applied sciences

MDPI

Review

Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance

Rao Faizan Ali [1,*], P. D. D. Dominic [1,*], Syed Emad Azhar Ali [2], Mobashar Rehman [3] and Abid Sohail [4]

[1] Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Seri Iskandar 32610, Perak Darul Ridzuan, Malaysia
[2] Department of Management & Humanities, Universiti Teknologi PETRONAS, Seri Iskandar 32610, Perak Darul Ridzuan, Malaysia; syed_17007896@utp.edu.my
[3] Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman, Kampar 31900, Perak Darul Ridzuan, Malaysia; mobashar@utar.edu.my
[4] Department of Computer Science, COMSATS University Islamabad, Lahore 54000, Pakistan; abidbhutta@cuilahore.edu.pk
* Correspondence: rao_16001107@utp.edu.my (R.F.A.); dhanapal_d@utp.edu.my (P.D.D.D.)

Abstract: A grave concern to an organization's information security is employees' behavior when they do not value information security policy compliance (ISPC). Most ISPC studies evaluate compliance and noncompliance behaviors separately. However, the literature lacks a comprehensive understanding of the factors that transform the employees' behavior from noncompliance to compliance. Therefore, we conducted a systematic literature review (SLR), highlighting the studies done concerning information security behavior (ISB) towards ISPC in multiple settings: research frameworks, research designs, and research methodologies over the last decade. We found that ISPC research focused more on compliance behaviors than noncompliance behaviors. Value conflicts, security-related stress, and neutralization, among many other factors, provided significant evidence towards noncompliance. At the same time, internal/external and protection motivations proved positively significant towards compliance behaviors. Employees perceive internal and external motivations from their social circle, management behaviors, and organizational culture to adopt security-aware behaviors. Deterrence techniques, management behaviors, culture, and information security awareness play a vital role in transforming employees' noncompliance into compliance behaviors. This SLR's motivation is to synthesize the literature on ISPC and ISB, identifying the behavioral transformation process from noncompliance to compliance. This SLR contributes to information system security literature by providing a behavior transformation process model based on the existing ISPC literature.

Keywords: information security behavior; information security policy compliance; systematic literature review (SLR); process management; compliance; noncompliance; transformation process

Citation: Ali, R.F.; Dominic, P.D.D.; Ali, S.E.A.; Rehman, M.; Sohail, A. Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Appl. Sci.* **2021**, *11*, 3383. https://doi.org/10.3390/app11083383

Academic Editor: George Drosatos

Received: 24 March 2021
Accepted: 6 April 2021
Published: 9 April 2021

1. Introduction

In today's hyperconnected world, businesses now use technology to collect, store and share essential information. There is a significant threat of that information being accessed, disrupted, modified, corrupted, or destroyed illegally by malicious and unauthorized actors. That is where information security comes in: these are the measures that companies put in place to stop the threats meted against their valued information. The extensive and variable risks businesses face upon falling victim to a data breach can damage business revenue and reputation [1,2]. Research shows that about 70% of incidents happened due to human negligence (intentional or unintentional). A study on security professionals' behavior concluded that 43% of data breaches are due to employees' behavior [3,4]. In 2014 IBM cybersecurity intelligence index reported almost 95% of information security

incidents to involve employee negligence [5]. Attackers target employees' behavior to execute their malicious activities. A British study concluded that 58 percent of attacks in British organizations are due to insider threats. Thirty-three per cent of these attacks are due to noncompliance with an organization's information security policies (ISP's) and regulations [6]. To mitigate organizational information security threats, most organizations have adopted standard guidelines provided by the National Institute of Standard and Technology (NIST). The NIST framework emphasized ISP Compliance and described it as an essential measure of information security [7].

Multiple information security management standards are used by the organizations, such as; Control Objectives for Information and Related Technologies (COBIT), International Organization for Standardization (ISO), and International Electrotechnical Commission (IEC) (ISO/IEC 27001). For extenuating security risks, organizations consider establishing information security standards (ISO/IEC 27001 and ISO/IEC 27002) for best practices. These guidelines and policies provide the best direction for information security. A detailed policy document contains behavioral checks, recovery processes, and technical controls to deal with a successful security breach [8]. Researchers have suggested many ways to adopt these standards, but there are behavioral issues in adapting the standards.

On the other hand, organizations do not focus on their internal problems while designing an information security policy [9]. Information security in organizations incorporates a complicated process that involves many factors, such as education, human factors, and technology, which it is necessary to manage under one security model [10]. Organizations need to monitor employees' behaviors and evaluate the factors which influence employees' work performance. Various studies suggested that stress, work impediment, and coworker behaviors influence employees' behaviors [11,12]. Furthermore, positive management behaviors (behaviors adopted by the organization's management) and social behaviors (coworkers' and peers' behaviors) help enhance security-aware behaviors, which leads to good security culture in organizations.

Information security policy compliance (ISPC) is a matter of human behavior. Numerous researchers tried to provide solutions with the help of psychological theories [13–15]. Many frameworks are provided by researchers using different external factors and theoretical constructs. ISPC research evaluates human behavior in two main dimensions—intention to comply and intention to violate. More specifically, researchers try to determine what motivates employees to comply and to violate the ISP. Many researchers, for instance, [3,15–17], focused on behaviors related to compliance with ISP. In contrast, many studies such as [13,18–20] explored violation behaviors. Studies evaluating compliance behaviors concluded that effective security management, proper security awareness, a good security culture, and other behavioral factors enhance employee ISP compliance, while studies focused on noncompliance stated that employees' noncompliance with ISP could be intentional or unintentional, psychological or external.

The assessment of human behavior is a complicated phenomenon, and several psychological theories have been proposed to cover different aspects of human behavior. Likewise, assessing individual's intention towards information security is a complicated subject [21]. In this regard, multiple IS researchers proposed various research models and theories to assess individuals' behaviors towards information security policies [12,22,23]. To some extent, researchers have successfully incorporated behavioral theories in the IS context, but still, many gaps remain open. For instance, [13] described that deterrence theory has multiple behavioral outcomes and inconsistent results.

Similarly, the authors in [24] provided a taxonomy for the theory of protection motivation and described the reasons for inconsistent outcomes for protection motivation theory in IS research. Moreover, they stated that researchers must use core and full constructs of protection motivation theories in a correct manner for measuring protection motivation behaviors. Likewise, there are similar outcomes for each behavioral theory used in the IS research. Multiple frameworks are available to assess human intentions towards information security policies, but none of the frameworks can be used as a standard behavioral process

model. All the frameworks defined in the extant literature are either specific to a sector (for example, finance, higher education) [25,26] or specific to various theories [18,24,27]. None of the previous studies has made an effort to develop a consolidated information security behavior process which can exhibit the transformation process from noncompliance to compliance. There is a dire need to identify a behavioral transformation process incorporating major behavioral theories and components affecting information security behavior.

This paper aims to determine employees' noncompliance behavior's transformation steps to compliance behavior to develop a process model. For this purpose, the authors have systematically reviewed studies that have addressed the nexus of information security behavior and ISPC. We have analyzed the results, sample sizes, methodologies, and frameworks published in studies published in the last decade (i.e., 2010 to 2020). Moreover, the current paper has reviewed and analyzed the available literature systematically to acquire insight into the behavioral theories and factors that contribute significantly to ISPC. Our systematic literature review (SLR) followed the review protocol from [25,28]. A standard modeling language and platform are used in the current study to generate a formal process model for information security behavior transformation.

In order to develop a process model, process management is deemed as the next crucial step. Typically, process management is explained as an effective way to present all the objective and subjective business goals in graphical format [29]. A process is a pictorial illustration of a specific goal, while Business Process Management is the art of skillfully presenting the said goal [30,31]. There are many modeling languages available for process modeling, such as Business Process Modeling Notation (BPMN), Event-Driven Process Chains (EPC), Yet Another Workflow Language (YAWL), and Petri nets. In this paper, the authors follow the standard language BPMN. The process for behavior transformation has been drawn using SIGNAVIO, an online tool available for process development. The developed process model can help information security managers to understand the behaviors related to security policy compliance/noncompliance. Thus, this paper focused on information security behavioral studies to evaluate all the concepts used in the last decade for information security behavior (ISB) towards ISP compliance/noncompliance. The current review will also help researchers find the transformation activities and noncompliance behavior events to compliance behavior.

Section 2 describes the related literature and its limitations, together with the motivation for the current review. The formulation and methodology of the research questions are described in Section 3. Section 4 shows a detailed evaluation of the literature review results. Section 5 (i.e., discussion) sheds light on the summary of the findings as well as the theoretical and practical implications of this study. Finally, an appendix section details the terminologies/factors used in this review.

2. Literature Review

A significant body of research has discussed various information security policy compliance/noncompliance behaviors [28,32,33]. Various studies presented behavioral theories as influential factors in individuals' information security behavior [13,28,34]. Another class of studies focuses on providing composite information security compliance frameworks with previous literature [35]. Some researchers enhanced the body of knowledge by providing taxonomies of information security behaviors [36,37]. Both types of behaviors (i.e., compliance/noncompliance) have direct or indirect effects on organizations' information security. Compliance enhancement studies mainly discuss the methods and procedures that can improve individuals' psychological behavior towards organizational security policies [11,12,15]. On the other hand, studies focusing on noncompliance provide solutions towards mitigating the individuals' malicious behaviors [34,38,39]. Among all the information security policy compliance systematic literature reviews, we did include studies focusing on enhancing compliance and discouraging noncompliance behavior from well-established information systems security journals and conferences.

2.1. Information Security Behavior and Compliance towards Information Security Policies

Information security behavior comprised many psychological components. Most of the researchers examined information security behavior with the help of psychological theories such as protection motivation theory [24,40], the theory of planned behavior [14], the theory of reasoned action [41], and many other valuable theories. Information security behavioral studies primarily focus on organizational information security policies compliance/noncompliance by employees. Several researchers presented helpful solutions towards the ISPC [11,42]. The researchers posed information security policy compliance as a behavioral problem, and discussed many factors that could enhance compliance towards organizations' ISPs [15,18]. For instance, [43,44] discussed the fact that behavioral activities vary from culture to culture, as any region's national culture influences ISB's compliance with ISPs. Meanwhile, many researchers argued that intrinsic (i.e., self-esteem and achievements) and extrinsic motivations (i.e., rewards and appreciation) play a vital role in enhancing compliance behavior among employees [8,18].

Moreover, several researchers examined protection motivations upon information security behavior and established that an individual's compliance with organizational policies depends on the perceived protection motivations [40,45]. Studies have argued that information security culture and information security awareness are the most influential factors in this regard. It has also been argued that organizations with better information security culture are less likely to face an information security breach [46]. Similarly, information security awareness among employees creates a healthy security culture [47]. However, it is the organization's management's responsibility to enhance information security awareness among its employees. In most cases, an organization's management's good strategies for enhancing information security policy compliance lead them to cultivate a good information security culture [48,49].

2.2. Information Security Behavior and Noncompliance towards Information Security Policies

Besides enhancing compliance behavior, it is also essential to evaluate the causes and solutions of employees' noncompliant behavior—there is plenty of literature on the causes of and solutions for noncompliance or the intent to violate security policies. For instance, researchers have indicated that sometimes employees perceive information security as an external stress. They do not feel that security is their responsibility, so they indulge in security-related conflicts, resulting in noncompliant behavior [39,40,42]. Other than this, literature suggested that heavy security requirements cause security-related stress among employees, and they tend to violate information security policy without volitional intent [12,20]. Furthermore, the literature suggested that most employees violate organizational policies because of injustice in the workplace by top management. Organizational injustice causes a lack of motivation among employees and elicits negative emotions, resulting in noncompliance behavior [12]. The existing studies further elaborated that employees justify their wrongdoings in several ways. Gresham Sykes described this process as neutralization [50]. They have enlisted seven neutralization techniques on how an individual justifies their criminal activities.

Most researchers provided solutions for noncompliant behavior with criminological theories (for instance, crime pattern theory, social control theory, deterrence theory) [39,51,52]. Furthermore, some researchers provided solutions with deterrence or punishments to insiders [23,34]. However, many researchers argued that punishments and deterrence are not always the right way to mitigate noncompliance [53]. Multiple studies provided solutions for theory and practice with longitudinal studies and stated that enhanced employee socialization and protective behaviors could mitigate noncompliance behaviors [11,54]. In short, several researchers have presented solutions to behavioral noncompliance and have also recommended solutions for employee behavioral compliance. Nevertheless, none of the researchers provided any generic process outlining causes and solutions for noncompliance to compliance behavior. Thus, a systematic literature review concerning noncompliance to compliance behavior will equip information security

researchers with a pragmatic timeline that allows other behavioral information security avenues to be examined.

2.3. Related Research and Motivations for the Current Review

The current systematic literature review is among the reviews on information security behavior and information security policy compliance. The existing studies in this regard are either providing insights into components that influence information security policy compliance (i.e., security culture, security awareness, security management) or examine behavioral theories (i.e., deterrence, protection motivation, planned behavior, and others).

A component-based literature review covering 51 articles was performed by [26], addressing information security culture, awareness, and management issues. Similarly, [55] performed systematic literature of 79 studies emphasizing information security culture issues. Another literature review by [25] analyzed the dimensions of information security management from 43 studies for higher education institutes. Likewise, [56] conducted a systematic literature review to evaluate multiple dimensions for information security management and stated that a more holistic approach is needed to manage information security in organizations.

A systematic literature review on deterrence theory and its implication towards information systems literature has been performed by [13]. Similar efforts have been performed by [34] through a meta-analysis covering 35 articles based on deterrence theory towards ISPC research. Furthermore, [37] developed a systematic taxonomy for protecting insider employees' motivated behaviors. Similarly, [32] presented a meta-analysis covering 30 research articles on protection motivation theory and its effects on information security behavior. The most relevant literature review has been conducted by [28] in which 60 compliance and noncompliance are influencing factors were fetched from 29 articles. According to their review, there were no clear winners of most influencing factors or the theory for compliance or incompliance. It was the first systematic review that measured variables that influence compliance/incompliance with information security policies. To the best of our knowledge, none of the previous systematic literature reviews simultaneously integrated theory and components. The current study has integrated both (i.e., components and theories) to design a behavior transformation process.

In light of the studies mentioned above, the current systematic literature review will illuminate the studies examining compliance and noncompliance theories and components, but importantly reviews the literature to draw a behavior transformation process from noncompliance to compliance. Furthermore, this study has systematically reviewed and analyzed the available literature to gain insights into the components and theories influencing compliance and noncompliance. In brief, this systematic literature review is expected to contribute to the current body of information systems reviews with a novel behavior transformation process that will help information security researchers and managers to understand what causes noncompliance and what strategies enhance compliance behaviors. A detailed comparison of the existing studies' limitations is presented in Table 1.

Table 1. Comparison with existing literature (limitations of existing reviews).

Authors	Sample Size	Category	Findings	Limitations
[26]	51 articles	Component-based SLR	Information security awareness, culture, and management are critical factors for the assessment of information security policy compliance	1. Review was only related to higher education institutions 2. Only three components were discussed (awareness, culture and, management)
[55]	79 articles	Component-based SLR	Information security culture is a multidimensional component and essential for incorporating information security policy compliance (ISPC) behaviors in organizations	1. Review was only targeted towards one component of behavioral information security domain (information security culture)

Table 1. *Cont.*

Authors	Sample Size	Category	Findings	Limitations
[25]	43 articles	Component-based SLR	Information security management can enhance ISPC in higher education institutions	1. Only one component of behavioral information security discussed. 2. Review was only targeted towards higher education institutions.
[56]	39 articles	Component-based SLR	Management role should be considered to cultivate good ISPC in organizations	1. Review was only targeted towards one component of the behavioral information security domain (information security management)
[13]	60 articles	Theory-based SLR	Methodological and additional substantive issues are the reason for the inconsistent results of deterrence theory.	1. The systematic literature review (SLR) was only related to deterrence theory
[34]	35 articles	Theory-based SLR	Deterrence theory (except sanction celerity) affects ISP compliance behavior, and deterrence effects vary with different cultures	1. The review only discusses the problems and inconsistencies related to deterrence theory
[32]	30 articles	Theory-based SLR	Protection motivation behaviors are critical for enhancing ISPC	1. SLR was only based on protection motivation behaviors
[28]	29 articles	Variable based SLR	There were no clear winners of the most influencing variable or the theory for compliance or incompliance	1. Small dataset 2. Variable based analysis

3. Methodology

The grounded theory approach has been used for this systematic literature review. The authors followed the theory proposed by [57]. This theory helps researchers to review step by step and explore more depth and breadth on the topic. The acquired approach consisted of five main phases (define, search, select, analyze, and present) illustrated in Figure 1.

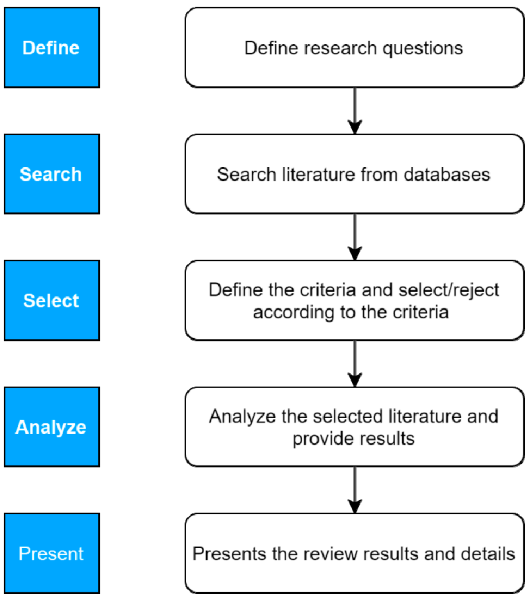

Figure 1. Literature review methodology.

First, a review plan has been designed, and research questions are formulated to extend the investigation [58].

1. What are the behavioral factors concluded in studies as a significant determinant of information security policy compliance?
2. What are the behavioral factors concluded in studies as a significant determinant of information security policy noncompliance?
3. What are the best possible transformation steps of behavior as analyzed in studies from noncompliance to compliance?

Second, the search scope is defined and restricted to computer science, social science, information systems, and information security (behavioral aspect). This study focused on automated and manual search processes to gain as many research articles as possible to fulfill the defined objectives. Queries and keywords were developed according to research objectives to search databases enlisted in Table 2. As discussed earlier, a manual search process has also been performed through search engines and reference lists of related articles.

Table 2. Keywords and queries.

Keywords	Queries
Information security behavior	"Information security policy" OR "security policies" OR" policy compliance" AND "information security behavior"
Inform security policy compliance	"Information security behavioral compliance" AND "organizational ICT" OR "IT"
ICT	" ICT policies OR security policy" AND" information security behavioral compliance"
Organizational information security policy	" Organizational security policy" OR" regulations" OR" guidelines" OR" policies compliance" AND" information security behaviors"
Information security policy	Employee OR user OR "staff information security policy compliance" AND "violations" OR "non-compliance behaviors"
Information security policy behavioral compliance	"Information security policy compliance" OR "behavioral policy compliance" AND "information security behaviors"
Information security policy noncompliance	"Information security policy non-compliance" OR "violations" AND "information security behaviors"
Information security policy violations	"Information security policy violation" OR "deviance" OR "volitional security behavior"

Keywords and queries were mapped onto the downloaded articles from reliable search engines and databases listed in Table 3. Full texts and downloaded abstracts were thoroughly explored, and 514 articles were selected in the first phase.

Table 3. Databases and search engines.

Data Bases	Search Engines
Scopus®®® by Elsevier B.V IEEE Xplore®®® Digital Library by IEEE ScienceDirect®®® by Elsevier B.V Web of Science™ by Clarivate AIS Electronic Library ACM Digital Library	Google Scholar®®® by Google Yahoo!™ RefSeek™ (privately held)

Third, the selection process performed by the defined selection and rejection criteria as follows: articles were selected for study if:

1. English is the language of the article.
2. Articles are related to information security behavior and information security policy compliance.

3. Article was published in a journal between 2010 and 2020.

Articles were rejected for review if:

1. The article is related to information security behavior but not information security policy compliance or vice versa.
2. Articles are related to other than organizational security policy compliance. For example, home users.
3. Articles with just management/awareness/culture without any behavioral aspect.
4. Articles related to cybersecurity not information security.
5. Articles without any methodological evidence.
6. A book, magazine, thesis, or a report.

After applying the selection criteria to 514 downloaded articles, 41 articles were excluded due to duplication, 215 articles were rejected after reading the abstract, and two experts reviewed the remaining 258 papers. One hundred and eighty papers were rejected after a full read of articles by two experts with reasons. Finally, two papers were added from references. Hence, 80 studies (qualitative, quantitative, and literature review) in total were selected for this review. Figure 2 presents the studies' inclusion and exclusion process Figure 3 exhibits the year wise study inclusion, whereas Figure 4 depicts the methodologies adopted in each study.

Figure 2. Flow diagram regarding the inclusion and exclusion of studies in this review.

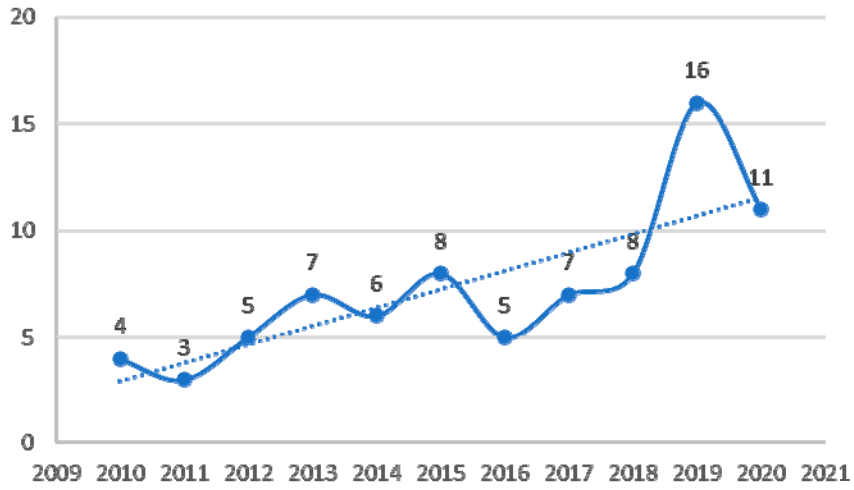

Figure 3. Number of publications per year.

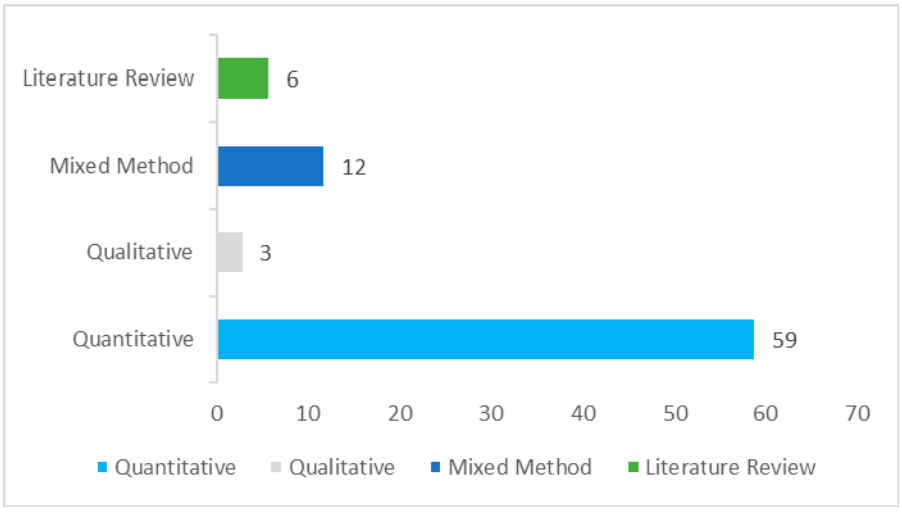

Figure 4. Research methodologies adopted in the sample.

Fourth, analysis of the 80 studies was performed by text coding [57]. Following the research questions, categories and subcategories identified and clarified every subcategory attribute by open coding. Axial coding is performed by drawing the logical connection between each category and subcategory. Fifth, the results of the analysis of the selected studies are presented in detail.

4. Results and Analysis

4.1. Analysis of Compliance Behavior

This section sheds light on the RQ1 of this SLR (i.e., What are the behavioral factors concluded in studies as a significant determinant of influencing information security policy compliance?). In this section, we have evaluated the studies related to supportive factors towards information security policy compliance. This section analyzed the studies' results related to national culture, protection motivations, security awareness, culture, social behaviors, management behaviors, and actual compliance effects on employees' compliance to information security policies.

4.1.1. National Culture and Compliance

Among many factors, national culture influences the psychology of individuals. Cultural variation affects human compliance towards ISP. In this context, [44] conducted a qualitative study based on the analytical grounded theory approach. The study's primary

purpose was to identify the effects of national culture on ISB employees towards ISP. The researchers conducted 19 semi-structured interviews with participants from the US and Ireland. After summarizing the results, it was established that US employees have more adaptive behavior towards security policies and procedures than Irish employees.

Consequently, three main findings were enlisted by the authors. First, organizations with more robust institutional controls have a higher degree of compliance with the ISP. Second, higher sociability organizations are less in line with the ISP. Finally, organizations that have more interaction between managers and employees seem to be more ISP compliant. A summary of the literature on national culture and ISPC is presented in Table 4.

Table 4. Studies on national culture and ISPC.

Authors	Research Method	Sample Size	Findings
[44]	Qualitative study analytical grounded theory approach adopted	19 semi-structured interviews from the US and Ireland	US employees have more adaptive behavior toward security policies and procedures than Irish employees.

4.1.2. Intrinsic/Extrinsic Motivations and Compliance

Motivation plays a vital role in the behaviors of employees. Various psychology researchers classify motivations into two significant classes: intrinsic motivations (motivation for own's sake) and extrinsic motivations (perceived motivation from the environment). A detailed study has been performed by [8] in the context of motivations. He examined the intrinsic and extrinsic motivation models for ISB on 602 employees from different organizations. He concluded that intrinsic motivations (perceived legitimacy, perceived value congruence) affect employees' ISB towards ISPC more significantly than extrinsic motivations (perceived deterrent certainty, perceived deterrent severity). Reference [36] presented a taxonomy of ISB for the betterment of information security management. Furthermore, researchers examined extrinsic motivation factors in detail and concluded that extrinsic motivation factors significantly affect employees' ISB. Similarly, [59] argued that deterrence is not as effective as internal motivation. They developed a framework to test internal and external motivations' effects on the ISB of employees. Their results showed that an external perceived locus of causality (sanctions and deterrence) has negligible effect on ISB compared to one's internal perceived locus of causality (own values, personal liking/disliking). The studies evaluate the intrinsic, extrinsic motivations enlisted in Table 5.

Table 5. Studies on intrinsic/extrinsic motivations and ISPC.

Authors	Research Method	Sample Size	Findings
[8]	A quantitative method for framework validation, SEM used for hypotheses testing	A total of 602 employees from different organizations participated	Intrinsic motivation model factors have better results than extrinsic motivation model factors on employees' behavior towards ISP compliance
[36]	Overview of behavior articles to develop a taxonomy of compliant information security behavior	Almost 35 studies reviewed information security behavior	Intrinsic and extrinsic factors reviewed; extrinsic factors reviewed in detail. Extrinsic factors have a significant effect on ISB, but intrinsic factors need more exploration
[59]	Quantitative research methodology adapted and PLS used for hypothesis testing	444 respondents participated	Effects of external PLOC (Perceived locus of causality) and Internal PLOC examined, internal PLOC find to be more significant than external

4.1.3. Protection Motivation Behaviors and Compliance

Employees with better-perceived protection motivations are likely to have higher compliance behaviors towards ISP. Protection motivation theory is used to assess protection motivation behaviors. It poses a better understanding of the severity of the threat (severity of a threatening event, vulnerability) and perceived coping capability (recommended preventive behavior, self-efficacy) that can enhance ISPC. Reference [60] clearly defined that fear appeal (an employees' degree of the perceived threat and expected harm from that threat), protection motivation (self-efficacy and response efficacy), and social influence have a powerful effect on employees' security behavior. Likewise [14] has briefly identified factors that influence ISB towards ISPC. The researcher proposed a research model based on the theory of planned behavior (TPB) following the protection motivation theory (PMT) and tested his model on 124 IS and security managers. It has been shown that self-efficacy, attitude toward compliance, subjective norms, response efficacy, and perceived vulnerability positively influence ISP behavioral compliance. Reference [61] introduces the past behavior (habit) concept first time in ISPC. They examined habit with PMT. This study's results have a significant effect on protection motivation, which increases the behavioral compliance of an employee towards ISP.

The insiders' behavior research was mainly examined with the help of PMT. Similarly, [37] have briefly outlined the taxonomy for protection motivated behaviors of insiders. They also discussed that behavioral information security is a dynamic field. Protection-motivated behaviors will change with time, and updates will be continuously required. Similarly, [24] identified the use of core and complete PMT elements for measuring protection motivation behaviors (PMB); they argued PMT is the most used theory in ISPC; however, no researcher used PMT with its complete elements. Fear and maladaptive rewards were the neglected elements that were never tested before. They have proposed a research framework based on complete PMT elements and tested it with two studies (longitudinal and cross-sectional). In brief, they concluded that full use of PMT (fear appeals and maladaptive rewards) has better results on security-related behaviors. Reference [32] conducted a meta-analysis on PMT and ISB; their results showed that PMT leads to a slightly better performance of involuntary security behaviors than mandatory security behaviors. Second, PMT will be a good predictor of ISB if a threat or coping method is specific. Third, PMT predicts ISB better for threats related to the individual, not to organizations. Reference [62] have used updated and enhanced fear appeal rhetoric with PMT and proved that the conventional fear appeal approach was not enough to distinguish between the threats to humans and information assets. They added sanctions to the previous fear appeal rhetoric and proved that enhanced rhetoric leads to better intentions to comply with ISPC.

Information security adaptation and its continuance is the reflection of perceived motivated behavior. Reference [54] identified the gap between initial security adaptation and continuance of protective security behavior. In this study, the PMT-based model proposed and tested with 253 end-users, it has been shown that changing or updating in security policy or procedures makes the continuance of security behavior difficult, although self-efficacy, perceived threat severity, and perceived threat susceptibility significantly affect employees' continue protective behaviors. Reference [63] examined psychological capital (hope, optimism, self-efficacy, resilience) with PMT constructs (threat appraisal and coping appraisal). This study has shown that psychological capital can play a vital role in developing employees' protective motivated behaviors. Reference [64] briefly outlined that existing information security behavior research addresses one threat and one behavior at a time while users perform multiple security behaviors to mitigate security threats. Their study examined three security threats (data loss, security-related performance degradation, identify theft) on 279 computer users and showed that users perform multiple security behaviors to deal with these threats. The study's results have been analyzed with multidimensional scaling analysis and have shown that response efficacy and response cost are the key factors that explain why people choose a specific security behavior. Reference [65] eval-

uated the factors influencing employees' intention of engaging in antimalware behaviors. A PMT-based research model was proposed with additional experience factors (psychological ownership, organizational citizenship, security responsibility). The research model tested 526 employees with three different antimalware security behaviors (i.e., scanning USB with antivirus, avoiding clicking on suspicious emails, installing appropriate software updates). This study determined that all PMT factors were positively significant to facilitate antimalware behaviors except response cost; moreover, additional factors showed unique variance in different security behaviors.

A study conducted by [66] examined IT employees' behavior towards information security. It has been argued in this study most of the InfoSec research focused on non-IT employees, whereas this study focused only on IT employees. The proposed research framework developed with PMT, DT (deterrence theory), and TRA (theory of reasoned action). This study provided exciting and unexpected results, and researchers proposed ten hypotheses; only three hypotheses were supported. Self-efficacy and perceived effect have positive effects on IT employees' intention to practice information security. Reference [45] examined moral intensity effects with organizational criticality on insiders' protection behaviors; researchers considered moral intensity a multidimensional construct. That was a scenario-based quantitative study performed upon 216 employees of a university. The researchers designed four scenarios; the first two scenarios for high criticality protection behaviors, and the other two involved low criticality protection behaviors. The study results showed that dimensions of moral intensity affect moral beliefs and vary with different organizational criticality among insiders. Reference [27] have presented a multi theory framework to assess higher education employees' behavior toward ISPC. Four significant theories (PMT, GDT, TPB, OT) constructs were used for compliance assessment. A total of 206 higher education employees responded correctly to this study. This study concluded that PMT (perceived vulnerability, response efficacy, and response cost) is the best predictor of ISPC in higher education. In contrast, punishments for peer pressures, sanctions, and top management supervision do not matter in this context. Likewise, [67] presented a framework based on eight behavioral theories constructs. They took nine influential variables and tested them with a survey of 433 employees. Their study concluded that among multiple ISB factors, self-efficacy and religion or self-morality are the best predictors of employees' ISPC. A summary of the PMB's selected literature is provided in Table 6.

Table 6. Studies on PMB's and ISPC.

Authors	Research Method	Sample Size	Findings
[60]	Mixed method research design structural equation modeling used for framework testing	275 usable responses from collected from a university	Fear appeal, response efficacy, self-efficacy, and social influence have significant effects on information security behavior
[14]	The quantitative research methodology adopted and SEM used for research model testing	124 business managers and professionals participated	Self-efficacy, attitude toward compliance, subjective norms, response efficacy, and perceived vulnerability positively influence ISP behavioral compliance intentions of employees
[61]	The hypothetical research design adopted (pre- and post-test), and SEM used for research model testing	210 participants responded correctly from a Finnish organization	Past behavior (habit) has a significant effect on protection motivation and employees' intentions to comply with ISP
[37]	A six steps Mixed (Qualitative and Quantitative) Methodology adopted to develop a taxonomy for protection motivation behaviors (PMB)	67 classes identified for the protection motivation behaviors of insiders	PMBs taxonomy will provide a nomenclature that will increase practitioners and academicians' understanding of IS security behaviors

Table 6. *Cont.*

Authors	Research Method	Sample Size	Findings
[24]	The mixed research methodology adopted, and STATA softeare was used for model fitness and hypotheses testing	A total of 452 business and psychology students participated	For measuring protection motivation behaviors, researchers must use core and full constructs of protection motivation theory (PMT)
[32]	Literature Review (Meta-Analysis)	A total of 30 research articles reviewed	PMT explains voluntary security behavior better than mandatory. PMT predicts better ISB if the threat and the coping process are specific, and PMT is a good predictor of ISB for individuals' threats, not the organizational threats
[62]	Mixed method approach used and PLS used for research model testing	559 insiders participated from the city government of Finland	Enhanced fear appeal with PMT has better results on ISPC
[54]	The longitudinal research design was adopted. PLS is used for data and model testing	253 valid responses were collected	Self-efficacy perceived threat severity, and perceived threat susceptibility significantly affect employees' continue protective behaviors
[63]	The quantitative research design adopted SEM used for model and hypothesis testing	377 usable responses from the public and private organizations	Psychological capital has positive effects on employees' protective motivated behaviors
[64]	Mixed method research with multidimensional scaling analysis	Seven expert interviews and 279 computer users participated	Users perform multiple security behaviors to deal with security threats. Response efficacy and response cost help users to choose security protection behaviors
[65]	The quantitative research methodology adopted regression is used for data and model testing	526 employees participated	Along with additional parameters, PMT s threat appraisal was less predictive than coping appraisal to detect employees' intent to engage in antimalware behaviors
[66]	Quantitative study design and SEM used for results analysis	70 responses IT personals collected from New Zealand	Perceived impact and self-efficacy have positive effects on intention to practice information security
[45]	Scenario-based quantitative study design. PLS used for model testing	261 participants from a university	Dimensions of moral intensity and organization criticality have significant effects on insiders' protection behaviors
[27]	Quantitative study. SEM used for model and hypothesis testing	206 correct responses were collected from the higher education sector	PMT is the best predictor of employees' behavior towards ISPC in the higher education sector
[67]	Quantitative research design	433 employees participated in this study	Self-efficacy and morality are the most influential factors of ISB.

4.1.4. Security Culture, Awareness Behaviors and Compliance

Organization management enhances security-aware behaviors of employees, which later guarantee good security culture. Reference [16] identifies four information security behavior modes (Not Knowing–Not Doing, Not Knowing–Doing, Knowing–Not Doing, Knowing–Doing) contributing to security culture. The researchers argued that employees' knowledge and skills significantly affect ISP compliance and develop a good security culture. Employees often consider that information security is the IT staff's responsibility, so they themselves are not part of IS security. For changing the views of employees, organizations must cultivate a good security culture, and top management should play its role.

Similarly, [49] emphasized a top management role to cultivate good security culture and behavior in organizations. These researchers presented a framework and tested it on 148 alumni of a public sector university. Their study findings showed that organizations' top management influence employees' perceived security culture and their beliefs towards ISPC. Reference [46] presented a framework based on security culture and organizational behavior constructs. The research highlighted the behavioral effects of security culture and organizational behavior (job satisfaction and perceived organizational support) towards ISPC. Their research findings showed that security culture and job satisfaction influence behavioral compliance towards ISP, whereas perceived organizational support has no significance on employees' behavior.

Reference [68] argued that different levels of knowledge about ISP influence behavioral compliance; they developed a framework to test their hypothesis and divided the participants into two groups—(1) high knowledge group (2) low knowledge group—with the help of interviews and questionnaire. Their results showed significant differences between both groups and inconsistency in the results due to different ISP knowledge levels. However, 80 percent of the respondents of both groups showed their intention to comply with ISP. Reference [47] examined the factors influencing conscious care information security behavior; security awareness and organizational security policy showed positive effects on the subjective norms and attitude towards employees' conscious care security behaviors. Threat appraisal and self-efficacy proved to be significant factors towards the formation of the conscious behaviors of employees. Furthermore, they discussed how the conscious care behavior of employees significantly reduces the risk of information security breaches.

Reference [17] focused on early conformance with updated ISP. They argued that early conformance with ISP is much beneficial for organizations than late conformance or nonconformance. Employees' intentions and attitudes were tested for determining early conformance with ISP; a TPB-based research model was developed and tested on 535 employees. The results showed that awareness has a positive effect on the attitude, and attitude shapes the early intentions to conform, which later on become early conformance behavior towards ISP. Reference [33] conducted a systematic literature review and identified competencies (knowledge and skills) related to ISP compliance; these researchers argued that employees must be competent enough to comply with ISP. In this review, the researchers reviewed a total of 32 articles and eight internationally published professional competence frameworks. Three significant dimensions (attitude, knowledge, skills) and 11 factors regarding ISP competency were identified. In this study, an ISP compliance competence model was presented and analyzed with professional competency frameworks. This study identified the gap between the literature and the professional frameworks. The findings revealed that most behavioral theories imply that compliance with ISP needs specific competencies, but professional frameworks lack the ability to present those competencies. In Table 7, a detailed analysis of the selected studies provided information about culture and security-aware behaviors' effects towards compliance.

4.1.5. Management Behaviors and Compliance

The information security of any organization depends on the management behaviors towards information security policy implementation. Reference [48] created a typology for ISB for security managers to understand different security behaviors. They argued that discipline and agility shape different security behaviors in an organization. Reference [69] analyzed the factors influencing computer security behaviors in organizations. They proposed a research model to evaluate computer security behaviors and concluded that organizational norms, moral obligation, and attitude toward computer security behavior have significant effects on employees' behavioral intentions. Reference [70] worked on health information systems. They developed a behavioral ISPC framework for health employees. Their result shows that leadership, management, and security awareness positively affect the ISB of health employees. It is believed that an employee's behavior

is effected by his social circle. Social pressures, norms, and activities have a significant influence on employees' behavior. Reference [71] stated that high working experience employees have more absorbing capacity regarding new tools and technology adaptation, which causes a reduction in risks related to information security. The results of the study also showed that management support and security awareness have significant effects on employees' information security compliant behavior.

Table 7. Studies on culture/security awareness behaviors and compliance.

Authors	Research Method	Sample Size	Findings
[16]	Qualitative study	47 semi-structured interviews conducted	Different modes of behavior affect information security culture differently in organizations
[49]	Quantitative study. SEM used for Model testing	148 responses collected from a public university	Top management can cultivate good security culture, and a security culture help shaping employees' behavior towards ISPC
[68]	Mix method research methodology adopted. SPSS is used for descriptive analysis, and PLS is used for data analysis.	513 responses were collected from 4 Finnish firms	Different levels of ISP knowledge influence information security behavioral compliance
[46]	A quantitative study, PLS used for hypothesis testing	127 correct response were collected from various organizations	Security culture and organizational behavior are the vital drivers of ISPC
[47]	Mixed methodology adapted. Data and model tested with SEM	212 IS experts and professionals participated from different Malaysian firms	Security awareness, organizational security policy, threat appraisal, and self-efficacy positively affect employees' information security-conscious care behaviors
[17]	The quantitative research methodology was adopted, and the model was tested with PLS.	535 usable responses collected from a university	Attitude and intention are significant predictors of actual early compliance behavior towards ISP
[33]	Systematic literature review	A total of 32 articles and eight professional frameworks were analyzed regarding users' competencies associated with ISP compliance	Professional frameworks fail to recommend competencies associated with ISP compliance

The effect of the status (hierarchal rank) of an employee on perceived behavioral control (self-efficacy and controllability) was explored by [72]. The study focused on investigating the effects of different status employees' perceived behavioral control over interactive security threats and controls, including explicitly tailgating (unauthorized access to a restricted area). The findings of the study clearly showed the effect of status on the perceived behavioral control of employees. Employees who have more control over their coworkers have positive perceived behavioral control effects on tailgating behaviors; on the other hand, low-status employees with less control over their coworkers adversely perceived behavioral control effects on tailgating behaviors. Reference [73] introduced the psychological contract factor in ISPC research. A psychological contract means an explicit (give and take) contract between an employee and his organization. They argued that if an employee feels that his organization is not fulfilling the psychological contract, the employee may reduce his contribution to the organization.

On the other hand, if an employee develops an over fulfillment behavior, then there is a good chance that he will put his extra efforts towards the organization. They created a research model consisting of security countermeasures (ISP and awareness) and rational choice theory (perceived cost and perceived benefits) with the perceived psychological

contract. The research model was tested upon two groups' managers and employees. Their results showed that psychological contract is an essential factor. It has significant effects on ISP compliant behavior; furthermore, the psychological contract has more significant effects on manager groups than employees.

The perception of corporate social responsibility (the way to manage companies' business process) on employees' ISP behavior was evaluated by [74]. These researchers examined RCT constructs' effects (cost of compliance, the benefit of compliance, and cost of noncompliance) and corporate social responsibility dimensions (moral, discretionary, relational) upon employees' ISB. This study concluded that only the moral dimension of corporate social responsibility has significance towards ISP compliance. There is no effect of the cost of compliance on the ISB of employees. Reference [75] provided a quantitative analysis of information security assurance behavior (intense password usage and regular data backups). This study's authors proposed that social learning factors and security monitoring significantly affect employees' security assurance behavior. It has been shown that monitoring has substantial effects on an increase in assurance behavior, whereas employees perceived inconvenience (behaviors difficult to adopt) for the employees has adverse effects on assurance behavior. Reference [76] identified employment status (permanent and temporary) as a critical behavioral factor influencing ISP compliance. This study evaluated differences in organizational commitment and perceived organizational support among permanent and temporary employees. The authors concluded that permanent employees have more positive behavior towards ISP compliance than temporary employees. Reference [77] briefly explained shadow IT security behavior (unauthorized software use and download), which significantly affects ISP compliance. The central theme of the study is based on the theory of individual and organizational inertia. These researchers examined the effects of individual and organizational inertia on shadow IT security behavior. The study shows that organizational inertia shaped individual cognitive inertia and cognitive inertia significantly affects individuals' shadow IT behavior. Reference [78] examined four predictors of ISPC among 237 university employees—their study proved that effective leadership from the management could enhance employees' trusting beliefs and value building. Furthermore, the study results predicted that good leadership could increase ISP awareness, which is a significant predictor of ISPC. Likewise, [22] examined the roles of supervisor guanxi and employees' organizational commitment. Their results proved that better support from subordinates and supervisors could enhance employees' organizational commitment, which weakens employees' perceived costs and perceived effectiveness towards compliance behavior. Moreover, supervisors' guanxi has a positive direct and indirect effect on the employees' compliance behaviors. Table 8 shows the detailed summary of management behaviors and compliance studies.

4.1.6. Social Behaviors and Compliance

Organizations mainly invest in technical solutions, whereas information security is a multidimensional problem (i.e., technical and behavioral). Multiple researchers provided technical solutions for employees' social factors, such as [79], who developed a fake online repository generation engine for cyber deception. The concept of deception is used for solving behavioral information security problems using a technical method. Furthermore, [80] presented a multimedia probabilistic logic graphs model for improving behavioral information security in organizations. Multiple researchers tried to solve the ISPC problem with technical controls, but technical solutions are not enough to solve behavioral information security problems. There must be administrative controls (i.e., security awareness via social techniques, top management support for enhancing social behaviors) to enhance ISP compliance [81].

Table 8. Studies on management behaviors and compliance.

Authors	Research Method	Sample Size	Findings
[48]	The mixed research methodology adopted, case study, and qualitative analysis	Seven semi-structured interviews conducted with crucial personals (managers and operational staff)	An organization's existing culture and management discipline and agility shape different types of information security behaviors
[69]	Quantitative research methodology and structural equation modeling used	162 employees participated in multiple Korean organizations.	Organizational norms, moral obligations, and attitude toward the computer and security behavior have significant effects on employees' behavioral intentions
[70]	The quantitative research methodology was adopted. SPSS used for data analysis	42 employees participated from the health sector	Leadership, management, user's awareness, and training significantly affect information security compliant behavior
[71]	The quantitative research methodology was used. SEM used for hypotheses testing.	454 health personals participated	Management and security awareness have significant effects on ISB. Furthermore, employee experience is a crucial factor and has much significance towards ISB of Health employees
[72]	Pre- and post-tested quantitative research design. Covariant based SEM used for research model testing	317 correct responses from the department of defense USA	Employees' status (hierarchal rank) significantly affects the perceived behavioral control over tailgating behaviors.
[73]	Pre and post-test quantitative methodology used. PLS is used for data and research model analysis	213 total responses were collected from two groups (supervisors and supervisee)	The psychological contract is an essential factor, and it affects ISP compliance intention significantly
[74]	The quantitative research approach adopted and PLS used for data and hypothesis analysis	162 employees participated from South Korea	Moral corporate social responsibility and RCT factors have significant effects on ISP compliance behavior
[75]	The quantitative research methodology was adopted. SEM used for model testing	525 employees from the telecommunication sector	Information security monitoring and social learning factors significantly affect employees' security assurance behavior
[76]	In a quantitative study, PLS used for results analysis	619 usable responses collected	Employment status affects ISP compliance behavior of employees
[77]	Quantitative research methodology. PLS used for hypothesis and model testing	A final sample of 404 respondents	Organizational inertia and individual inertia have significant effects on shadow IT security behavior
[78]	Quantitative study	237 employees from a university participated	Leadership, belief, values, and ISP awareness positively associated with ISPC
[22]	Empirical quantitative study	235 government employees from China participated	Supervisors' support enhances organizational commitment, which has positive effects on employees' compliance behaviors

Employees seek help and guidance from their social circle, and they often adopt behaviors from their peers or coworkers. Reference [22] tested their ISB framework on 400 military personnel in Malaysia. Their study showed that employee socialization and individual factors (computer self-efficacy, personal innovativeness, IS perception) have positive effects on ISB towards ISPC. Similarly, [82] demonstrated the significance of the social bonding and social cognition factors on ISP behavior. He developed a research model with social bond theory, social cognitive theory, and planned behavior theory. His

results summed up social, cognitive, and psychological factors have significant effects on employees' ISB. Reference [83] conducted a qualitative study on different US (United States) sectors to detect the insider (employees') behavior towards ISPC. A total of 33 (11 security professionals, 22 insiders) PMT-based interviews were conducted. Based on the interviews' observations, they concluded that insiders adopt behaviors from social influences; they rely on learning security-based knowledge and self-efficacy improvements. SETA (Security Education and Training) programs should be more effective and redesigned accordingly. Rewards (financial and verbal) were found to have low influence on insiders' motivation to comply with ISP.

Information security controls (i.e., social and formal) were examined by [41] with two types of IS behaviors (extrarole and irole). Social controls were developed from social control theory, whereas formal controls consisted of rewards, evaluation, and specification. This study proved that formal control with social control has significant positive effects on security behaviors, improving ISP effectiveness; on the contrary, this was the first study that has examined controls with extrarole behaviors. Reference [84] established that ISP-related personal norms are essential predictors of information security compliant behavior. The study combined the principle of ethical climate constructs with personal norms (subjective, injective, and descriptive) to measure the ISB. In short, the results of the study have shown that the principle ethical climate affects the social norms of employees and that social norms effect personal norms (i.e., subjective, injective and descriptive) moreover ISP related awareness and ISP related ascription of personal responsibility was also having significant effects on Information security compliant behavior.

Similarly, [85] analyzed involvement theory within the social bond theory. They have developed a framework with social bond theory (involvement, commitment, attachment, personal norms) and involvement theory (knowledge sharing, collaboration, intervention, and experience) and tested their framework on four different Malaysian organizations. The study determines that information security knowledge sharing and collaboration can increase awareness among employees. Experience or mastery of safeguarding information security assets is another significant factor that influences the attitudes of employees. It has been shown that all social bond factors except attachment have significant effects on information security compliance behavior.

A research framework for reducing insider threats has been proposed by [86]. The framework was based on Situational Crime Prevention Theory (SCPT) and Social Bond Theory (SBT). The researchers proposed elements of SCPT (increase effort and risk to commit a crime, reduce rewards and provocations and remove excuses) and SBT (commitment, attachment, involvement with ISP and personal norms) to help positively to promote the negative attitude towards security misbehavior and intention. This study's results have clearly shown that the SCPT and SBT constructs significantly promote negative attitude towards misbehavior, whereas reducing provocation and attachment did not significantly reduce insiders' misbehavior and intention. Reference [87] highlighted that person–organization fits (i.e., interaction between organization and employee) effect extra role behaviors. These researchers argued that person–organization fits (perceived demand–ability, need–supply, and value) increase employees' commitment to security and decrease apathy effects. This study proved that employees with increased commitment and low apathy are more likely to engage in extra role security behaviors. For the first time, [88] examined the moderating role of social influence on individual and organizational level factors towards ISPC. The study results proved that social factors (i.e., rules-oriented ethical climate and susceptibility) could weaken the effect of the command and control and self-regulatory approaches of ISPC on an individual and organizational level. An empirical study [3] examined organizational governance and social bond factors' effects on ISPC. The study results proved that an organization with good organizational governance could enhance social bonding among employees, improving the ISPC in the organizational context. Social behaviors and compliance studies are thoroughly summarized in Table 9.

Table 9. Studies on social behaviors and compliance.

Authors	Research Method	Sample Size	Findings
[89]	Quantitative research methodology adapted, and SPSS used for instrument validation and regression analysis	400 participants from the Malaysian army	Social and individual factors have positive effects on information security compliant behavior
[82]	The quantitative research methodology used, SEM used for hypotheses testing and data analysis.	68 employees of different firms responded	Social, cognitive, and psychological factors influence information security behavior towards ISP
[83]	The qualitative research methodology adopted	A total of 33 semi-structured interviews (22 from insiders and 11 from security professionals) conducted from different sectors of the US	Insiders adopt behaviors from social influence; they depend on knowledge from one another
[41]	Quantitative research methodology with SEM testing.	217 employees and 78 IS managers participated from 78 different organizations in Taiwan	Extrarole behaviors and in role behaviors have significant effects on ISP effectiveness
[84]	The quantitative research methodology adopted, and PLS is used for data testing	201 employees participated	ISP-related personal norms have positive effects on information security compliance behavior
[85]	Quantitative method used for research. SEM used for data and hypothesis testing	462 correct responses were collected from four different firms in Malaysia	Social bonding with an extending view of involvement has positive effects on ISPC behavior
[86]	The mixed-method research methodology was adopted. SEM used for model and data testing	518 correct responses were collected	Situational Crime Prevention Theory (SCPT) and Social Bond Theory (SBT) components significantly affect insiders' (employee) attitude towards misbehavior except for attachment and reducing provocations
[87]	Quantitative research menology adopted. PLS used for result analysis	253 responses collected from organizations in China	PO fit has positive effects on employees' extrarole security behavior and adverse effects on apathy
[88]	Quantitative study design	122 females and 124 males participated	Rules-oriented ethical climate and susceptibility weaken the effect of regulatory factors towards ISPC
[3]	Mixed method research design	254 Malaysian employees participated	Good organizational governance can enhance employees' social bonding, which later improves ISPC

4.1.7. Actual Behavior and Compliance

Most ISPC studies evaluated the employees' intentions, but intention alone is not enough to measure one's behavior. Some of the studies argued that intention is the strongest predictor of actual compliance. Few studies evaluate employees' actual behaviors. Reference [15] presented a multitheoretical framework to measure employees' actual compliance with ISP. These researchers used the TRA, PMT, and Deterrence theory constructs to measure actual compliance behavior towards ISP. This study's results suggested PMT constructs (threat appraisal self-efficacy response efficacy) and visibility positively affect the intention to comply with ISP. In contrast, intention and deterrence constructs have significant predictors of actual compliant behavior. Reference [90] explained and illustrated intended behavior and actual behavior; the researcher described a gap between intended behavior and actual behavior; moreover, he examined the factors influencing intended behavior towards actual behavior.

According to a literature review done by [35], protection motivation and sanctions have significant effects on attitude, and attitude determines behavioral intent; moreover, perceived behavioral control and subjective norms also significantly affect behavioral intent. These researchers indicated that behavioral intent carves the actual behavior of an individual. Reference [91] also analyzed the TPB predictors with four types of dysfunctional security behaviors (a naive mistake, dangerous thinking, harmful misuse, and intentional destruction); it has been shown that the TPB elements have different effects and the intentions of employees vary among multiple dysfunctional security behaviors, and intention is the strongest predictor of actual behavior. Reference [92] discussed the fact that intention is not the only predictor of actual behavior, and not all intentions become actions. Their result shows that not all misuse behaviors are intended; sometimes, it is an unreasoned action.

In the same way, they have argued that security managers are more interested in actual behaviors than intention. Reference [93] presented a TPB, GDT (i.e., sanction severity, sanction certainty), and SCPT based framework to mitigate insiders' information security misbehavior. This framework was tested upon a total of 444 employees from different organizations. This study concluded that all GDT and SCPT significantly affect employees' negative attitudes towards misbehavior except reducing provocations and remove excuses; furthermore, all of TPBs constructs have significant effects on employees' actual ISB. Table 10 summarizes the actual compliance studies.

Table 10. Studies on actual compliance behaviors.

Authors	Research Method	Sample Size	Findings
[15]	Quantitative study. SPSS and Amos were used for model and data testing.	917 usable responses collected	Deterrence and intention are the best predictors of actual compliance behavior towards ISP
[90]	The quantitative methodology used and research model tested with partial least squares	Randomly selected persons from different firms having more than 500 employees—exact number of participants not mentioned	The difference between intended information security behavior and actual security behavior is addressed in this study. Intended behavior does have a significant effect on actual behavior
[35]	Literature review	A composite theoretical information security behavioral compliance model developed with the help of previous studies	Attitude, perceived behavioral control, organizational commitment, and subjective norms have significant effects on behavioral intent
[91]	Quantitative research methodologyused. SEM used for model and hypotheses testing	387 usable responses collected from SMEs in Malaysia	Intentions of employees depend upon theory of planned behavior (TPB) predictors and dysfunctional IS behaviors
[92]	The quantitative research methodology adopted, and PLS is used for hypothesis testing	208 computer users participated via a web-based survey	The intention is not the only predictor of actual behavior
[93]	Quantitative study design SEM used for results analysis	444 correct responses considered	SCPT and GDT have significant effects on the insider's negative attitude towards misbehavior

4.2. Analysis of NonCompliance Behaviors

In line with RQ2 of this SLR, the current section exhibits the behavioral factors concluded in studies as a significant determinant of influencing information security policy noncompliance. This section evaluated studies related to factors that cause information security policy noncompliance. This section analyzed the studies' results related to neutralization, security-related stress, security-related value conflicts, and deterrence strategies effects that can cause employees' noncompliance with information security policies.

4.2.1. Neutralization, SRS and Noncompliance

Employees sometimes neutralize the values which prohibit them from violating ISP, while security-related stress often causes deliberate misbehavior. Reference [94] analyzed neutralization with deterrence to find out the intention to violate ISP. These researchers discussed neutralization and sanctions in detail. The data have been collected from three Finnish firms and framework tested with 1449 employees. The study's results provided vital evidence that neutralization is the significant predictor of ISP violation, whereas formal and informal sanctions and shame have no effects on ISP violation intention. Reference [95] designed a framework using neutralization techniques, PMT, TPB, and TRA. The neutralization theory suggests that an individual justifies his/her violation of the rules in seven ways. All of the seven techniques were considered significant towards ISPC; moreover, all of the constructs were significant, but self-efficacy was not significant in this study. Reference [20] examined the concept of SRS (i.e., security-related stress) and concluded that complex security-related requirements lead to deliberate ISP violating behavior via moral disengagement.

Moreover, they argued that workplace-related factors also affect security behavior. In conclusion, they suggested security-related requirements should not be a burden to the employees; all requirements should be easy to understand, whether ISP or SETA programs. Reference [52] developed a research model for factors evaluating noncompliance with ISP. The research model has two significant parts: organizational security efforts (security education, security systems, security visibility) and individual noncompliance causes (i.e., noncompliance behaviors of peers, work impediment, and security system anxiety). The study results concluded that work impediment, system anxiety, and noncompliance behaviors of peers significantly affect an individual's noncompliance intention with ISP.

Organizational injustice affects employees' computer abusive behaviors with moderating effects of neutralization and deterrence, as evaluated by [96]. Distributive organizational injustice (i.e., injustice in employees' rewards) and procedural organizational injustice (injustice in organizational procedures) were tested thoroughly with 968 employees. In brief, the study proved that procedural injustice causes employees to engage in abusive behaviors; in simple words, employees become more upset when they perceive that a procedure is unfair than when they perceive an injustice in rewards and compensations. Moreover, the study concluded that employees rationalize their abusive actions with neutralization techniques (i.e., denial of the victim, metaphor of the ledger). In contrast, perceived sanction certainty significantly influences employees' abusive behaviors towards ISP. Reference [97] derived a unified model for ISPC from eleven frequently used theories in the ISPC literature. They provided a multilevel study design to derive a unified model and test it with three ISP violation scenarios. Their results explained that neutralization is a significant predictor of employees' reactance towards intention to violate ISP, although, deterrence, rewards, and social factors were not found to be significant towards ISPC.

Reference [12] explored the daily basis SRS effects on ISP compliance in an advanced manner. The study proposed that SRS causes frustration and fatigue elements in employees. Employees cope with frustration and fatigue with neutralization (justification of negative behavior). Due to the requirement of daily basis behavior evaluation, the researchers adopted the experience sampling method (ESM) (i.e., within individual measures) survey. Results have been shown that SRS has positive effects on emotional reactions (i.e., frustration and fatigue), and emotional reactions, often coupled with the neutralization, which has adverse effects on employees' behavioral intent to comply with ISP. Likewise, [98] measured technostress among various IT professionals and found that all technostress creators (i.e., overload, complexity, invasion, uncertainty, and insecurity) were significant technostress predictors in organizations. Furthermore, their results indicated that technostress is positively associated with perceived strain and intention to violate ISPs. Reference [11] analyzed the daily ISPC behavior of employees. These researchers proposed a research model based on cognitive beliefs and moral considerations. This research was based on the experience sampling method to evaluate employees' attitudes daily. The

research concluded that work impediments (i.e., daily work stress), positive affect, negative affect, and computer monitoring influence compliance attitude towards compliance behavior daily.

An ethical work climate, neutralization, and beliefs (i.e., about the perceived cost of compliance, the perceived cost of noncompliance, and the benefits of compliance) interact towards employees' noncompliance behavior with ISP, as demonstrated in detail by [51]. These researchers presented a framework based on social information processing theory. The work climate consists of three significant bases of moral judgment: egoism (i.e., self-centeredness), benevolent (i.e., maximize other's interests), and principled climates (i.e., binding with laws and policies). The study concluded that work climates influence neutralization and beliefs differentially. Furthermore, the neutralization of noncompliance and the perceived cost of compliance significantly affect ISP employees' noncompliance behavior.

Furthermore, moral beliefs, coworker compliance, and self-efficacy also influence daily compliance behavior positively. Reference [99] evaluated cross-cultural factors with deterrence theory. This study examined the influence of culture, deterrence, shame, neutralization, and moral beliefs on ISP compliance. Employees of a large multinational company who were based in forty-eight countries' participated in this study. The results demonstrated that cross-cultural factors were not significant towards deterrence.

In contrast, shame, neutralization, and moral beliefs significantly affect ISP noncompliance across all global cultures. Similarly, [100] presented a framework based on punishments, rewards, and situation-specific ethical orientation. They tested their model with six neutralization scenarios. The results of the study proved that gender has no effects on noncompliance intent with ISP, whereas noncompliance with ISPs' vary from person to person and with different situations. The study further stated that rewards and punishments are dependent on the internal and external situation-specific ethical orientation (gender and neutralization techniques). Table 11 shows a complete demonstration of the neutralization and noncompliance studies.

Table 11. Studies on SRS, neutralization, and noncompliance.

Authors	Research Method	Sample Size	Findings
[94]	The quantitative research methodology was adopted. SEM is used for model testing.	1449 employees participated	Neutralization is a significant predictor of employees' intention to violate ISP.
[95]	The quantitative methodology was adopted. SPSS used for data analysis; PLS used for hypothesis testing	179 employees from 10 different industries participated	Neutralization techniques should be considered when designing an ISPC model. Attitude and response efficacy are also helpful. Self-efficacy was not found to be effective.
[20]	Quantitative method used. SEM is used for results and analysis	539 usable responses of the computer using professionals collected from different organization	The stress of security requirements leads to moral disengagement, which increases violating ISB.
[52]	The quantitative research methodology was adopted. SEM is used for hypothesis and model testing	415 usable responses were collected from manufacturing and services firms	Noncompliance behaviors of peers, work impediments, and security system anxiety is the causes of noncompliance with ISP.
[96]	A scenario-based quantitative study. SPSS and PROC MIXED used for hypothesis and data testing	968 complete responses collected	Procedural, organizational injustice causes computer abuse behavior; sanction certainty reduces injustice effect and intention to abuse ISP.
[97]	Mixed method research design	924 Finnish employees participated.	Neutralization was found to be a significant predictor of reactance towards ISPC.

Table 11. *Cont.*

Authors	Research Method	Sample Size	Findings
[12]	Experience sampling method adopted. hierarchical linear modeling used for results analysis	138 accurate responses collected	Stress-related security requirements cause fatigue and frustration, which later on relate to neutralization. Moreover, neutralization has a negative behavioral effect on ISP compliance.
[11]	ESM research design adopted. HLM is used for results and analysis.	77 recruited participants filled surveys correctly	Work impediment, positive affect, negative affect, and computer monitoring influence compliance behavior's daily compliance attitude.
[98]	Quantitative study design	356 employees from the IT industry participated	Technostress is positively associated (direct and indirect) with perceived strain and intention to violate ISP
[51]	Quantitative research. PLS used for Hypothesis testing	393 employees from different organizations	Neutralization and beliefs have significant effects on employees' noncompliance.
[99]	Scenario-based quantitative study design. PLS used for result analysis.	615 employees from 48 countries.	National culture does not affect deterrence. Shame, neutralization, and moral beliefs have significant effects on ISP noncompliance intention of employees from all cultures.
[101]	Quantitative study design	120 female and 101 males participated in this study	Gender has no effects on ISP noncompliance; however, rewards and punishments are dependent upon the situation-specific ethical orientation

4.2.2. Value Conflicts and Noncompliance

Employees develop various value conflicts towards ISP; they often violate ISP because of their preference-based conflicts. Reference [39] argued that employees' noncompliant behavior is not only because of risk perceptions but also from task completion impediments. Employees often engage in noncompliant security behaviors because of task completion deadlines; they often indulge in a value conflict (i.e., task completion is above ISP compliance). It has been shown in this study that self-justification (to justify the noncompliant act to oneself) and sunk-cost (i.e., lack of loss acceptance) are the main influential factors for engaging in noncompliant behavior towards ISP. Reference [42] emphasized the value of information; these researchers conducted a qualitative study on seven focus groups from Brunei's government. A total of 55 semi structured interviews were conducted with IT managers and professionals and a value-driven information security compliance theory was developed. This study suggests that users' perceptions about the value of information (i.e., how vital the information is) determine their compliance behavior with ISP. Furthermore, the theory of value-driven proposals based on a qualitative study, which still needs to be tested with quantitative studies, has been discussed.

An empirical study presented by [40] has examined ISP noncompliance behavior with PMT and IT vision conflict. This study focused on measuring IT vision conflict mediation effects on PMT constructs and attitude towards ISP noncompliance. The authors argued that users' perceptions of IT and ISP were such that they believed that IT is much different to the rest of the organization, which in turn causes a conflict called IT vision conflict. Hence, this study concluded that IT vision conflict influences only perceived severity, not all PMT constructs; furthermore, it has been shown that PMT constructs have significant effects on noncompliance behaviors towards ISP. Reference [101] discussed the reasons for employees' less effortful behaviors towards information security tasks. In this study, the researchers elaborated on two coping mechanisms—procrastination (i.e., saving present time and pushing security tasks for the future) and psychology detachment

(i.e., denial of the importance of security tasks)—which employees use to avoid security task performance. Employees think the security risks are external factors (i.e., perceived externalities), and their business tasks are more important than the security tasks (triage). This study concluded that employees consider security tasks to be external and less valued and avoid procrastination and psychology detachment. Reference [102] described consequence-delayed information security violation (CDISV). It has been discussed in detail that most employees indulge in risky ISB because of their late results. Long-term orientation towards ISP is considered as the main factor to reduce CDISV intention.

Employees having high organizational value identification are more likely to develop long-term orientation (LTO) behavior. LTO has three main dimensions: futurity, perseverance, and continuity. LTO, with the addition of stewardship theory and need theory constructs, was tested to determine LTO's effects on CDISV intention. It has been shown that the degree of LTO negatively affects CDISV intention. Table 12 shows author names, methodologies, and observations from the literature related to value conflicts and noncompliance.

Table 12. Studies on value conflicts and noncompliance.

Authors	Research Method	Sample Size	Findings
[39]	Pre and post-test quantitative research methodology. SEM used for results and analysis	500 employees participated from different organizations	Task completion impediments significantly influence employees' noncompliance behavior towards ISP.
[42]	Qualitative study design and results analysis conducted with NVivo 11.	A total of 55 semi-structured interviews conducted	The value of information is a determinant of users' compliant behavior.
[40]	The quantitative research methodology used and PLS used for results and analysis	275 correct responses considered	IT vision conflict influence perceived severity and attitude towards ISP noncompliance behavior.
[101]	Quantitative research methodology. PLS used for hypothesis testing	223 usable responses collected	Perceived externalities and triage are the leading causes for less effortful behavior of employees towards information security.
[102]	Pre and post-test quantitative methodology adopted. PLS used for hypothesis testing.	170 usable responses from a global firm	Long-term orientation ISB discourages consequence-delayed information security violation intention.

4.2.3. Deterrence and Noncompliance

When considering ISPC research using deterrence techniques from many decades, deterrence proved to be a significant factor in enforcing ISP compliance and deterring noncompliance behaviors. Reference [13] provided a literature review to obtain insights into the inconsistent results of deterrence theory in IS research. A total of 60 research articles that used deterrence theory from IS and other disciplines were reviewed. These researchers identified methodological and substantive issues with deterrence theory. They suggested contingency variables (i.e., self-control, computer self-efficacy, moral beliefs, virtual status, and employee position) to improve the deterrence results. The researchers argued that when using the deterrence approach towards ISB, one must consider these issues (methodological substantive) and contingency variables to obtain better results. Reference [103] explored the factors causing the ISP violating behaviors of employees in organizations; they argued that formal and informal controls can mitigate the violation behaviors: however, their findings suggest that social bonding, social pressures, and proper controls (i.e., perceived severity and perceived certainty) have significant effects on employee violation behavior.

A safe security behavior evaluation was performed by [104]. They presented a framework to determine safe information security behavior. The study results proved that if an employee knows the harmful effects of his actions, the severity of the threat, the fear of

getting caught, and the severity of punishment, he/she will have safe behavior towards information security. Moreover, satisfaction with colleagues also has a positive effect on an employees' safe information security behavior. Reference [105] introduced the concept of personality traits in behavioral information security. They tested two personality traits (i.e., stability and plasticity) with protection motivation and general deterrence elements for the first time. The stability meta-trait consists of emotional stability, agreeableness, and conscientiousness, whereas the plasticity meta-trait includes extraversion and dominant openness. The study concluded that employees with dominant stability traits are less likely to violate the ISP, whereas employees with plasticity traits violate ISP behavior more. Reference [38] examined the effects of the threat of sanctions on attitudes towards information security behavior. They have argued that rational use of section threats develops the attitude of employees. Moreover, attitude developed by the threat of sanctions is also biased by the previous punishment experience of employees, and that attitude affects the behavioral intention to comply with ISP.

Behavioral resistance towards ISP was highlighted by [23]. The authors argued that punishment or sanctions positively affect employees' descriptive and moral norms, which later decrease resistance behavior towards ISP compliance. Deterrence (punishment severity, the certainty of detection) and the norms-based research model were tested on 139 employees from ten different organizations. The study concluded that deterrence has significant effects on norms, which substantially influences ISP resistance behavior. Reference [34] has performed a meta-analysis on deterrence theory. The meta-analysis's primary purpose was to identify the overall deterrence effects on policy compliance, cultural effects on deterrence, and the effects of the methodological choices of behavior measurement on deterrence. A total of 35 studies were analyzed from 2003 to 2018 based on the correlation between deterrence theory constructs and ISP compliance behavior. The meta-analysis concluded that all deterrence theory constructs have significant effects on compliance behaviors except sanction severity.

Furthermore, sanction severity has a better correlation with noncompliance (i.e., malicious behavior), and sanction certainty correlates with positive behavior. Second, Deterrence effects vary with different organizational cultures. Third, the variance in the findings of the deterrence effects in various studies is not because of the methodological choices of behavior measurement (hypothetical and actual or generic and specific). Reference [106] introduced the concept of deterrability with a group-based study. They examined ISP awareness in groups of employees (i.e., inclined and declined). Their results confirmed that ISP awareness influenced employees' personal sanctions, whereas ISP awareness showed a partially stronger association towards declined employees' social and formal sanctions.

Moreover, they found that employees who are inclined towards ISPs are nondeterrable, and employees with declined behavior towards ISPs are deterrable. Similarly, [107] examined the deterrence effects on employees' intentions towards organizational ISPs. They proved that if an employee knows that there will be a sanction or punishment for his volitional intent, employees are more likely to comply with organizational ISPs. Their results suggested that sanctions severity, sanctions celerity, and certainty positively help reduce ISP violations in an organization. Table 13 illustrates the research methods, sample sizes, and main findings of the studies evaluating deterrence and noncompliance.

Table 13. Studies on deterrence and noncompliance.

Authors	Research Method	Sample Size	Findings
[13]	Literature review	60 articles reviewed on deterrence theory	Methodological and additional substantive issues are the reason for the inconsistent results of deterrence theory
[104]	Pre and post-test quantitative research methodology used for instrument validation, while PLS used for hypotheses and data analysis	A total data of 185 employees tested	Deterrence, social bonds, and social pressures play a vital role in preventing ISSP violation behaviors

Table 13. *Cont.*

Authors	Research Method	Sample Size	Findings
[105]	The quantitative research methodology adopted	112 correct responses collected	Susceptibility of the threat, the severity of the threat, certainty of detection, punishment severity and satisfaction have positive effects on secure ISB
[106]	The mixed-method research methodology used, and PLS is used for data and hypothesis testing	317 correct responses were collected	Different personality traits have significant effects on ISP violating behavior
[38]	The quantitative research methodology was adopted. Covariant-based SEM used for research model testing.	239 employees participated from the US department of defense	Rational use of sanctions creates attitude-dependent ISB. Attitude developed by sanction threats biased by previous punishment experience
[23]	Quantitative research design. PLS used for model testing	139 employees from 10 different organizations	Deterrence factors shape employees' norms, which influence behavioral resistance towards ISP compliance
[34]	A meta-analysis (literature review)	A total of 35 studies analyzed	(1) Deterrence theory (except sanction celerity) affects ISP compliance behavior (2) deterrence effects vary with different cultures
[107]	Quantitative research method	311 public sector employees participated	Information security awareness positively influences inclined employees personally and declined employees' formal and social sanctions
[108]	Scenario-based quantitative study	320 Chinese employees participated	Sanction severity, celerity, and certainty can reduce ISP violations

5. Discussion

The current systematic literature review has highlighted the information security behavior, its factors, and its theoretical implications towards information security policy compliance. The review focused on determining the behavior transformation from non-compliance behavior to compliance behavior presented in Figure 5. The transformation process has never been highlighted in the ISPC literature. For this purpose, the researchers reviewed the literature from 2010 to 2020 in two dimensions: (1) studies measuring compliance behavior; (2) studies measuring noncompliance behavior. The literature was reviewed and categorized according to the dimension of the studies. Seven categories were identified as factors influencing compliance behaviors. Three categories were highlighted for the factors influencing noncompliance given in Appendix A Tables A1, A2 and A5. Figure 5 demonstrates the activities and events extracted from a detailed literature review of ISB with ISPC. The process model has two lanes: (1) employees' noncompliance and (2) employees' noncompliance to compliance. The combination and transformation of activities have been discussed in detail in the following paragraphs.

RQ1: What are the behavioral factors concluded in studies as a significant determinant of information security policy compliance?

As seen in Section 4.1 of the Results section, there are seven major categories of significant behavioral factors of compliance behavior that have been classified from the last decade of the literature. Appendix A Table A5 lists all of the significant determinants of compliance behavior. The literature review results indicated that national culture has a variety of effects on employee enforcement behavior. Multiple studies have shown that national culture can affect ISPC in organizations [43,99]. Due to the studies' related concepts, we only included one study [44] on national culture, which significantly demonstrated that national culture is a powerful determinant of compliance behavior.

Intrinsic/extrinsic motivations were established as the second influencing factor in the enforcement behavior in the literature. Motivation is an essential element in human behavior. The ISPC literature discusses a variety of motivations as influential factors in improving compliance behavior. In total, 18 studies (i.e., motivation) were taken from the previous

behavioral security literature for this SLR. Three of them were from intrinsic/extrinsic motivations and 15 from protection motivation. Intrinsic motivations are self-motivation (the act of doing something without earning any rewards). All studies have shown that this is the most effective form of motivation. If organizations' management effectively improves their workers' intrinsic motivations, they would be less likely to breach any organizational policy [8,59]. Extrinsic motivation is described as the act of doing something for the sake of obtaining external rewards. Extrinsic incentives have been shown in research to increase ISPC and significantly impact compliance behavior [19,36]. Protection motivation, on the other hand, is characterized as the motivation to protect oneself. Protection motivation has a long history in ISPC literature, and it has been described as one of the most effective means of motivation to protect organizational assets [61]. According to the literature, organizations use some strategies to strengthen their employees' protection motivation behaviors, such as deterrence, punishments, or fines [18,45].

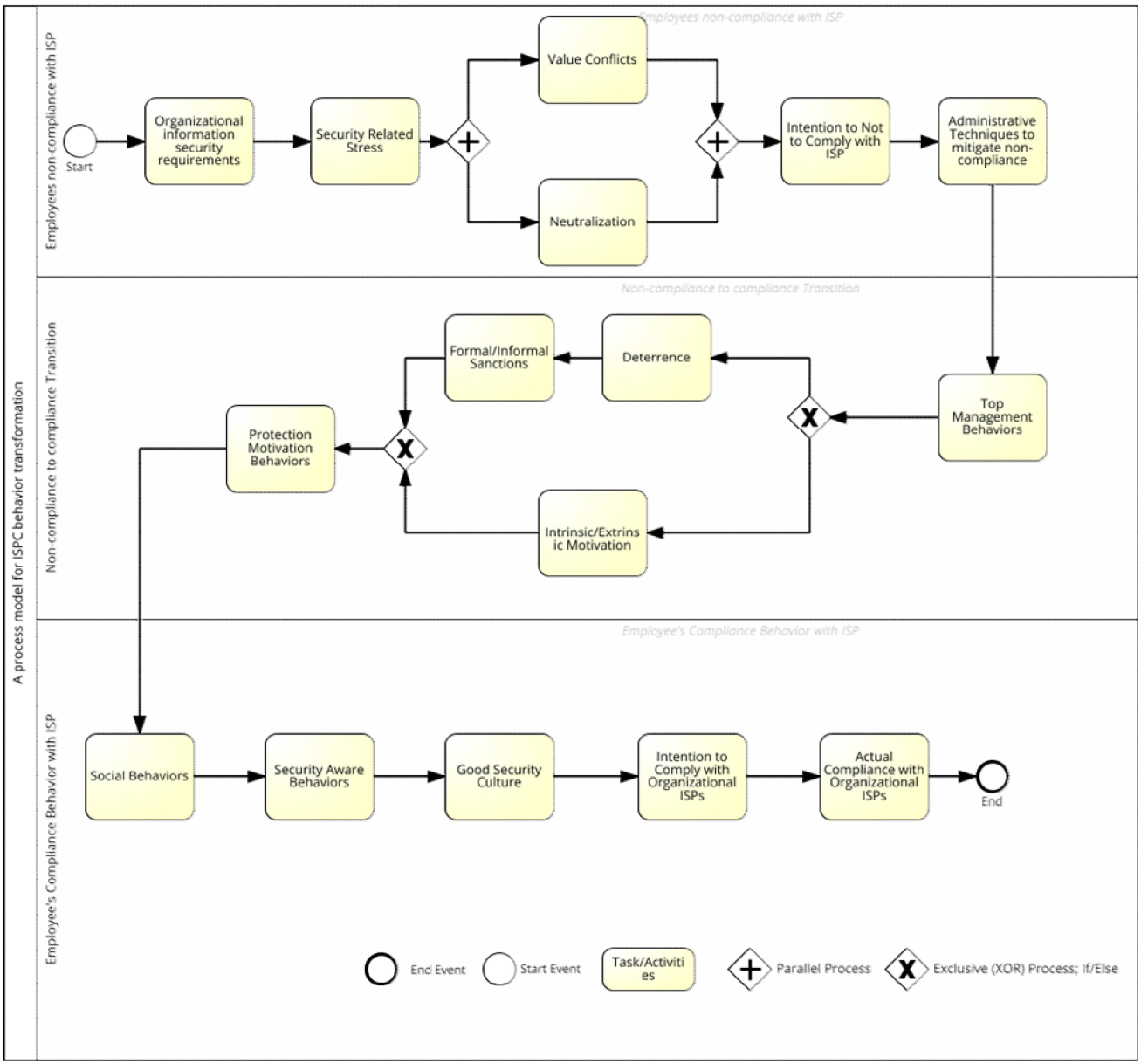

Figure 5. Behavior transformation from noncompliance to compliance with ISP.

Information security culture and awareness were also found to be influential factors in ISPC. According to a literature review, information security culture and awareness are directly proportional [109]. Information security awareness enhances an organization's information security culture, and a developed security culture improves employees' information security awareness [16,47]. Furthermore, current SLR indicated that information security culture and knowledge are solely based on management behaviors. Efficient management behaviors towards ISPC are regarded as crucial factors in enhancing compliance behaviors [77,109]. Similarly, ten studies conclude that social behaviors are also crucial for improving compliance behaviors. Several studies have shown that top management of companies is trying to improve ISPC by enhancing their employees' social behaviors [3,4].

RQ2: What are the behavioral factors concluded in studies as a significant determinant of information security policy noncompliance?

Security-related stress/neutralization, value conflicts, and deterrence are the three main categories of factors driving noncompliance. According to a literature review, workers often consider ISPs as difficult to follow, which later becomes a type of stress known as security-related stress. Employees neglect the organization's ISPs in order to avoid tension. According to several studies, employees regarded ISPs as external and stressful to obey [11,46]. Employees unwittingly formed noncomplaining behavior and used those tactics to neutralize their wrongdoing [12]. These tactics are based on the theory of neutralization. Five neutralization methods were initially included in the theory. The first is a denial of liability, in which the perpetrator says he or she is not liable for the breach [50,110]. The second is the denial of damage, in which they argue that what they did was the best way to mitigate harm to the organization. The third is that the perpetrator claims close ties to the organization. They argue that what they did was wrong, but their goal was to protect and help the organization. The fourth neutralization is condemnation of those who oppose them. It means that perpetrators justify their misconduct by condemning anyone who points out the violators' wrongdoing. The last one is the victim's denial of wrongdoing. They agree that the victims should be prosecuted using this technique. Typically, this is used to justify attacks on minority groups such as homosexuals [111]. Similarly, along with neutralization, employees can establish value conflicts, such as believing that work is more important than adhering to organizational ISPs, which leads to noncompliance with organizational ISPs [42,78,112].

RQ3: What are the best possible transformation steps of behavior as analyzed in studies from noncompliance to compliance?

Based on the above discussion, we have formulated transformation steps from noncompliance to compliance and developed a process model (Figure 5). These steps' layout is based on the previously described factors and their theoretical underpinnings in Section 5.1.

5.1. Theoretical Implications

Law abidance is a practice that varies from region to region and country to country. National culture is tested in the ISPC domain, and researchers found it significant toward compliance [43,44]. Some researchers considered national culture as a dimension of organizational culture and suggested national culture can be rationalized with the organizational culture [55]. Significantly, security awareness is the primary factor contributing to good security culture. Effective SETA programs make it possible to provide awareness with ease. Security aware behaviors such as knowledge of information security policy, conscious care behaviors towards ISP, early conformance of updated ISP, and employees' competency levels about ISP have significant effects on ISPC [17,90], while top management also plays a vital role in compliance with security policies. Many studies analyzed and discussed management behaviors that determine the direction of security policy compliance. An organization's information security depends on the management's actions and adopted

behaviors, such as declaring ISP mandatory to follow, management support, controllability, and correct use of rank or status [110]—see also Humaidi et al., 2015 [72].

Motivations play a critical role in compliance behaviors. Motivations are categorized into two classes—(1) intrinsic motivations and (2) extrinsic motivations—by ISPC researchers. Intrinsic motivations are self-motivations, i.e., performing an activity for its own sake or for personal rewards, while extrinsic motivation can be defined as performing an activity to avoid punishment [8].

Employees' motivations towards protection show a significant effect on ISPC. The literature supports the claim that if an employee is motivated to protect assets or have protection motivation behavior, they will have substantial chances to comply with ISP. Researchers tested protection motivation behaviors with protection motivation theory (PMT) in the ISPC domain. PMT proposes that people perform two types of actions in a threatening situation. They first evaluate how significant the threat is (threat appraisal) and how to deal with it (coping appraisal). The researchers determined that PMT is the most commonly used theory in ISPC studies (compliance and noncompliance). Several studies tested the strength of threat appraisal and coping appraisal among employees towards ISPC. The literature supports that employees who perceived information security threats severity and perceived coping strategies with the threat have more compliant behaviors [24,37]. Employees perceive extrinsic motivations from their social circle or their peers. Social behaviors influence compliance towards ISP. The researchers outlined many social factors, such as social bonding and social cognition, social pressures, and norms that significantly affect compliance behaviors [82].

The literature about noncompliance behavior suggests that employees' noncompliance with ISP can be intentional or unintentional. Employees indulge in various value conflicts. For instance, a job task's value is perceived to be more critical than information security or the importance of conflict. Security-related stress is a crucial factor for employees' noncompliance [39]. Complex security-related requirements cause negligence and deliberate volitional behavior. Employees who violate the ISP neutralize their actions with the seven techniques defined by David Matza in 1964 [94]. Employees' noncompliance behavior can be deterred by additional sanctions (formal and informal) and punishments. Several studies used deterrence theory in noncompliance behavior and determined that deterrence negatively affected noncompliance [13].

5.2. Practical Implications

This systematic literature review has provided numerous practical contributions/implications for behavioral information security research. This review provided a comprehensive behavior transformation process. The transformation process helps security practitioners understand the reasons for employees' noncompliance and helps them transform employees' deviance into compliant behavior. Previous research shows that most security professionals design ISP in a generic format, which becomes the main reason for employees' noncompliance [40]. Simultaneously, most researchers suggested that information security policy must be structured according to the organizations' needs and operations [74,84]. This study provided all the major compliance/noncompliance factors that can help practitioners design specific information security policies according to their organization's needs.

The literature review evaluated that employees indulge in different value conflicts (i.e., work deadlines and IT vision) while complying with information security guidelines. Our literature analysis suggested that information security professionals must consider all types of conflicts while implementing an information security policy. Furthermore, security-related stress is another noncompliance factor of employees. Employees develop stressed behavior while following complex information security requirements [12]. The current literature review has provided enough evidence that security practitioners must focus on complexity while designing or implementing a security policy.

Information security practitioners must focus on intrinsic/extrinsic motivations. The practitioners must advise the management to provide some rewards to the most compliant employees to promote ISPC. Likewise, this review further revealed that various motivations (i.e., intrinsic/extrinsic and protection motivation) increase social behavior. Multiple research articles showed that better social bonding among employees significantly enhances ISPC [51,72]. Security policymakers must take advantage of this valuable information to enhance compliance intention. For instance, organizations should seek help from influential personalities who can steer employees' opinions and mindset towards ISPC.

Moreover, the management can assign tasks to the team leads inside organizations to motivate employees towards organizational policies. Employees with a better understanding of IS policies and behaviors must be highlighted so that other employees can view them as role models and copy the behavior of individuals whose values reflect their organization's ideals [113,114]. This study further concluded that socially motivated employees foster an excellent security culture in an organization. In comparison, multiple studies proved that organizations with a good security culture are less likely to encounter an information security breach [108].

As a final remark, a detailed investigation of literature about ISB towards ISPC was conducted in this study. According to the best of the authors' knowledge, none of the studies focused on behavior transformation. The current study is the first that highlighted the behavior transformation process of employees. In the next section, recommendations and future directions are provided for researchers and managers.

5.3. Limitations and Future Research

A rigorous approach was adopted for the selection of studies in this review. However, there is still a chance that there are some missing studies that could enhance this literature review's findings. The literature review has presented a process model that needs to be validated. In the future, the research team intends to perform some query-based analysis to validate this process model. Short queries will be generated in the BPMN-Q language for every activity to perform validations. The results showed that the existing compliance checking approaches are not enough to solve the problem. The researchers intend to solve this problem with the help of process management tools and techniques. In contrast, this research is the first step towards modeling and behavioral compliance towards information security policies. In future studies, researchers should focus on transforming employees' behaviors rather than measuring compliance and noncompliance. One must identify the reasons for the noncompliance then apply compliance techniques accordingly. Second, there is much more literature available on compliance behaviors than noncompliance; there is a need to explore more theories and factors incorporated with noncompliance behaviors. Third, information security policy development is another area that needs attention. ISP makers design ISPs without thinking about their own organization's environment and needs. For instance, health employees or IT employees have a more stressful job than many other sectors, so the design of an ISP must focus on the sector or organization's needs. Researchers should research the organization's needs and then suggest how an organization can enhance its ISP according to its needs. Fourth, technology-based solutions are needed, for example, compliance management systems, compliance support systems, and compliance reporting systems. Researchers must see how to incorporate technology in this area and make ISPC more efficient. Fifth, there is still a need to explore more about actual compliance than intention. This literature review revealed that few studies are focusing on actual compliance behavior.

6. Closing Remarks

The current literature review has revealed behavioral factors, concepts, and theories used for ISPC in the last decade. Behaviors associated with compliance and noncompliance were analyzed rigorously. This study proved that while there is no universal generalization of human behaviors towards ISPC, there is also no mutual agreement on the most significant

dimension of behavior toward ISPC. This study concludes that employee noncompliance is because of value conflicts, security-related stress, and neutralization, among many other factors listed in Appendix A Table A2. To transform employees' noncompliance behavior into compliance behavior, management behaviors, security awareness, culture, protected motivated behaviors, and deterrence techniques can play a vital role. This literature review is an effort to develop a behavioral transformation process of violation to compliance. Many vital factors identified from the literature and a process have been drawn for the ISB transformation presented in Figure 1. Although human behavior transformation is a complex phenomenon, this study will contribute towards the body of knowledge as a novel effort to identify the gap. IT professionals, ISPC practitioners, and researchers can benefit from this literature review and expand their view of information security behaviors. Security managers can gain insight from the depicted transformation process towards various security behaviors and practice it in their organizations.

Some of the recommendations have been drawn from peer reviewed studies. First, the ISP should be convenient to understand because inconvenient methods cause security-related stress, which leads to noncompliance. Second, work deadlines must not be overlapped with ISP. Third, managers should evaluate employees' behaviors regularly, and scale their awareness level, provide training if needed till they ultimately adopt security-aware behaviors. Fourth, whistleblowing campaigns should be arranged to convince employees to file a report if they see something suspicious. Fifth, organizations should provide motivational training, and covey how an employee is an asset to the organization, and not let somebody use this asset against the organization. Last, include SETA programs in the daily work routine so that employees can learn about ISP passively.

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

Funding: This work was funded by the Department of Computer and Information Sciences, Universiti Teknologi PETRONAS (UTP) under grant cost center YUTP-FRG Grant (015LCO-171). The APC was funded through this grant.

Institutional Review Board Statement: Not applicable: This research involves no human subjects, human material, human tissues, or human data.

Informed Consent Statement: Not applicable: This research involves no human subjects, human material, human tissues, or human data.

Data Availability Statement: Not applicable: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The authors would also like to thank the Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Malaysia, for facilitating this research study. The authors would also like to thank the anonymous reviewers for their valuable suggestions to enhance the manuscript.

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

Appendix A

Table A1. Overview of factors influencing compliance.

Study	Theory Used	Influencing Factors
[44]	Grounded Theory	Information security value, formalized controls, and workplace relationships
[99]	Theory of Neutralization, Deterrence Theory	Power distance, masculinity, individualism, moral beliefs

Table A1. *Cont.*

Study	Theory Used	Influencing Factors
[8]	General Deterrence Theory	Perceived legitimacy, perceived value congruences, perceived severity, perceived certainty
[59]	TPB, Self-Determination and Organismic Integration Theory	General motivations (locus of control) and situational motivations
[60]	PMT, TPB	Social influence, response efficacy, self-efficacy
[14]	PMT, TPB	Perceived vulnerability, response efficacy, self-efficacy, attitude, subjective norms.
[61]	PMT	Habit, rewards, vulnerability, perceived severity
[37]	PMT	Criticality
[24]	PMT	Fear and protection motivation
[62]	PMT	Fear and protection motivation
[54]	PMT	Continues intention, perceived extraneous circumstances
[63]	PMT	Hope, optimism, self-efficacy, resilience, fear, and protection motivation
[64]	PMT	Response efficacy and response cost
[65]	PMT	Responsibility, OCB, psychological ownership, and protection motivation
[66]	PMT, Health Belief Model, DT, TRA	Self-efficacy and impact
[45]	Ethical Decision-Making Model, and Value Congruence Theory	Moral beliefs
[27]	PMT, TPB, GDT, and OT	Vulnerability, self-efficacy, response efficacy, response-cost
[16]	TRA, TPB	Knowledge, value, skills, culture
[49]	TPB	Top management, culture, attitude, perceived compliance control, subjective norms
[46]	Social Exchange Theory	Job satisfaction, perceived organizational support, and security culture
[68]	PMT	Knowledge and protection motivation
[47]	PMT, TPB	Awareness, subjective norms, attitude, perceived behavioral control
[52]	PMT and Health Belief Model	Security systems, security education, security visibility
[17]	TPB	Security awareness, intention to confirm early
[48]	Theory of Organizational Behavior and Strategic Management Theory	Discipline and agility
[69]	PMT	Moral obligations, attitude
[70]	TPB and Theory of Acceptance Model	Leadership, training, and perceived usefulness of security
[71]	TPB and Health Believe Model	Management, awareness, working experience
[72]	TPB	Status (rank), perceived behavioral control
[73]	RCT	Psychological contract, perceived cost, perceived benefit
[74]	RCT	Corporate social responsibility, perceived benefit, perceived benefit
[75]	Social cognitive learning theory	Security monitoring, outcome expectation, self-efficacy
[76]	Social Exchange Theory	Organizational commitment, perceived organizational support, response cost
[77]	Theory of Inertia	Cognitive inertia, it usage inertia
[15]	TRA, PMT, GDT, Innovation Diffusion Theory	Deterrence and intention to comply
[90]	TPB	Intended behavior, perceived behavior control
[35]	PMT, TPB, GDT	Organizational commitment, subjective norms, perceived behavior control, attitude
[91]	TPB	Organizational culture, behavior type
[92]	TPB	Intention to commit, desire to commit
[93]	GDT, SCPT, TPB	Subjective norms, intention to prevent misbehavior
[89]	Social Cognitive Theory	Coworker socialization, computer self-efficacy, personal innovations
[103]	GDT, Social Bond Theory(SBT)	Commitment, involvement, personal norms, social pressure, perceived severity, and certainty
[82]	TPB, SBT, Social Control Theory (SCT)	Attitude, subjective norms, locus of control, self-efficacy
[83]	PMT	Social influence, knowledge, self-efficacy

Table A1. *Cont.*

Study	Theory Used	Influencing Factors
[41]	SCT	Attachment, commitment, involvement, personal norms, specification, evaluation, reward
[84]	Norm Active Theory, Theory of Social Norms	Personal norms, awareness, ascription of personal responsibility
[85]	SBT, Involvement Theory	Attachment, commitment, involvement, personal norms, knowledge sharing, collaboration, intervention, experience and attitude
[86]	SBT, SCPT	Commitment, involvement, personal norms, misbehavior reduction intention
[87]	Person-Organization fit theory	Security commitment, apathy, and fit elements

Table A2. Overview of factors influencing compliance.

Studies	Theory Used	Influencing Factors
[38]	TPB, PMT, GDT	Previous punishment experience
[40]	PMT	IT vision conflict
[20]	Coping Theory, Disengagement Theory,	SRS, realism, perceived sanctions
[12]	Theory of Neutralization	SRS fatigue, and frustration
[11]	TPB, RCT	Negative affect, work impediment, and daily deviance
[42]	Grounded Theory	Value assignment, perception of information value
[51]	Theory of Neutralization	Ethical work climate, beliefs
[105]	PMT and GDT	Human personality traits (stability and plasticity)
[95]	Theory of Neutralization, PMT, TPB	Normative faith
[104]	GDT	Satisfaction and safe behavior
[39]	Prospect Theory, RCT, self-justification Theory, Approach AvoidanceTheory	Sunk cost, self-justification, and risk perception
[102]	Stewardship Theory	Value identification, trusted relationship fulfillment, growth need fulfillment, long-term orientation, the intention of CDSIV.
[23]	TPB, GDT	Descriptive norms, moral norms
[15]	Theory of Neutralization	Sanctions (formal. Informal), shame
[40]	Coping Theory	Perceived externality, triage, procrastination, psychological detachment
[96]	Theory of Neutralization, Deterrence	Organizational injustice (procedural and distributive)

Table A3. The most common theories used for compliance studies.

No	Theory Name
1	Theory of Planned Behavior
2	Protection Motivation Theory
3	Social Cognitive Theory
4	Social Bond Theory
5	Social Control Theory
6	Rational Choice Theory
7	Health Belief Model
8	Social Exchange Theory
9	Agency theory
10	General Deterrence Theory

Table A4. Most common theories used for noncompliance studies.

No	Theory Name
1	Theory of Neutralization
2	General Deterrence Theory
3	Protection Motivation Theory
4	Coping Theory
5	Rational Choice Theory
6	Self-Justification Theory

Table A5. Category wise study list.

Category	Compliance/Noncompliance	Number of Studies
National culture	Compliance	1
Intrinsic/extrinsic motivations	Compliance	3
Protection motivation behaviors	Compliance	15
Culture/aware behaviors	Compliance	7
Management behaviors	Compliance	12
Social behaviors	Compliance	10
Actual compliance behaviors	Compliance	6
SRS/neutralization	Noncompliance	12
Value conflicts	Noncompliance	5
Deterrence	Noncompliance	9
Total		80

Table A6. Terminologies used in the study.

Terminology	Meaning
ISPC	Information security policy compliance
SLR	Systematic literature review
ISP	Information security policy
ISB	Information security behavior
BPMN	Business process modeling notation
ICT	Information communication technology
PMB	Protection motivation behaviors
PMT	Protection motivation theory
TPB	Theory of planned behavior
TRA	Theory of reasoned action
SBT	Social bond theory
DT	Deterrence theory
GDT	General deterrence theory
OT	Operational theory
RCT	Rational choice theory
SCPT	Situational crime prevention theory
SRS	Security-related stress
CDISV	Consequence-delayed information security violation
LTO	Long-term orientation

References

1. Ali, S.E.A.; Lai, F.-W.; Hassan, R.; Shad, M.K. The Long-Run Impact of Information Security Breach Announcements on Investors' Confidence: The Context of Efficient Market Hypothesis. *Sustainability* **2021**, *13*, 1066. [CrossRef]
2. Ali, S.E.A.; Lai, F.-W.; Hassan, R. Socio-Economic Factors On Sector-Wide Systematic Risk Of Information Security Breaches: Conceptual Framework. In Proceedings of the International Economics and Business Management Conference, Melaka, Malaysia, 2–3 November 2020; pp. 502–512.
3. Ali, R.F.; Dominic, P.; Ali, K. Organizational governance, social bonds and information security policy compliance: A perspective towards oil and gas employees. *Sustainability* **2020**, *12*, 8576. [CrossRef]
4. Dong, K.; Ali, R.F.; Dominic, P.; Ali, S.E.A. The Effect of Organizational Information Security Climate on Information Security Policy Compliance: The Mediating Effect of Social Bonding towards Healthcare Nurses. *Sustainability* **2021**, *13*, 2800. [CrossRef]
5. Services, S. *IBM Infographic: Cyber Security Intelligence Index*; IBM: Armonk, NY, USA, 2014. Available online: http://www-935.ibm.com/services/us/en/it-services/security-services/2014-cyber-security-intelligence-index-infographic (accessed on 7 September 2019).
6. PWC. *UK Organisations Still Failing to Prepare Effectively for Cyber Attacks*; PWC: Cambridge, UK, 2017. Available online: https://www.pwc.co.uk/press-room/press-releases/global-state-information-security-survey-2018-uk.html (accessed on 12 March 2020).
7. NIST. *NIST Standards and Guidlines*; NIST: Gaithersburg, MD, USA, 2019. Available online: https://www.nist.gov/topics/cybersecurity (accessed on 14 April 2020).
8. Jai-Yeol, S. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Inf. Manag.* **2011**, *48*, 296–302. [CrossRef]

9. Siponen, M.; Willison, R. Information security management standards: Problems and solutions. *Inf. Manag.* **2009**, *46*, 267–270. [CrossRef]
10. Yildirim, E.Y.; Akalp, G.; Aytac, S.; Bayram, N. Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey. *Int. J. Inf. Manag.* **2011**, *31*, 360–365. [CrossRef]
11. D'Arcy, J.; Lowry, P.B. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Inf. Syst. J.* **2019**, *29*, 43–69. [CrossRef]
12. D'Arcy, J.; Teh, P.-L. Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Inf. Manag.* **2019**, *56*, 103–151. [CrossRef]
13. D'Arcy, J.; Herath, T. A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *Eur. J. Inf. Syst.* **2011**, *20*, 643–658. [CrossRef]
14. Ifinedo, P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Comput. Secur.* **2012**, *31*, 83–95. [CrossRef]
15. Siponen, M.; Pahnila, S.; Mahmood, M.A. Compliance with information security policies: An empirical investigation. *Computer* **2010**, *43*, 64–71. [CrossRef]
16. Alfawaz, S.; Nelson, K.; Mohannak, K. Information security culture: A behaviour compliance conceptual framework. In Proceedings of the Eighth Australasian Conference on Information Security-Volume 105, Brisbane, Australia, 10 January 2010; pp. 47–55.
17. Bélanger, F.; Collignon, S.; Enget, K.; Negangard, E. Determinants of early conformance with information security policies. *Inf. Manag.* **2017**, *54*, 887–901. [CrossRef]
18. Herath, T.; Rao, H.R. Protection motivation and deterrence: A framework for security policy compliance in organisations. *Eur. J. Inf. Syst.* **2009**, *18*, 106–125. [CrossRef]
19. Herath, T.; Rao, H.R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decis. Support Syst.* **2009**, *47*, 154–165. [CrossRef]
20. D'Arcy, J.; Herath, T.; Shoss, M.K. Understanding employee responses to stressful information security requirements: A coping perspective. *J. Manag. Inf. Syst.* **2014**, *31*, 285–318. [CrossRef]
21. Corradini, I. Security: Human Nature and Behaviour. In *Building a Cybersecurity Culture in Organizations*; Springer: Cham, Switzerland, 2020; Volume 1, pp. 23–47.
22. Liu, C.; Wang, N.; Liang, H. Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *Int. J. Inf. Manag.* **2020**, *54*, 102152. [CrossRef]
23. Merhi, M.I.; Ahluwalia, P. Examining the impact of deterrence factors and norms on resistance to information systems security. *Comput. Hum. Behav.* **2019**, *92*, 37–46. [CrossRef]
24. Boss, S.; Galletta, D.; Lowry, P.B.; Moody, G.D.; Polak, P. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Q.* **2015**, *39*, 837–864. Available online: https://www.jstor.org/stable/26628654 (accessed on 15 March 2020). [CrossRef]
25. Bongiovanni, I. The least secure places in the universe? A systematic literature review on information security management in higher education. *Comput. Secur.* **2019**, *86*, 350–357. [CrossRef]
26. Hina, S.; Dominic, P.D.D. Information security policies' compliance: A perspective for higher education institutions. *J. Comput. Inf. Syst.* **2018**, *60*, 201–211. [CrossRef]
27. Rajab, M.; Eydgahi, A. Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Comput. Secur.* **2019**, *80*, 211–223. [CrossRef]
28. Sommestad, T.; Karlzén, H.; Hallberg, J. A meta-analysis of studies on protection motivation theory and information security behaviour. *Int. J. Inf. Secur. Priv.* **2015**, *9*, 26–46. [CrossRef]
29. Shahzad, K.; Nawab, R.M.A.; Abid, A.; Sharif, K.; Ali, F.; Aslam, F.; Mazhar, A. A process model collection and gold standard correspondences for process model matching. *IEEE Access* **2019**, *7*, 30708–30723. [CrossRef]
30. Shankararaman, V. *Business Enterprise, Process, and Technology Management: Models and Applications*; IGI Global: Hershey, PA, USA, 2012.
31. Shahzad, K.; Shareef, K.; Ali, R.F.; Nawab, R.M.A.; Abid, A. Generating process model collection with diverse label and structural features. In Proceedings of the 2016 Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, Ireland, 24–26 August 2016; pp. 644–649.
32. Sommestad, T.; Hallberg, J.; Lundholm, K.; Bengtsson, J. Variables influencing information security policy compliance. *Inf. Manag. Comput. Secur.* **2014**, *22*, 42–75. [CrossRef]
33. Tsohou, A.; Holtkamp, P. Are users competent to comply with information security policies? An analysis of professional competence models. *Inf. Technol. People* **2018**, *31*, 1047–1068. [CrossRef]
34. Trang, S.; Brendel, B. A meta-analysis of deterrence theory in information security policy compliance research. *Inf. Syst. Front.* **2019**, *21*, 1–20. [CrossRef]
35. Salvatore, A. A Composite Framework for Behavioral Compliance with Information Security Policies. *J. Organ. End User Comput.* **2013**, *25*, 32–51. [CrossRef]
36. Padayachee, K. Taxonomy of compliant information security behavior. *Comput. Secur.* **2012**, *31*, 673–680. [CrossRef]

37. Posey, C.; Roberts, T.L.; Lowry, P.B.; Bennett, R.J. Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Q.* **2013**, *37*, 1189–1210. Available online: http://www.jstor.org/stable/43825787 (accessed on 28 April 2020). [CrossRef]
38. Aurigemma, S.; Mattson, T. Deterrence and punishment experience impacts on ISP compliance attitudes. *Inf. Comput. Secur.* **2017**, *25*, 421–436. [CrossRef]
39. Kajtazi, M.; Cavusoglu, H.; Benbasat, I.; Haftor, D. Escalation of commitment as an antecedent to noncompliance with information security policy. *Inf. Comput. Secur.* **2018**, *26*, 171–193. [CrossRef]
40. Chang, K.-C.; Seow, Y.M. Protective measures and security policy non-compliance intention: It vision conflict as a moderator. *J. Organ. End User Comput.* **2019**, *31*, 1–21. [CrossRef]
41. Hsu, J.S.-C.; Shih, S.-P.; Hung, Y.W.; Lowry, P.B. The role of extra-role behaviors and social controls in information security policy effectiveness. *Inf. Syst. Res.* **2015**, *26*, 282–300. [CrossRef]
42. Doherty, N.F.; Tajuddin, S.T. Towards a user-centric theory of value-driven information security compliance. *Inf. Technol. People* **2018**, *31*, 348–367. [CrossRef]
43. Dinev, T.; Goo, J.; Hu, Q.; Nam, K. User behaviour towards protective information technologies: The role of national cultural differences. *Inf. Syst. J.* **2009**, *19*, 391–412. [CrossRef]
44. Connolly, L.Y.; Lang, M.; Wall, D.S. Information Security Behavior: A Cross-Cultural Comparison of Irish and US Employees. *Inf. Syst. Manag.* **2019**, *36*, 306–322. [CrossRef]
45. Lankton, N.K.; Stivason, C.; Gurung, A. Information protection behaviors: Morality and organizational criticality. *Inf. Comput. Secur.* **2019**, *27*, 468–488. [CrossRef]
46. D'Arcy, J.; Greene, G. Security culture and the employment relationship as drivers of employees' security compliance. *Inf. Manag. Comput. Secur.* **2014**, *22*, 474–489. [CrossRef]
47. Safa, N.S.; Sookhak, M.; Von Solms, R.; Furnell, S.; Ghani, N.A.; Herawan, T. Information security conscious care behaviour formation in organizations. *Comput. Secur.* **2015**, *53*, 65–78. [CrossRef]
48. Harnesk, D.; Lindström, J. Shaping security behaviour through discipline and agility: Implications for information security management. *Inf. Manag. Comput. Secur.* **2011**, *19*, 262–276. [CrossRef]
49. Hu, Q.; Dinev, T.; Hart, P.; Cooke, D. Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decis. Sci.* **2012**, *43*, 615–660. [CrossRef]
50. Sykes, G.M.; Matza, D. Techniques of neutralization: A theory of delinquency. *Am. Sociol. Rev.* **1957**, *22*, 664–670. [CrossRef]
51. Gwebu, K.L.; Wang, J.; Hu, M.Y. Information security policy noncompliance: An integrative social influence model. *Inf. Syst. J.* **2020**, *30*, 1350–1917. [CrossRef]
52. Hwang, I.; Kim, D.; Kim, T.; Kim, S. Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Inf. Rev.* **2017**, *41*, 2–18. [CrossRef]
53. Anderson, C.L.; Agarwal, R. Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Q.* **2010**, *34*, 613–643. [CrossRef]
54. Merrill, W.; Allen, C. Continuance of protective security 1301 behavior: A longitudinal study. *Decis. Support Syst.* **2016**, *92*, 25–35. [CrossRef]
55. Nasir, A.; Arshah, R.A.; Ab Hamid, M.R. Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture: A Conceptual Framework. In Proceedings of the 2017 International Conference on Information System and Data Mining, South Carolina, SC, USA, 1–3 April 2017; pp. 56–60.
56. Soomro, Z.A.; Shah, M.H.; Ahmed, J. Information security management needs more holistic approach: A literature review. *Int. J. Inf. Manag.* **2016**, *36*, 215–225. [CrossRef]
57. Wolfswinkel, J.F.; Furtmueller, E.; Wilderom, C.P. Using grounded theory as a method for rigorously reviewing literature. *Eur. J. Inf. Syst.* **2013**, *22*, 45–55. [CrossRef]
58. Booth, A.; Sutton, A.; Papaioannou, D. *Systematic Approaches to a Successful Literature Review*; Sage: London, UK, 2016.
59. Kranz, J.; Haeussinger, F. Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior. In Proceedings of the International conference on information systems, Auckland, New Zealand, 14–17 December 2014; pp. 23–44.
60. Warkentin, M.; Johnston, A.C. Fear appeals and information security behaviors: An empirical study. *Mis Q.* **2010**, *34*, 549–566. [CrossRef]
61. Vance, A.; Siponen, M.; Pahnila, S. Motivating IS security compliance: Insights from habit and protection motivation theory. *Inf. Manag.* **2012**, *49*, 190–198. [CrossRef]
62. Warkentin, M.; Siponen, M. An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Q.* **2015**, *39*, 113–134. Available online: https://www.jstor.org/stable/26628343 (accessed on 30 April 2020).
63. Burns, A.; Posey, C.; Roberts, T.L.; Lowry, P.B. Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Comput. Hum. Behav.* **2017**, *68*, 190–209. [CrossRef]
64. Crossler, R.E.; Bélanger, F.; Ormond, D. The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. *Inf. Syst. Front.* **2017**, *21*, 343–357. [CrossRef]
65. Blythe, J.M.; Coventry, L. Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Comput. Hum. Behav.* **2018**, *87*, 87–97. [CrossRef]

66. Hooper, V.; Blunt, C. Factors influencing the information security behaviour of IT employees. *Behav. Inf. Technol.* **2019**, *39*, 1–13. [CrossRef]
67. Alanazi, S.T.; Anbar, M.; Ebad, S.A.; Karuppayah, S.; Al-Ani, H.A. Theory-Based Model and Prediction Analysis of Information Security Compliance Behavior in the Saudi Healthcare Sector. *Symmetry* **2020**, *12*, 1544. [CrossRef]
68. Pahnila, S.; Karjalainen, M.; Siponen, M.T. Information Security Behavior: Towards Multi-Stage Models. In Proceedings of the Pacific Asia Conference on Information Systems, Jeju Island, Korea, 18–22 June 2013; pp. 102–122.
69. Yoon, C.; Kim, H. Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. *Inf. Technol. People* **2013**, *26*, 401–419. [CrossRef]
70. Humaidi, N.; Balakrishnan, V. Exploratory factor analysis of user's compliance behaviour towards health information system's security. *J. Health Med. Inform.* **2013**, *4*, 2–9. [CrossRef]
71. Humaidi, N.; Balakrishnan, V. The Moderating effect of working experience on health information system security policies compliance behaviour. *Malays. J. Comput. Sci.* **2015**, *28*, 70–92. Available online: https://ejournal.um.edu.my/index.php/MJCS/article/view/6856 (accessed on 15 May 2020).
72. Aurigemma, S.; Mattson, T. Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Comput. Secur.* **2017**, *66*, 218–234. [CrossRef]
73. Han, J.; Kim, Y.J.; Kim, H. An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Comput. Secur.* **2017**, *66*, 52–65. [CrossRef]
74. Kim, H.L.; Han, J. Do employees in a "good" company comply better with information security policy? A corporate social responsibility perspective. *Inf. Technol. People* **2018**, *32*, 858–875. [CrossRef]
75. Ahmad, Z.; Ong, T.S.; Liew, T.H.; Norhashim, M. Security monitoring and information security assurance behaviour among employees: An empirical analysis. *Inf. Comput. Secur.* **2019**, *27*, 165–188. [CrossRef]
76. Sharma, S.; Warkentin, M. Do I really belong? Impact of employment status on information security policy compliance. *Comput. Secur.* **2019**, *87*, 101397. [CrossRef]
77. Sillic, M. Critical impact of organizational and individual inertia in explaining non-compliant security behavior in the Shadow IT context. *Comput. Secur.* **2019**, *80*, 108–119. [CrossRef]
78. Koohang, A.; Nowak, A.; Paliszkiewicz, J.; Nord, J.H. Information Security Policy Compliance: Leadership, Trust, Role Values, and Awareness. *J. Comput. Inf. Syst.* **2020**, *60*, 1–8. [CrossRef]
79. Chakraborty, T.; Jajodia, S.; Katz, J.; Picariello, A.; Sperli, G.; Subrahmanian, V. FORGE: A fake online repository generation engine for cyber deception. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 518–533. [CrossRef]
80. Han, Q.; Molinaro, C.; Picariello, A.; Sperli, G.; Subrahmanian, V.S.; Xiong, Y. Generating Fake Documents using Probabilistic Logic Graphs. *IEEE Trans. Dependable Secur. Comput.* **2021**, 1–15. [CrossRef]
81. Naseer, S.; Faizan Ali, R.; Dominic, P.; Saleem, Y. Learning Representations of Network Traffic Using Deep Neural Networks for Network Anomaly Detection: A Perspective towards Oil and Gas IT Infrastructures. *Symmetry* **2020**, *12*, 1882. [CrossRef]
82. Ifinedo, P. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Inf. Manag.* **2014**, *51*, 69–79. [CrossRef]
83. Posey, C.; Roberts, T.L.; Lowry, P.B.; Hightower, R.T. Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Inf. Manag.* **2014**, *51*, 551–567. [CrossRef]
84. Yazdanmehr, A.; Wang, J. Employees' information security policy compliance: A norm activation perspective. *Decis. Support Syst.* **2016**, *92*, 36–46. [CrossRef]
85. Safa, N.S.; Von Solms, R.; Furnell, S. Information security policy compliance model in organizations. *Comput. Secur.* **2016**, *56*, 70–82. [CrossRef]
86. Safa, N.S.; Maple, C.; Watson, T.; Von Solms, R. Motivation and opportunity based model to reduce information security insider threats in organisations. *J. Inf. Secur. Appl.* **2018**, *40*, 247–257. [CrossRef]
87. Chen, H.; Li, W. Understanding commitment and apathy in is security extra-role behavior from a person-organization fit perspective. *Behav. Inf. Technol.* **2019**, *38*, 454–468. [CrossRef]
88. Yazdanmehr, A.; Wang, J.; Yang, Z. Peers matter: The moderating role of social influence on information security policy compliance. *Inf. Syst. J.* **2020**, *30*, 787–790. [CrossRef]
89. Jaafar, N.I.; Ajis, A. Organizational climate and individual factors effects on information security compliance behaviour. *Int. J. Bus. Soc. Sci.* **2013**, *4*, 1–13.
90. Cox, J. Information systems user security: A structured model of the knowing—Doing gap. *Comput. Hum. Behav.* **2012**, *28*, 1849–1858. [CrossRef]
91. Djajadikerta, H.G.; Roni, S.M.; Trireksani, T. Dysfunctional information system behaviors are not all created the same: Challenges to the generalizability of security-based research. *Inf. Manag.* **2015**, *52*, 1012–1024. [CrossRef]
92. Chu, A.M.; Chau, P.Y.; So, M.K. Explaining the misuse of information systems resources in the workplace: A dual-process approach. *J. Bus. Ethics* **2015**, *131*, 209–225. [CrossRef]
93. Safa, N.S.; Maple, C.; Furnell, S.; Azad, M.A.; Perera, C.; Dabbagh, M.; Sookhak, M. Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Gener. Comput. Syst. 2019 97*, 587–597. [CrossRef]

94. Mikko, S.; Vance, A. Neutralization: New insights into the problem of employee information systems 1407 security policy violations. *MIS Q.* **2010**, *34*, 487–502. [CrossRef]
95. Kim, S.H.; Yang, K.H.; Park, S. An integrative behavioral model of information security policy compliance. *Sci. World J.* **2014**, *2014*, 463870. [CrossRef] [PubMed]
96. Willison, R.; Warkentin, M.; Johnston, A.C. Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Inf. Syst. J.* **2018**, *28*, 266–293. [CrossRef]
97. Moody, G.D.; Siponen, M.; Pahnila, S. Toward a unified model of information security policy compliance. *MIS Q.* **2018**, *42*, 285–302. [CrossRef]
98. Shadbad, F.N.; Biros, D. Technostress and its influence on employee information security policy compliance. *Inf. Technol. People* **2020**, *2*, 1–23. [CrossRef]
99. Vance, A.; Siponen, M.T.; Straub, D.W. Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. *Inf. Manag.* **2020**, *57*, 103212. [CrossRef]
100. Xu, Z.; Guo, K. It ain't my business: A coping perspective on employee effortful security behavior. *J. Enterp. Inf. Manag.* **2019**, *32*, 824–842. [CrossRef]
101. Bansal, G.; Muzatko, S.; Shin, S.I. Information system security policy noncompliance: The role of situation-specific ethical orientation. *Inf. Technol. People* **2020**, *34*, 250–296. [CrossRef]
102. Li, Y.; Zhang, N.; Siponen, M. Keeping secure to the end: A long-term perspective to understand employees' consequence-delayed information security violation. *Behav. Inf. Technol.* **2019**, *38*, 435–453. [CrossRef]
103. Cheng, L.; Li, Y.; Li, W.; Holm, E.; Zhai, Q. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Comput. Secur.* **2013**, *39*, 447–459. [CrossRef]
104. Klein, R.H.; Luciano, E.M. What influences information security behavior? A study with Brazilian users. *J. Inf. Syst. Technol. Manag.* **2016**, *13*, 479–496. [CrossRef]
105. Johnston, A.C.; Warkentin, M.; McBride, M.; Carter, L. Dispositional and situational factors: Influences on information security policy violations. *Eur. J. Inf. Syst.* **2016**, *25*, 231–251. [CrossRef]
106. Jaeger, L.; Eckhardt, A.; Kroenung, J. The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis. *Inf. Manag.* **2020**, *1*, 103318. [CrossRef]
107. Chen, L.; Zhen, J.; Dong, K.; Xie, Z. Effects of sanction on the mentality of information security policy compliance. *Rev. Argent. Clínica Psicológica* **2020**, *29*, 39–49. [CrossRef]
108. Da Veiga, A.; Astakhova, L.V.; Botha, A.; Herselman, M. Defining organisational information security culture—Perspectives from academia and industry. *Comput. Secur.* **2020**, *92*, 101713. [CrossRef]
109. Boss, S.R.; Kirsch, L.J.; Angermeier, I.; Shingler, R.A.; Boss, R.W. If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *Eur. J. Inf. Syst.* **2009**, *18*, 151–164. [CrossRef]
110. Rogers, J.W.; Buffalo, M. Neutralization techniques: Toward a simplified measurement scale. *Pac. Sociol. Rev.* **1974**, *17*, 313–331. [CrossRef]
111. Lee, S.; Lee, M. An exploratory study on the information security culture indicator. *Informatiz. Policy* **2008**, *15*, 100–119.
112. Myyry, L.; Siponen, M.; Pahnila, S.; Vartiainen, T.; Vance, A. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *Eur. J. Inf. Syst.* **2009**, *18*, 126–139. [CrossRef]
113. Robinson, S.L.; O'Leary-Kelly, A.M. Monkey see, monkey do: The influence of work groups on the antisocial behavior of employees. *Acad. Manag. J.* **1998**, *41*, 658–672. [CrossRef]
114. Thomas, J.G.; Griffin, R.W. The power of social information in the workplace. *Organ. Dyn.* **1989**, *18*, 63–75. [CrossRef]