 2016, pp. 1–9.
[99] T. Sommestad, H. Karlzén, and J. Hallberg, "The theory of planned behavior and information security policy compliance," *J. Comput. Inf. Syst.*, vol. 59, no. 4, pp. 344–353, Jul. 2019.
[100] S. Hina and D. D. Dominic, "Need for information security policies compliance: A perspective in higher education institutions," in *Proc. Int. Conf. Res. Innov. Inf. Syst. (ICRIIS)*, Jul. 2017, pp. 1–6.
[101] S. Kurowski and F. Dietrich, "Response and cultural biases in information security policy compliance research," Open Identity Summit, Karlstad, Sweden, 2017, pp. 13–24.
[102] M. Niemimaa, "The incorrect compliance and the correct noncompliance with information security policies: A conceptual categorization of seven types of rule-related behavior," in *Proc. 12th Pre-ICIS Workshop Inf. Secur. Privacy*, Seoul, South Korea, Dec. 2017.
[103] A. Alzahrani, C. Johnson, and S. Altamimi, "Information security policy compliance: Investigating the role of intrinsic motivation towards policy compliance in the organisation," in *Proc. 4th Int. Conf. Inf. Manage. (ICIM)*, May 2018, pp. 128–132.
[104] N. Depaula, "Understanding insiders: Theories and challenges in information security policy compliance research," *World Sci. B. Chapters*, vol. 4, no. 5, pp. 27–45, 2018.
[105] M. Park and S. Chai, "Internalization of information security policy and information security practice: A comparison with compliance," in *Proc. 51st Hawaii Int. Conf. Syst. Sci.*, 2018, pp. 4723–4731.
[106] T. B. Lembcke, S. Trang, P. Plics, K. Masuch, S. Hengstler, and M. Pamuk, "Fostering information security compliance: Comparing the predictive power of social learning theory and deterrence theory," in *Proc. 25th Amer. Conf. Inf. Syst. (AMCIS)*, 2019, pp. 1–10.
[107] Y. Gangire, A. Da Veiga, and M. Herselman, "A conceptual model of information security compliant behaviour based on the self-determination theory," in *Proc. Conf. Inf. Commun. Technol. Soc. (ICTAS)*, Mar. 2019, pp. 1–6.
[108] M. Alotaibi, S. Furnell, and N. Clarke, "A framework for reporting and dealing with end-user security policy compliance," *Inf. Comput. Secur.*, vol. 27, no. 1, pp. 1–21, Sep. 2019.
[109] S. H. Bhaharin, U. A. Mokhtar, R. Sulaiman, and M. M. Yusof, "Issues and trends in information security policy compliance," in *Proc. 6th Int. Conf. Res. Innov. Inf. Syst. (ICRIIS)*, Dec. 2019, pp. 1–6.
[110] C. I. Torres and R. Crossler, "Information security compliance: A complete values view," in *Proc. 25th Amer. Conf. Inf. Syst. (AMCIS)*, 2019, pp. 1–5.
[111] A. Koohang, J. H. Nord, Z. V. Sandoval, and J. Paliszkiewicz, "Reliability, validity, and strength of a unified model for information security policy compliance," *J. Comput. Inf. Syst.*, vol. 61, no. 2, pp. 99–107, Mar. 2021.

MADA ALASSAF received the B.S. degree in computer science from the University of Hafer Albatin, in 2016. She is currently pursuing the master's degree in information security with the College of Computer, Qassim University, Saudi Arabia. Her research interests include the behavioral and organizational aspects of information security.

ALI ALKHALIFAH received the B.S. degree in computer science from Qassim University, in 2007, the master's degree (Hons.) in IT from the University of Newcastle, in 2010, and the Ph.D. degree in information systems from the University of New South Wales, Australia, in 2013. He is currently an Associate Professor with the IT Department, College of Computer, Qassim University. He has been involved in several program committees and is being a reviewer in different international conferences and journals. He has a number of high ranking journal and conference papers research. His research interests include information security, information systems, IT adoption, E-commerce, and human–computer interaction.