The Effect of Organizational Factors on the Mitigation of Information Security Insider Threats

information

MDPI

Article

The Effect of Organizational Factors on the Mitigation of Information Security Insider Threats

Nader Sohrabi Safa [1,*] and Hossein Abroshan [2]

[1] Department of Computing, Worcester Business School, University of Worcester, Worcester WR1 3AS, UK
[2] School of Computing and Information Sciences, Anglia Ruskin University, Cambridge CB1 1PT, UK; hossein.abroshan@aru.ac.uk
* Correspondence: n.sohrabisafa@worc.ac.uk

Abstract

Insider threats pose significant challenges to organizations, seriously endangering information security and privacy protection. These threats arise when employees with legitimate access to systems and databases misuse their privileges. Such individuals may alter, delete, or insert data into datasets, sell customer or client email addresses, leak strategic company plans, or transfer industrial and intellectual property information. These actions can severely damage a company's reputation, result in revenue losses and loss of competitive advantage, and, in extreme cases, lead to bankruptcy. This study presents a novel solution that examines how organizational factors such as job satisfaction and security, organizational support, attachment, commitment, involvement in information security, and organizational norms influence employees' attitudes and intentions, thereby mitigating insider threats. A key strength of this research is its integration of two foundational theories: the Social Bond Theory (SBT) and the Theory of Planned Behavior (TPB). The results reveal that job satisfaction and security, affective and normative commitment, information security training, and personal norms all contribute to reducing insider threats. Furthermore, the findings indicate that employees' attitudes, perceived behavioral control, and subjective norms significantly influence their intentions to mitigate insider threats. However, organizational support and continuance commitment were not found to have a significant impact.

Keywords: information security; insider threats; social bond; commitment; human factors

Academic Editors: Rami Puzis and Aneta Poniszewska-Maranda

Received: 29 April 2025
Revised: 26 May 2025
Accepted: 18 June 2025
Published: 25 June 2025

Citation: Safa, N.S.; Abroshan, H. The Effect of Organizational Factors on the Mitigation of Information Security Insider Threats. *Information* **2025**, *16*, 538. https://doi.org/10.3390/info16070538

1. Introduction

Insider threats in organizations jeopardize confidentiality, integrity, and availability (CIA) of information [1]. Insider threats refer to employees who have access to different systems, files, and databases due to their roles and responsibilities, which have been defined for them [2]. They misuse this privilege to create job security, earn more money, gain a better position in other companies, get revenge, and so on [3]. These damage the reputation of an organization, cause loss of revenue, income and market, loss of intellectual properties, and in a worst-case scenario, bankruptcy [4]. It has been acknowledged that lack of commitment to organizational aims and targets, absence of attachment to plans and policies, and less involvement in information security enhance the risk of information security breaches in organizations [5–7]. Experts in the field of information security believe that awareness about information security plays an essential role in this domain [8,9]. We have considered information security (IS) training as the involvement and the role in

employees' engagement in information security in our study and investigated its effect on insider threats. Insider threats also negatively affect compliance with General Data Protection Rules and regulations (GDPR); we investigate this aspect of information security (privacy protection) as another important part of this study. The GDPR has seven principles, one of which is integrity and confidentiality. Mitigation of insider threats in organizations protects privacy and confidentiality, which is required by the GDPR.

Organizational factors encompass a wide range of contextual elements within a workplace, such as communication flow, job satisfaction and security, organizational support, emotional attachment, commitment, etc., that collectively shape the behaviors of individuals and groups [10]. The novelty of this research originates from the investigation of organizational factors, including job satisfaction, job security, and organizational support, as factors that show attachment. This study also considers three different types of commitments on employees' behavior towards the mitigation of insider threats for the first time; the entire conceptual model has been covered by the Social Bond Theory (SBT), and the Theory of Planned Behavior (TPB). More explanations about the conceptual model will be presented in the following sections.

This study draws on the Social Bond Theory (SBT) and the Theory of Planned Behavior (TPB) as its theoretical foundations. The SBT explains how strong social ties, such as attachment, commitment, and involvement, reduce the likelihood of deviant acts, making it relevant for insider threat mitigation [11]. TPB complements this by linking attitudes, subjective norms, and perceived behavioral control to behavioral intentions, offering insight into why employees comply with security policies [12]. Together, these theories provide a robust framework for analyzing the relational and cognitive factors that influence employee behavior in information security contexts.

This study contributes both theoretically and practically to the field of information security. Theoretically, it is the first to integrate the SBT and the TPB to examine insider threat mitigation, offering a dual-lens framework that captures both socio-emotional and cognitive-behavioral drivers of secure behavior. Practically, the study identifies actionable organizational factors, such as job satisfaction, affective commitment, and information security training, that can be strategically managed to reduce the likelihood of insider threats. This approach provides organizations with a holistic, evidence-based model that goes beyond technical controls and incorporates human and organizational dynamics.

We have organized the rest of this paper as follows: the theoretical background and explanations of the SBT and the TPB and the rationale behind their applications have been explained in Section 2. The definitions and justifications for the effective factors supported by essential theories and the hypotheses are presented in Section 3. The research methodology and the steps that have been taken to complete this research have been elaborated in Section 4. The results that come from different statistical tests, structural equation modelling (SEM), the structural model, and the measurement model are presented in Section 5. The positive effects of this study on information security in organizations are demonstrated in Section 6. Conclusions, limitations, and future works are defined in Section 7.

2. The Theoretical Background

Different social, psychological, managerial, and educational theories help researchers to explain different phenomena and changes that happen around us. Researchers use these theories to explain how various factors affect each other to solve a problem. For instance, the Technology Acceptance Model (TAM) is used to show the adoption of new technology such as cloud computing, fog computing, smart objects, and so on [13,14]; the Theory of Planned Behavior (TPB) is applied to explain the change of employees' behavior

based on organizational information security policies and procedures [10,15]; the Protection Motivation Theory (PMT) has been used to clarify how information security-conscious care forms in an organization [16]; the Social Bond Theory (SBT) is used to explain how we can mitigate misuse or abuse of privilege in an organization. Experts in this domain have applied a variety and combination of these theories to solve different problems in the field of the human aspects of information security. These theories not only explain different changes and phenomena, but also show the reliability of a conceptual framework. It has been acknowledged that the reliability of a model originates from a strong literature review, theoretical background, experts' opinion in this domain in two or more rounds (the Delphi method), and the results of data analysis. Although this research does not focus on research methodology, we believe that this explanation helps the readers of this article and researchers understand different steps in this research better. The applied theories in this study are explained more in the following sections.

2.1. Social Bond Theory

The SBT has been used in many studies due to its ability to explain the effect of individual norms, involvement, attachment, and commitment on human or employees' behavior in organizations. These four factors influence human attitudes and justify their behavior in many cases [17,18]. Hirschi [11] discussed these factors and claimed that humans have the potential of deviation from rules and regulations. The SBT explains how individuals who have strong bonds engage less in illegal behavior; deviance happens when the relationship between the individuals and the group is weak. The more employees are bonded to an organization, the less likely they are to deviate from its rules and regulations [15]. These factors have been used to explain that the development of attachment, commitment, involvement in different aspects of information security, and negative belief about information security misbehavior in organizations can reduce insider threats.

The SBT can explain how the attachment of teenagers to different groups, their commitment to their values and goals influence the direction of their behavior to violate rules and regulations in our society [19]. The scope of applications of the SBT was extended to human aspects of information security in recent years. Ifinedo [17] and Sohrabi Safa, Von Solms and Furnell [15] have used the SBT to clarify the breach of information security policies in organizations and explained how different forms of attachment, commitment, involvement, and personal norms influence employees' attitudes towards complying with Organizational Information Security Policies (OISPs). In another study, Safa, Maple, Watson and Furnell [6,20] have applied the SBT to develop an effective and efficient information security collaboration in organizations. In this study, we have developed a new version of the SBT to mitigate insider threats in organizations.

2.2. Theory of Planned Behavior

The justification of human behavior based on subjective norms, attitude, perceived behavioral control, and intention was presented by [12]. Human attitude is an important factor in the formation of behavior and is influenced by environmental factors, education, culture, values, intervention, rules and regulations such as GDPR [21,22]. The TPB has been widely applied in different domains to explain the behavior of adolescents, customers, patients, students, employees, and so on [23,24]. An attitude develops a positive sense about behavior, and has a learning tendency to assess things, people, objects, issues, and events in a particular way. The attitude and behavior change when the assessment results in a change in behavior [25]. Implicit attitudes unconsciously affect our behavior and beliefs, but in implicit attitudes, we are consciously aware that effective factors influence our beliefs and behavior [26]. Personal experience, different training methods, and observations can

also affect our attitude [27]. Organizational factors such as job satisfaction, job security, and administrative support create a pleasant sense and affect employees' attitudes [28]. The sense of commitment and the reasons for the commitment are other important factors that affect employees' attitudes [29]. These factors will be explored more in the following sections. The definitions of attitude, perceived behavioral control, intention, subjective norms, and other influential factors have been presented in Table 1. The conceptual framework has been covered with the SBT and TPB. Figure 1 shows the model.

Table 1. A Summary of Effective Factors.

	Factors	Description
1	Job Satisfaction (JS)	JS is a measure of employees' contentedness with their job and originates from respect, recognition, fair compensation, and motivation.
2	Job Security (JSe)	JSe refers to the probability of keeping a job. In other words, there is a small chance of losing a job.
3	Organizational Support (OS)	OS refers to the employees' perception that the organization cares about their well-being and values their contribution.
4	Affective Commitment (AC)	AC shows that employees feel that they are part of the organization and like it. A good working experience is an important factor in this regard.
5	Continuance Commitment (CC)	CC refers to the cost of leaving an organization for the employee. The result of cost and benefit assessment motivates employees to stay and maintain their commitment or leave the organization.
6	Normative Commitment (NC)	NC refers to the employees' decision without any external obligation. NC is built upon duties and values.
7	IS Training (IST)	IST refers to all types of information security training that an employer provides for its employees.
8	Personal Norms (PN)	PN refers to the values and moral obligations in which an individual believes.
9	Attitude (AT)	AT refers to an individual's tendency about feeling, emotion, position, that they have about a person or things.
10	Perceived Behavioral Control (PBC)	PBC refers to having a perception of the ability to complete a task. In this study—the ability to avoid any information security risk, considering legitimate access to systems and data.
11	Subjective Norms (SN)	SN refers to the belief that a group of people or important persons will approve and support a particular behavior.
12	Intention (IN)	IN refers to an assumption that explains a commitment to carrying out an action now or in the future.
13	Insider Threat (ITh)	ITh refers to abuse of legitimate access to systems and data for financial benefits or other reasons.

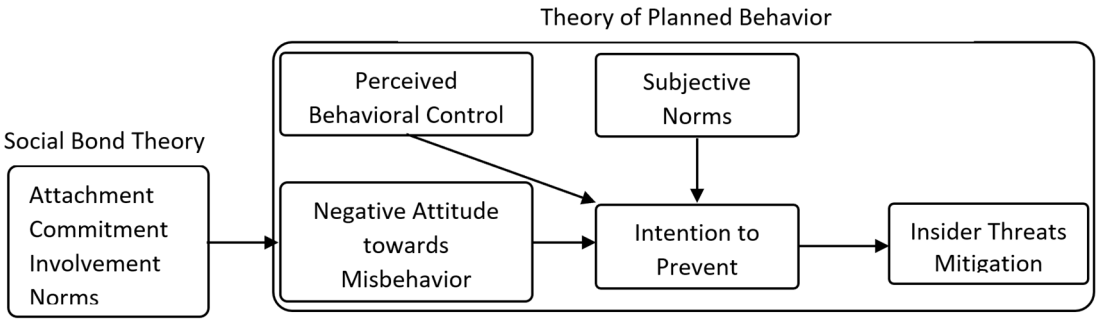

Figure 1. The Conceptual Framework.

2.3. Research Gap and Justification

Although insider threats have garnered significant attention in the field of information security, existing studies have taken a narrow view, particularly in their focus on aspects such as individual differences, technical safeguards, or awareness revision.

Insider threats have been receiving increasing attention in the field of information security; however, much of the existing research has taken a fairly narrow view, primarily focusing on aspects such as individual deterrence, technical safeguards, or raising awareness. For example, Safa, Maple, Furnell, Azad [3] examined how punishment and prevention might be effective, while Johnston and Warkentin [30] investigated how fear can motivate people to follow security policies. While these approaches offer some insight, they tend to overlook the broader picture, particularly the organizational and psychological factors that influence how employees behave in real-world, complex environments.

Another issue is that many studies rely on just one theoretical approach, which can limit their ability to explain what is going on in depth. For instance, Siponen, Mahmood and Pahnila [31] based their work entirely on deterrence theory, and Ifinedo [10] focused only on cognitive elements. What is still not fully understood is how workplace factors—like job satisfaction, perceived support from the organization, and emotional commitment—interact with how individuals think and behave when it comes to security.

This study aims to fill that gap by bringing together the Social Bond Theory (SBT), which looks at deviant behavior through the lens of attachment, commitment, and involvement, and the Theory of Planned Behavior (TPB), which focuses on attitudes, perceived control, and social expectations. By combining these two perspectives, we provide a fresh framework for understanding how both relationships and intentions influence employees' decisions regarding security. To the best of our knowledge, no other study has taken this integrated approach to insider threats from such a broad organizational perspective, making our research both relevant and original.

3. Conceptual Model and Hypotheses

This research aims to examine the effect of different forms of attachment, commitment, involvement, and employees' beliefs and norms on mitigating insider threats. This study presents a conceptual model based on two main theories that, although different, complement each other quite well: the Social Bond Theory (SBT) and the Theory of Planned Behavior (TPB). The SBT [11] essentially argues that the stronger someone's emotional ties, whether to people, their work, or the organization, the less likely they are to engage in behavior that harms that system. In workplaces, this plays out as lower risks of insider threats when people feel satisfied with their job, supported by the company, or emotionally invested in their role.

The TPB [12] takes a more psychological route. It states that people's actions are influenced by their thoughts about the behavior, the level of control they feel they have, and what they believe others expect of them. So, when someone has received solid security training, believes in doing the right thing, and feels capable of following through, that shapes what they are likely to do.

By blending these two theories, we are not just examining behavior from a technical or surface level; we are delving into both the emotional and intentional layers of why employees might act securely or not. The hypotheses presented in the next section are based on this combined theoretical perspective.

3.1. Job Satisfaction

Job satisfaction points to the extent to which a member of staff is motivated to complete his/her tasks, duties, and feel content [32]. In simple words, people feel positively or

negatively about their jobs. Job facets play an important role in the formation of job satisfaction. The nature of work, working environment, salary, supervision, and career advancement play important roles in the formation of job satisfaction [33]. Eliyana, Ma'arif and Muzakki [34] have mentioned personal achievement and recognition as other vital factors in the formation of job satisfaction.

It has been acknowledged that satisfied employees perform on a higher level, engage more with their tasks and roles, and are more productive [35]. There is a strong relationship between job satisfaction and job performance [36]; satisfied employees do not jeopardize their job by creating risks such as damaging organizational reputation, intellectual properties, and breach of rules and regulations in an organization [37]. In addition, job satisfaction is an intrinsic motivation which is supported by motivation theory, but considering other effective factors, we made the decision to use the Social Bond Theory to have a more robust framework and solution. Based on this justification, we have concluded that satisfied employees do not engage in breaching information security and privacy considerations in their daily activities. The hypothesis below has been presented based on the above-mentioned justifications:

H1: *Job satisfaction positively influences employees' attitude towards mitigation of insider threats in organizations.*

3.2. Job Security

Insider threats originate from current and former employees that are the most challenging subject to detect and prevent [38]. Job security can be an intrinsic motivational factor to avoid any misconduct such as violation of information security policies and procedures that mitigate information security breaches in organizations [39]. When employees feel their job is unstable, they may experience stress, resentment, or fear which can lead to malicious behavior, be more susceptible to external coercion such as espionage or bribery, rationalize unethical actions such as stealing data before an anticipated layoff [40]. On the other hand, job security promotes trust and engagement. Job security demonstrates higher organizational loyalty, reducing the likelihood of violating trust. The above explanations motivated us to present the hypothesis below:

H2: *Job security positively influences employees' attitude towards mitigation of insider threats in organizations.*

3.3. Organizational Support

Perceived organizational support is about employees' belief that their organization values their well-being, their contributions, and organizational attention to socioemotional needs [41]. Organizational support creates a reciprocity process that positively influences productivity in an organization; the support motivates employees to reciprocate favorable treatments and rewards [42]. Organizational support attracts the attention of experts during the investigation of employees' commitment to an organization and vice versa. They realized that factors such as respect and care, benefits such as medical support and wages play important roles in this process, and influence moral aspects of employees' behavior [43]. Employees who feel supported are more emotionally attached to the organization. This loyalty and trust reduce the likelihood of malicious behavior such as data theft or sabotage. Supportive environments foster a culture of integrity and accountability. Employees are more likely to align with the organization's values and policies, including information security protocols. High morale reduces grievances, resentment, and frustration—common precursors to insider threats. Satisfied employees are less likely to act out in destructive ways [44].

Garcia, Amarnani, Bordia and Restubog [45] studies have revealed that problem-solving, continuous learning, teamwork, and active work are important factors in organizational support. Ding, Hao, Li, Liang [46] have divided organizational support into reinforcement support and inhibitive support; their studies show that sense of belonging plays a mediating role in this process that enhances employees' performance. This performance and productivity cover all aspects of employees' behavior. That is why we have assumed that organizational support influence employees' behavior towards the mitigation of insider threats.

H3: *Perceived organizational support positively influences employees' attitude towards the mitigation of insider threats in organizations.*

3.4. Affective Commitment

Commitment is not a unidimensional construct; rather, it has been widely conceptualized in organizational behavior literature as consisting of three distinct components: affective, continuance, and normative [47]. Affective commitment reflects emotional attachment to the organization, continuance commitment relates to perceived costs of leaving, and normative commitment stems from a sense of moral obligation. This multidimensional approach offers a deeper understanding of how various motives for staying in an organization influence behavior. By incorporating all three types, this study offers a more comprehensive analysis of how various commitment forms contribute to mitigating insider threats.

Commitment shows individuals' dedication and loyalty to an organization and has been acknowledged as an important variable for understanding employee behavior in an organization [48]. Commitment positively affects individuals' motivation and the achievement of organizational goals. Committed persons spend more energy and time on their successful career and endeavor to gain reputation, personal achievement, and high-status jobs in their workplace [49]. A committed person does not jeopardize their situation by breaking rules and regulations or spoil their career aspirations. Ifinedo [17] showed that organizational commitment significantly influences employees' attitude towards complying with Organizational Information Security Policies (OISPs). Ng [50] discussed employees' loyalty and divided their organizational commitment into affective, normative and continuance commitment. A commitment profile is a combination of these three components. Jahyun, Myung-Seong and Kim [51] investigated the information security climate and its effect on complying with OISPs. The results of their study revealed that affective commitment and normative commitment influence employees' compliance with OISPs.

Employees with affective commitment feel that they fit into the organization and are satisfied with their job. They are interested in staying at their organization and they identify with the organizational goals and feel valued [52]. Affective commitment originates from a positive emotional feeling about an organization. Employees with affective commitment are a great asset for companies [53]. Employees with affective commitment accept organizational aims and values and show more effort. That is why we postulated that employees with affective commitment try to protect organizational information assets and do not create any threat to these assets.

H4: *Affective commitment positively influences employees' attitude towards the mitigation of insider threats.*

3.5. Continuance Commitment

Employees need to continue their job to influence their continuance commitment. In other words, a lack of work alternatives and remuneration are the underlying reasons for

their commitment. Continuance commitment is driven by side-bets [54]. An employee needs to stay with an employer because of his or her salary, and fringe benefits would not improve if he or she moves to another organization. Continuance commitment refers to perceived costs associated with leaving [55]. Employees who perceive a high personal cost in losing their job are less likely to engage in risky or malicious behaviors, including data theft or sabotage. The fear of job loss due to policy violations can act as a deterrent. Continuance-committed employees may be more likely to follow rules, even if reluctantly, because non-compliance could jeopardize their position. These individuals may be risk-averse and prefer to avoid any action (intentional or not) that could be interpreted as a breach of trust or policy [56]. Therefore, employees can be led to continuance commitment; in this situation, they try to follow organizational aims and plans. That is why we conjecture that:

H5: *Continuance commitment positively influences employees' attitude towards mitigation of insider threats.*

3.6. Normative Commitment

Normative commitment originates from an internalized sense of duty or obligation to remain with the organization [47]. This form of commitment often arises when employees perceive that the organization has invested time, resources, or trust in their development, such as through training or mentorship. Employees may feel that leaving would betray this investment and disrupt the organization's operations or security posture, especially if their role is tied to critical knowledge or processes.

In the context of information security, such departures may create vulnerabilities due to gaps in institutional knowledge, risk assessment capabilities, or policy enforcement. Awareness of this potential impact can evoke guilt or moral discomfort, particularly in employees who value integrity and responsibility. As shown in Meyer and Parfyonova [52], this sense of guilt is a key feature of normative commitment. Employees with strong normative commitment are therefore more likely to align their actions with organizational values and avoid engaging in behavior, such as insider threats, that could harm the organization. For these reasons, we assume that:

H6: *Normative commitment positively influences employees' attitude towards mitigation of insider threats.*

3.7. IS Training

It has been acknowledged that information security training mitigates information security breaches in organizations [57]. The outputs of their research demonstrate the appropriate design of training in the domain of information security. Guidelines in web-based information security training and evaluating the training in terms of effectiveness are important characteristics of information security training. Other studies show that information security training has a positive effect on employees' attitudes and significantly reduces the effects of social engineering and phishing attacks in organizations [58]. The awareness program also positively influences the effectiveness of the information response team in organizations [59].

All organizations have to comply with General Data Protection rules and regulations (GDPR) from 25 of May 2018 in the UK; the violation of GDPR can have up to a twenty million pound fine. Information security training is widely regarded as a crucial organizational tool for enhancing employee awareness, shaping attitudes, and promoting compliance with security policies. It plays a crucial role in equipping staff with the knowledge and behavioral skills necessary to prevent security violations, including insider threats. This

training influences users' and employees' attitudes toward the mitigation of information security breaches [60].

Abawajy [27] studies show that information security knowledge transfer approaches such as contextual training, web-based training materials, embedded training, game-based, text-based, and video-based training approaches influence employees' attitudes in organizations and mitigate different types of information security breaches. Based on the abovementioned explanations we have postulated that:

H7: *Information security training positively influences employees' attitudes towards mitigation of insider threats in organizations.*

3.8. Personal Norms

Social and personal norms influence employees' beliefs and their sense of responsibility. In addition, the rewards which come from social norms affect individuals norms and their behavior [61]. Therefore, employees' norms originate from their values that affect their behavior.

Although personal norms are not part of the original core constructs of the Theory of Reasoned Action (TRA) or the Theory of Planned Behavior (TPB), several studies have extended TPB to include personal norms when investigating moral, ethical, or socially responsible behaviors [62,63]. In the context of information security, personal norms represent internalized moral obligations that can significantly influence employees' compliance intentions and behavior. Li, Zhang and Sarathy [62] showed that personal norms affect compliance with Internet use policies in organizations. Because of its potential to impact information security threats within organizations, ISC is an important behavior. The following hypothesis is presented based on the aforementioned explanations:

H8: *Personal norms positively influence employees' attitude towards mitigation of insider threats in organizations.*

3.9. Attitude

In this study, "attitude" refers specifically to employees' evaluations of and disposition toward mitigating insider threats through secure and responsible information security behavior. This includes attitudes toward complying with information security policies, protecting organizational data, and preventing the misuse of access privileges. According to the TPB [12], such attitudes, whether favorable or unfavorable, play a critical role in shaping individuals' behavioral intentions. An individual's attitude depends on their evaluation; if the evaluation changes, so will their attitude. It is therefore dynamic in nature how attitudes are formed. The factors such as personal norms, involvement attachment, and commitment influence employees' attitude and behavior [64]. Safa, Maple, Watson and Furnell [20] showed that characteristics such as attachment, commitment, and personal norms affect individuals' behavior towards collaboration in information security in organizations. That is why we have presented the below hypothesis:

H9: *Attitude positively influences employees' intention towards the mitigation of insider threats in organizations.*

3.10. Perceived Behavioral Control

Perceived behavioral control (PBC) refers to the sense of ability to conduct or control a specific behavior [65]. In this sense, beliefs can influence behavior. An individual's perception of the ease or difficulty of engaging in a particular behavior is indicative of their perceived control over it. Employees with more control in their behavior engage

more with their jobs [66]. Workman, Bommer and Straub [67] showed that employees with more control in their behavior follow more information security policies. We attempted to demonstrate that PBC has an important impact on employees' intention to decrease information security risks at work.

H10: *Perceived behavioral control positively influences employees' intention towards mitigation of insider threats in organizations.*

3.11. Subjective Norms

Subjective norms refer to the social normative beliefs and the expectations of important referents. Particularly, the strength of each normative belief is weighted by the motivation to perform the behavior [68]. Shibchurn and Yan [69] showed that subjective norms have a significant effect on the expose of information on social networks through perceived usefulness and perceived risk. In another study, Tamjidyamcholo, Bin Baba, Shuib and Rohani [70] asserted that social norms play an essential role in information security knowledge sharing in virtual communities. The perception of social pressure to engage in a behavior may also be subject to subjective norms. For instance, when the majority of employees in a department comply with organizational information security policies and procedures, this motivates other members to comply with these policies and procedures. Complying with GDPR is another behavior that influences other members to avoid the violation of the rules and regulations. That is why we assume that subjective norms positively influence employees' behavior to mitigate insider threats.

H11: *Subjective norms positively influence employees' intention towards the mitigation of insider threats in organizations.*

3.12. Intention

An intention means having a full understanding of a plan and having foresight to accomplish a goal. Individuals' desires and beliefs influence their intention and behavior [71]. Astington [72] explains in his study that there is a relationship among individuals' intention, behavior with desire, and beliefs to achieve a goal; the goal is the protection of information assets in the organization here. These links show the intentional chain and depict how desires cause intention, and, consequently, behavior. The intention is one of the elements in the TPB which has been used by several experts to explain complying with information security policies [15,31]. In another research, Shropshire, Warkentin and Sharma [73] used intention to show the adoption of information security behavior in organizations. Park, Gu, Leung and Konana [74] showed that intention plays a vital role in information-sharing in SMEs. In this research, we postulated that intention to information security protection significantly mitigates insider threats in organizations.

H12: *Intention to protect information positively influences employees' behavior towards the mitigation of insider threats in organizations.*

Figure 2 shows all factors, hypotheses, and theories in a concise form.

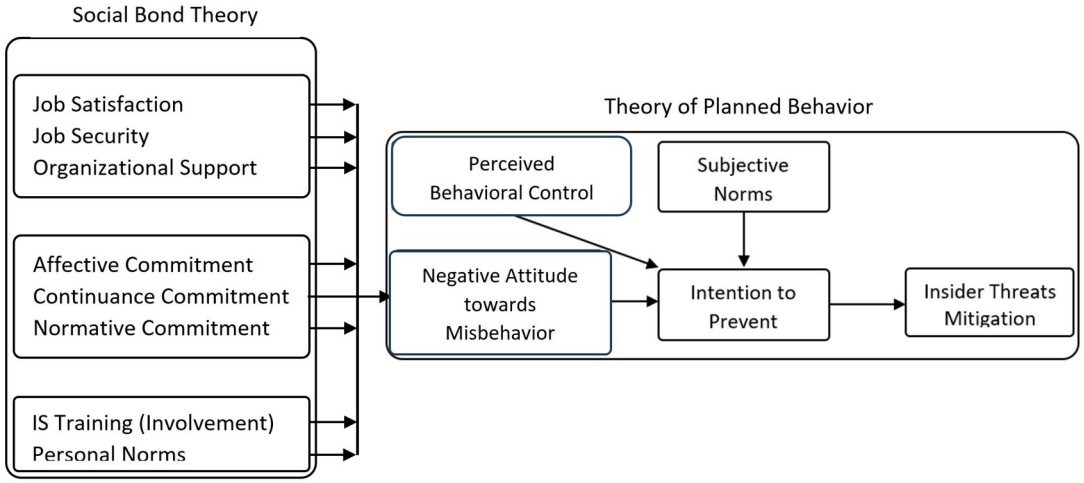

Figure 2. The model with more details.

4. Research Methodology

Insider threats are serious challenges in organizations and this research endeavors to investigate the factors which mitigate insider threats. A conceptual framework has been presented on the basis of a review of the literature. Two essential theories support the presented model—the Social Bond Theory and the Theory of Planned Behavior. The solution has been presented based on effective factors and the two basic theories in the form of conceptual framework. To improve the reliability and validity of the model, the Delphi method has been applied and the model with explanations about its effective factors have been sent to experts in this domain in two rounds. The framework has been improved based on experts' feedback. The experts were high-ranking cybersecurity academic and industry experts with more than 10 years of experience in the domain of cyber security. Two of them approved the effective factors which were extracted from a systematic literature review, and two of them suggested three more effective factors. The research team accepted their suggestion, and they were added to the model.

To show the reliability and validity of the model, data have been collected through a questionnaire. Confirmatory Factor Analysis (CFA) helped us to be sure whether the model and hypotheses which we have developed are correct. Structural equation modelling has been considered as a good approach to investigate the relationships between different type of factors in such a model [75]. IBM AMOS 20 was used to investigate the relationships between different factors. The Chi-square with degrees of freedom, goodness of fit index (GFI), the comparative fit index (CFI), the adjusted goodness of fit index (AGFI), and the root mean square error of approximation (RMSEA) were applied to investigate the testing of the hypotheses [76]. The results have been discussed in the last section. IBM SPSS Amos 29 was used for data analysis.

4.1. Data Collection

Employees of several companies whose main activity was business, providing educational services, and insurance provided the data. The questionnaire was developed considering previous similar studies. Based on a Likert scale, the responses ranged from (1) strongly disagree to (5) strongly agree. Participants were informed of the purpose of the research and then asked to fill out a questionnaire based on their knowledge and experience. The research group considered their consent very important. They were presented with the questionnaire after they indicated their consent to participate in the study. The data collected will remain confidential and will only be made available to academics in this project. A pilot test of the questionnaire with 38 participants was conducted to ensure

that the questions were comprehended, applicable, and could be interpreted uniquely by the participants. Our pilot test provided us with an opportunity to observe the participants' emotions, hesitations, and descriptions they requested for the items. Their feedback caused us to revise and rephrase a few words and sentences so that they would better understand the questions. The demography of participants can be seen in Table 2. The measurement items for each construct in the questionnaire were primarily adapted from validated scales in prior studies. Constructs such as job satisfaction, job security, organizational support, and commitment types were derived from the Three-Component Model of Organizational Commitment [47] and further informed by studies such as Eliyana, Ma'arif and Muzakki [34] and Naqvi and Bashir [54]. Items related to IS training, personal norms, attitude, perceived behavioral control, subjective norms, and intention were adapted from the TPB scale [12], Siponen, Mahmood and Pahnila [31], and Ifinedo [10]. Minor modifications in wording were made for contextual alignment with the domain of insider threats and information security. Table 3 includes references next to each construct indicating the original source. Various items were used to measure the various constructs in the final version of the questionnaire. It consisted of 56 questions. The formation of the constructs, including references, is evident in Table 3.

Table 2. Respondents' characteristics.

Measure	Items	Frequency	Percent
Gender	Male	336	69.78
	Female	146	30.22
Age	21 to 30	160	29.98
	31 to 40	195	32.92
	41 to 50	85	25.06
	Above 50	42	12.04
Position	Employee	438	92.38
	Chief employee	32	5.16
	Management	12	2.46
Work experience	1 to 2 years	128	16.71
	3 to 5 years	248	51.35
	Above 5 years	106	31.94
Education	Diploma	38	7.86
	Bachelor	306	71.25
	Master	114	18.92
	PhD	24	1.97

Table 3. The Statistical Measures.

Construct		Items	Mean	Std Dev	CFA Loading	Composite Reliability
Job Satisfaction [34,47]	JS1	My employer recognizes my effort.	4.32	0.762	0.632	0.736
	JS2	My employer respects me for my work.	4.02	0.782	0.522	
	JS3	My employer acknowledges my achievements.	3.98	0.746	Dropped	
	JS4	My employer appreciates when I have a good performance.	3.68	0.764	0.672	
	JS5	I am happy with my job.	3.42	0.702	0.634	
Job Security [33]	JSE1	I can work in this company for a long time.	4.22	0.729	0.720	0.814
	JSE2	The probability of losing my job is low.	4.26	0.745	0.547	
	JSE3	I can keep my job.	4.02	0.744	0.732	
	JSE4	I am not concerned about losing my job.	3.96	0.782	0.764	

Table 3. *Cont.*

Construct		Items	Mean	Std Dev	CFA Loading	Composite Reliability
Perceived Organizational Support [42]	POS1	My employer cares about my well-being.	4.16	0.762	0.726	0.724
	POS2	My employer values my contribution.	4.02	0.712	0.818	
	POS3	My socioemotional well-being is important to my employer.	3.98	0.854	0.822	
	POS4	My employer provides anything that I need to complete my tasks.	3.68	0.782	Dropped	
Affective Commitment [47,53]	AC1	I try to play an important role in my organization.	3.86	0.722	0.722	0.818
	AC2	I would like to remain a part of this organization.	4.12	0.864	0.621	
	AC3	I have positive emotions regarding my employer.	3.96	0.826	0.742	
	AC4	I help to achieve organizational aims.	4.02	0.724	0.812	
Continuance Commitment [55]	CC1	I am happy with my income in this organization.	4.04	0.716	0.732	0.762
	CC2	I will lose a lot if I leave this organization.	4.16	0.722	0.588	
	CC3	The benefits of staying in this organization outweigh the costs of moving somewhere else.	4.42	0.742	0.742	
	CC4	I have good colleagues in this organization; that is why I will stay here.	3.98	0.762	0.712	
Normative Commitment [52]	NC1	My employer has invested in me, that is why I want to stay here.	4.16	0.782	0.842	0.726
	NC2	My employer rewards to me encourage me to stay here.	3.64	0.728	0.722	
	NC3	My commitment to my employer originates from their care to me.	3.34	0.708	0.763	
	NC4	My colleagues recommend to me to stay here.	4.12	0.804	0.802	
IS Training [58]	IST1	Information security trainings help me to avoid mistakes in this domain.	3.24	0.818	0.732	0.762
	IST2	Information security trainings influence my attitude towards complying with policies and procedures.	3.22	0.752	0.744	
	IST3	Information security trainings help me to reduce information security risks.	4.34	0.822	0.726	
	IST4	Information security trainings influence my understanding about risk and make me act better.	3.64	0.722	0.642	
Personal Norms [62,63]	PN1	Protection of organizational information assets is very important to me.	4.62	0.742	0.722	0.742
	PN2	I believe that information security breaches have negative consequence for my organization.	4.22	0.712	0.818	
	PN3	Protection of information is our duty.	3.98	0.844	0.822	
	PN4	I am aware of GDPR; that is why I should not commit information security misconduct.	3.88	0.742	Dropped	
	PN5	COISPs are necessary to protect information assets.	4.12	0.736	0.714	

Table 3. *Cont.*

Construct		Items	Mean	Std Dev	CFA Loading	Composite Reliability
Attitude [12,31]	AT1	Protection of organizational information assets is a good practice.	3.96	0.849	0.722	0.748
	AT2	I should protect organizational information as much as I can.	3.42	0.715	0.754	
	AT3	Protection of information is a wise practice.	4.32	0.832	0.796	
	AT4	Protection of information is a valuable action.	3.64	0.742	0.662	
Perceived Behavioral Control [12,67]	PBC1	I have the necessary knowledge to protect organizational information.	4.26	0.762	0.842	0.842
	PBC2	I have the ability to protect our data and information.	3.34	0.768	0.782	
	PBC3	Protection of organizational information is not a tough task.	3.64	0.708	0.726	
	PBC4	I have the tools that I need to protect information in my organization.	4.12	0.864	0.801	
Subjective Norms [12,69]	SN1	We should protect organizational information.	3.86	0.716	0.824	0.728
	SN2	My line manager believes that information protection is a valuable culture.	3.94	0.780	0.812	
	SN3	The management team in my company have a positive view on information protection.	4.26	0.822	0.709	
	SN4	My colleagues encourage me to protect organizational information.	4.12	0.726	0.718	
Intention to Mitigate Risks [12,73]	IN1	I should protect organizational information.	3.98	0.643	0.942	0.754
	IN2	I am willing to protect organizational information.	4.22	0.546	0.722	
	IN3	I help my colleagues to protect organizational information.	4.32	0.782	Dropped	
	IN4	I am committed to protecting organizational information.	3.48	0.844	0.732	
	IN5	I put an effort into reducing information security risks.	4.24	0.702	0.62	
Insider Threats Mitigation [15]	ITM1	I do not abuse my legitimate access to systems.	4.48	0.826	0.712	0.762
	ITM2	I do not transfer organizational data outside of my organizations.	4.38	0.628	0.629	
	ITM3	I do not violate my organizational data protection regulations because of financial benefits.	3.62	0.639	0.598	
	ITM4	Protection of data about intellectual properties is important to me.	4.24	0.802	0.706	
	ITM5	Protection of data about organizational plans is important to me.	4.02	0.724	0.704	

4.2. Demography

The research team helped to collect data by sending emails to participants and distributed questionnaires. Five hundred thirty-five questionnaires were distributed, of which three hundred and eighty-four were online and one hundred fifty-one were paper-based questionnaires. Forty-six online questionnaires and seven paper-based questionnaires were ignored due to the same answer given to all of the questions or incomplete answers. At the end, four hundred and eighty-two questionnaires were selected for data analysis. Table 2 shows the characteristics of the participants.

5. Results

The variables, such as job satisfaction, job security, organizational support, commitment, and so forth, which are unobservable, we have measured with several independent variables. These variables were used to develop the measurement and structural models which are two important parts of structural equation modelling (SEM). Using the measurement model, we can see how the measured variables relate to latent variables. Prior to fitting the measurement model to the data, the indicators (observed variables) were examined for reliability and validity. A structural model was used to test the relationships between the latent variables. For these types of studies, structural equation modelling is the best method [76].

5.1. Measurement Model

The SEM has been mentioned as an appropriate technique for this kind of research, but we need to be sure that the distribution of data is normal, before applying this approach. The standard kurtosis and skewness showed that the distribution of the data is normal—between +2 and −2 [76]. Effective factors such as job satisfaction and job security and so on which cannot be measured directly are measured with several other items. To be sure that effective factors are measured correctly, factor loading has been used that shows a correlation between the main factor and the items which measure them. Convergent validity is demonstrated by the factor loading of the measurement variables. Factor loadings bigger than 0.5 show a reasonable convergent validity [76]. So, the items with a factor loading smaller than 0.5 were ignored from the conceptual model. The measure of Cronbach's Alpha depicts internal consistency. For each construct, Cronbach's Alpha exceeded 0.7, indicating that the constructs were compositely reliable [77].

In addition to factor loadings and reliability, Average Variance Extracted (AVE) was calculated for each construct to confirm convergent validity. AVE values exceeding 0.5 indicated that the latent constructs explained more than half of the variance in their respective indicators, consistent with the recommended thresholds.

Furthermore, to evaluate discriminant validity, we applied the Fornell–Larcker criterion, which compares the square root of each construct's AVE to its correlations with other constructs. Each construct's AVE square root exceeded its inter-construct correlations, confirming discriminant validity and indicating that the constructs were empirically distinct.

The factor loading and internal consistency have been presented in Table 3.

As these constructs are independent and unique, a dimensional grouping depicts convergent and discriminant validity. However, to examine the discriminant and convergent validity of the factors, we linked constructs together. Based on the research model, convergence validity was examined to see whether it gives any clue as to the relationships between two related items. According to discriminant validity, there is no relationship between those constructs that should not be related, based on the conceptual framework [76]. The correlation measured between every two factors has been presented in Table 4.

The grouping of independent factors in the form of conceptual framework shows discriminant validity. The correlations between all pairs show that a relationship between all pairs exists based on the framework.

Table 4. Correlation between different constructs.

		Mean	SD	1	2	3	4	5	6	7	8	9	10	11
1	JS	4.06	0.98	0.618										
2	JSE	3.98	0.88	0.202	0.558									
3	POS	4.01	1.05	0.401	0.312	0.496								
4	AC	4.02	1.14	0.309	0.286	0.312	0.589							

Table 4. *Cont.*

		Mean	SD	1	2	3	4	5	6	7	8	9	10	11
5	CC	3.98	1.02	0.289	0.404	0.470	0.265	0.488						
6	NC	3.92	1.08	0.286	0.225	0.368	0.367	0.208	0.472					
7	IST	3.89	0.98	0.264	0.421	0.242	0.236	0.319	0.369	0.818				
8	PN	4.26	1.16	0.312	0.421	0.211	0.361	0.449	0.336	0.325	0.885			
9	AT	4.12	1.26	0.198	0.430	0.396	0.267	0.203	0.295	0.375	0.402	0.799		
10	PBC	4.08	0.89	0.208	0.552	0.503	0.438	0.366	0.403	0.298	0.358	0.379	0.689	
11	SN	3.96	1.02	0.226	0.416	0.467	0.496	0.497	0.246	0.261	0.403	0.323	0.556	0.723
12	IN	4.28	0.98	0.488	0.622	0.622	0.524	0.562	0.622	0.466	0.444	0.622	0.425	0.524
13	ITM	4.22	0.88	0.742	0.802	0.742	0.426	0.664	0.642	0.562	0.624	0.421	0.624	0.642

5.2. Testing Structural Model

SEM can investigate relationships between the main factors and the items which measure them, where errors in statistical analysis are reduced. SEM can test our conceptual framework and its hypotheses with different measures. The acceptable measures and the measures which originate from our model have been presented in Table 5.

Table 5. Model fit indices.

Fit Indices	Model Value	Acceptable Standard
χ^2	1002.89	-
χ^2/Df	1.92	<2
GFI	0.924	>0.9
AGFI	0.946	>0.9
CFI	0.961	>0.9
IFI	0.944	>0.9
NFI	0.928	>0.9
RMSEA	0.074	<0.08

Table 6 shows the outputs of data analysis. The results revealed that all hypotheses were accepted except H1 and H5.

Table 6. The results of the hypotheses testing.

Path			Standardized Estimate	*p*-Value	Results
JS	→	AT	0.722	0.012	Support
JSE	→	AT	0.658	0.004	Support
POS	→	AT	0.302	0.061	Not Supported
AC	→	AT	0.604	0.012	Support
CC	→	AT	0.403	0.027	Not Supported
NC	→	AT	0.698	0.001	Support
IST	→	AT	0.716	0.002	Support
PN	→	AT	0.662	0.009	Support
AT	→	IN	0.546	0.009	Support
PBC	→	IN	0.724	0.001	Support
SN	→	IN	0.702	0.002	Support
IN	→	ITM	0.802	0.002	Support

The results of the data analysis show that the relationship between Perceived Organizational Support and employees' attitude, and between Continuance Commitment are not significant. Therefore, H5 and H3 have been rejected.

6. Contribution and Implementation

Information security in organizations covers different subjects such as complying with information security organizational policies and procedures, information security awareness and training, conscious care behavior in information security, information security response team and recovery, and so on. We have focused on information security insider

threats in this study due to its importance and its negative consequences for organizations. Although insider threats have recently attracted the attention of experts in the field of information security, there is a paucity of research on how we can mitigate insider threats in organizations. Deterrent factors such as severity and certainty of punishment, social bond factors such as creating attachment, commitment, involvement, and personal norms, as well as motivation to avoid information security misconduct are approaches that have been presented in previous studies. In this research, we have investigated the effect of organizational factors as an essential solution among different approaches to mitigate insider threats in organizations.

This study can be justified based on different theories; crime prevention theory explains that increasing the effort and risk for misbehavior, decreasing rewards that come from crime or misconduct, reducing excuses and provocations can mitigate information security misconduct [3]; development of job satisfaction and job security, IS training, and organizational support decrease employees' excuses and provocations for conducting information security misconduct. This study can be justified by motivation theory (intrinsic and extrinsic factors) as well. The above-mentioned factors can mitigate employees' motivation to avoid any action that jeopardizes information security in an organization. In other words, job satisfaction, job security, organizational support, and IS training motivate employees to protect information assets in an organization. These findings can be applied in any organization regardless of its size and type.

This study opens a new window for academics in the field of human aspects of information security. This investigation revealed that organizational factors and appropriate management approaches that pay attention to job satisfaction and security, organizational support, and proper training can influence the protection of information assets in organizations.

This study shows that information security has managerial, organizational, psychological, educational, and social aspects that should be considered besides technological aspects of information security.

7. Conclusions, Limitation, and Future Works

It has been acknowledged that we should use multiple approaches to overcome different challenges in the domain of information security. Previous studies have shown that managerial, psychological, educational, social, cultural, and economic factors play important roles in the field of human aspects of information security. However, there is a gap in the research about the effect of organizational factors on the mitigation of insider threats. This study has used confirmatory relationships by synthesizing several theories that explain human behavior in order to present a new approach that mitigates insider threats in organizations. The outputs of this research show that creating job satisfaction, job security, affective and normative commitment, IS training, and negative personal beliefs about information security misconduct affect employees' attitude and their intention and finally mitigate the risk of insider threats in organizations. Job satisfaction, job security, and appropriate training create loyalty and attachment in employees and have a positive effect on their attitude and intention to protect information assets in organizations. This study shows that managerial, educational, social, and psychological factors play important roles in the field of human aspects of information security.

Our previous studies showed that information security knowledge sharing (increasing awareness), conscious care behavior in information security (less risky behavior), information security collaboration, and complying with organizational information security policies and procedures (mitigation of risk) are different approaches that decrease the risk

of information security breaches in organizations. This study shows that the appropriate development of organizational factors also mitigates insider threats in organizations.

We faced several limitations in this study. The data were collected from several companies in the UK. The generalization of findings can be improved by collecting more data from different organizations. We had two or three email addresses for some participants; to be sure that they received our request to answer our questionnaire, we sent the questionnaire to all their email addresses, but fortunately, the proportion of these participants was less than one percent.

This study conceptualized a solution to mitigate insider threats in organizations; other experts can further develop this approach by investigating other organizational factors and using other theories that justify employees' behavior in this domain. Further investigation can be conducted using criminal, social, managerial, and educational theories, and to try to change employees' behavior. We believe that this study sheds a light on the formation of insider threats and provides a solution to mitigate insider threats for academics and managers in the field of information security.

Author Contributions: Both authors contributed equally. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: This study has ethical approval in 2024 from the University of Warwick-FTMSc—R_45D16BQDiOut4YN.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are available on request from the corresponding author due to confidentiality that has been mentioned in data collection forms.

Conflicts of Interest: There is no conflict of interest.

References

1. Colabianchi, S.; Costantino, F.; Nonino, F.; Palombi, G. Transforming threats into opportunities: The role of human factors in enhancing cybersecurity. *J. Innov. Knowl.* **2025**, *10*, 100695. [CrossRef]
2. Padayachee, K. Aspectising honeytokens to contain the insider threat. *Inf. Secur. IET* **2015**, *9*, 240–247. [CrossRef]
3. 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]
4. Al-Matari, O.M.M.; Helal, I.M.A.; Mazen, S.A.; Elhennawy, S. Adopting security maturity model to the organizations' capability model. *Egypt. Inform. J.* **2020**, *22*, 193–199. [CrossRef]
5. Szczepaniuk, E.K.; Szczepaniuk, H.; Rokicki, T.; Klepacki, B. Information security assessment in public administration. *Comput. Secur.* **2020**, *90*, 101709. [CrossRef]
6. 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]
7. 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]
8. Nasir, A.; Arshah, R.A.; Hamid, M.R.A.; Fahmy, S. An analysis on the dimensions of information security culture concept: A review. *J. Inf. Secur. Appl.* **2019**, *44*, 12–22. [CrossRef]
9. Mutlutürk, M.; Wynn, M.; Metin, B. Phishing and the Human Factor: Insights from a Bibliometric Analysis. *Information* **2024**, *15*, 643. [CrossRef]
10. 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]
11. Hirschi, T. *Causes of Delinquency*; Routledge: London, UK, 2017.
12. Ajzen, I. The theory of planned behavior. *Organ. Behav. Hum. Decis. Process.* **1991**, *50*, 179–211. [CrossRef]
13. Chen, C.-F.; Xu, X.; Arpan, L. Between the technology acceptance model and sustainable energy technology acceptance model: Investigating smart meter acceptance in the United States. *Energy Res. Soc. Sci.* **2017**, *25*, 93–104. [CrossRef]

14. Sepasgozar, S.M.E.; Hawken, S.; Sargolzaei, S.; Foroozanfa, M. Implementing citizen centric technology in developing smart cities: A model for predicting the acceptance of urban technologies. *Technol. Forecast. Soc. Change* **2019**, *142*, 105–116. [CrossRef]
15. Sohrabi Safa, N.; Von Solms, R.; Furnell, S. Information security policy compliance model in organizations. *Comput. Secur.* **2016**, *56*, 70–82. [CrossRef]
16. 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]
17. 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]
18. Dang-Pham, D.; Pittayachawan, S.; Bruno, V. Exploring behavioral information security networks in an organizational context: An empirical case study. *J. Inf. Secur. Appl.* **2017**, *34*, 46–62. [CrossRef]
19. 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 Pt B*, 447–459. [CrossRef]
20. Safa, N.S.; Maple, C.; Watson, T.; Furnell, S. Information security collaboration formation in organisations. *IET Inf. Secur.* **2017**, *12*, 238–245. [CrossRef]
21. Evans, M.; Maglaras, L.A.; He, Y.; Janicke, H. Human behaviour as an aspect of cybersecurity assurance. *Secur. Commun. Netw.* **2016**, *9*, 4667–4679. [CrossRef]
22. Safa, N.S.; Von Solms, R. An information security knowledge sharing model in organizations. *Comput. Hum. Behav.* **2016**, *57*, 442–451. [CrossRef]
23. Plotnikoff, R.C.; Costigan, S.A.; Karunamuni, N.; Lubans, D.R. Social cognitive theories used to explain physical activity behavior in adolescents: A systematic review and meta-analysis. *Prev. Med.* **2013**, *56*, 245–253. [CrossRef] [PubMed]
24. Hau, Y.S.; Kim, B.; Lee, H.; Kim, Y.-G. The effects of individual motivations and social capital on employees' tacit and explicit knowledge sharing intentions. *Int. J. Inf. Manag.* **2013**, *33*, 356–366. [CrossRef]
25. Hepler, J. A good thing isn't always a good thing: Dispositional attitudes predict non-normative judgments. *Personal. Individ. Differ.* **2015**, *75*, 59–63. [CrossRef]
26. Glock, S.; Kovacs, C. Educational Psychology: Using Insights from Implicit Attitude Measures. *Educ. Psychol. Rev.* **2013**, *25*, 503–522. [CrossRef]
27. Abawajy, J. User preference of cyber security awareness delivery methods. *Behav. Inf. Technol.* **2014**, *33*, 237–248. [CrossRef]
28. Hussain, M.; Mubarak, S. MEASURING HUMAN RESOURCE ATTITUDE USING ORGANISATIONAL THEORY OF RELATIONSHIP: THE WAY FORWARD. *Int. J. Manag. Stud.* **2021**, *28*, 57–88. [CrossRef]
29. Jigjiddorj, S.; Zanabazar, A.; Jambal, T.; Semjid, B. Relationship Between Organizational Culture, Employee Satisfaction and Organizational Commitment. *SHS Web Conf.* **2021**, *90*, 02004. [CrossRef]
30. Johnston, A.C.; Warkentin, M. Fear appeals and information security behaviors: An empirical study. *MIS Q.* **2010**, *34*, 549–566. [CrossRef]
31. Siponen, M.; Mahmood, M.A.; Pahnila, S. Employees' adherence to information security policies: An exploratory field study. *Inf. Manag.* **2014**, *51*, 217–224. [CrossRef]
32. Bezdrob, M.; Šunje, A. Transient nature of the employees' job satisfaction: The case of the IT industry in Bosnia and Herzegovina. *Eur. Res. Manag. Bus. Econ.* **2021**, *27*, 100141. [CrossRef]
33. Bhardwaj, A.; Mishra, S.; Kumar Jain, T. An analysis to understanding the job satisfaction of employees in banking industry. *Mater. Today Proc.* **2021**, *37*, 170–174. [CrossRef]
34. Eliyana, A.; Ma'arif, S. Job satisfaction and organizational commitment effect in the transformational leadership towards employee performance. *Eur. Res. Manag. Bus. Econ.* **2019**, *25*, 144–150. [CrossRef]
35. Mowbray, O.; Campbell, R.D.; Disney, L.; Lee, M.; Fatehi, M.; Scheyett, A. Peer support provision and job satisfaction among certified peer specialists. *Soc. Work Ment. Health* **2021**, *19*, 126–140. [CrossRef]
36. Sarwar, S.; Abugre, J. *The Influence of Rewards and Job Satisfaction on Employees in the Service Industry*; Centre for Business & Economic Research: London, UK, 2013; pp. 22–32.
37. Ahmad, K.Z.B.; Jasimuddin, S.M.; Kee, W.L. Organizational climate and job satisfaction: Do employees' personalities matter? *Manag. Decis.* **2018**, *56*, 421–440. [CrossRef]
38. Inayat, U.; Farzan, M.; Mahmood, S.; Zia, M.F.; Hussain, S.; Pallonetto, F. Insider threat mitigation: Systematic literature review. *Ain Shams Eng. J.* **2024**, *15*, 103068. [CrossRef]
39. Jeong, M.; Zo, H. Preventing insider threats to enhance organizational security: The role of opportunity-reducing techniques. *Telemat. Inform.* **2021**, *63*, 101670. [CrossRef]
40. Palmer, V. Systematic literature review on insider threat: Is the Australian aviation industry complacent or just not understanding insider threat? *J. Air Transp. Res. Soc.* **2025**, *4*, 100060. [CrossRef]
41. Wen, J.; Huang, S.; Hou, P. Emotional intelligence, emotional labor, perceived organizational support, and job satisfaction: A moderated mediation model. *Int. J. Hosp. Manag.* **2019**, *81*, 120–130. [CrossRef]

42. Akgunduz, Y.; Alkan, C.; Gök, Ö.A. Perceived organizational support, employee creativity and proactive personality: The mediating effect of meaning of work. *J. Hosp. Tour. Manag.* **2018**, *34*, 105–114. [CrossRef]
43. Loi, R.; Lin, X.; Tan, A.J.M. Powered to craft? The roles of flexibility and perceived organizational support. *J. Bus. Res.* **2019**, *104*, 61–68. [CrossRef]
44. Dang-Pham, D.; Thompson, N.; Ahmed, A.; Maynard, S. Shadow Information Security Practices in Organizations: The role of information security transparency, overload, and psychological empowerment. *Comput. Secur.* **2025**, *156*, 104538. [CrossRef]
45. Garcia, P.R.J.M.; Amarnani, R.K.; Bordia, P.; Restubog, S.L.D. When support is unwanted: The role of psychological contract type and perceived organizational support in predicting bridge employment intentions. *J. Vocat. Behav.* **2021**, *125*, 103525. [CrossRef]
46. Ding, K.; Hao, S.; Li, G.; Liang, X.; Chen, T.; Feng, X. The impact of organizational support on employee performance. *Empl. Relat. Int. J.* **2020**, *42*, 166–179. [CrossRef]
47. Meyer, J.P.; Allen, N.J. A three-component conceptualization of organizational commitment. *Hum. Resour. Manag. Rev.* **1991**, *1*, 61–89. [CrossRef]
48. TorlakTorlak, N.G.G.; BudurBudur, T.; KhanKhan, N.U.S.U.S. Links connecting organizational socialization, affective commitment and innovative work behavior. *Learn. Organ.* **2024**, *31*, 227–249. [CrossRef]
49. Reid, M.F.; Riemenschneider, C.K.; Allen, M.W.; Armstrong, D.J. Information Technology Employees in State Government: A Study of Affective Organizational Commitment, Job Involvement, and Job Satisfaction. *Am. Rev. Public Adm.* **2008**, *38*, 41–61. [CrossRef]
50. Ng, T.W.H. The incremental validity of organizational commitment, organizational trust, and organizational identification. *J. Vocat. Behav.* **2015**, *88*, 154–163. [CrossRef]
51. Jahyun, G.; Myung-Seong, Y.; Kim, D.J. A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate. *Prof. Commun. IEEE Trans.* **2014**, *57*, 286–308. [CrossRef]
52. Meyer, J.P.; Parfyonova, N.M. Normative commitment in the workplace: A theoretical analysis and re-conceptualization. *Hum. Resour. Manag. Rev.* **2010**, *20*, 283–294. [CrossRef]
53. Cakı, N.; Asfuroglu, L.; Erbas, O. The Relationship between the Level of Attachment in Romantic Relations, Affective Commitment and Continuance Commitment towards Organization: A Field Research. *Procedia Econ. Financ.* **2015**, *26*, 1007–1013. [CrossRef]
54. Naqvi, S.M.M.R.; Bashir, S. IT-expert retention through organizational commitment: A study of public sector information technology professionals in Pakistan. *Appl. Comput. Inform.* **2015**, *11*, 60–75. [CrossRef]
55. Powell, D.M.; Meyer, J.P. Side-bet theory and the three-component model of organizational commitment. *J. Vocat. Behav.* **2004**, *65*, 157–177. [CrossRef]
56. Gottschalck, N.; Rolan, L.; Kellermanns, F.W. The continuance commitment of family firm CEOs. *J. Fam. Bus. Strategy* **2023**, *14*, 100568. [CrossRef]
57. Abraham, S.; Chengalur-Smith, I. Evaluating the effectiveness of learner controlled information security training. *Comput. Secur.* **2019**, *87*, 101586. [CrossRef]
58. Caputo, D.D.; Pfleeger, S.L.; Freeman, J.D.; Johnson, M.E. Going spear phishing: Exploring embedded training and awareness. *IEEE Secur. Priv.* **2014**, *12*, 28–38. [CrossRef]
59. Bartnes, M.; Moe, N.B.; Heegaard, P.E. The future of information security incident management training: A case study of electrical power companies. *Comput. Secur.* **2016**, *61*, 32–45. [CrossRef]
60. Safa, N.S.; Mitchell, F.; Maple, C.; Azad, M.A.; Dabbagh, M. Privacy Enhancing Technologies (PETs) for connected vehicles in smart cities. *Trans. Emerg. Telecommun. Technol.* **2020**, *33*, e4173. [CrossRef]
61. Costa, A.I.d.A. Conceptualization and measurement of personal norms regarding meal preparation. *Int. J. Consum. Stud.* **2013**, *37*, 596–604. [CrossRef]
62. Li, H.; Zhang, J.; Sarathy, R. Understanding compliance with internet use policy from the perspective of rational choice theory. *Decis. Support Syst.* **2010**, *48*, 635–645. [CrossRef]
63. Ajzen, I.; Fishbein, M. Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychol. Bull.* **1977**, *84*, 888. [CrossRef]
64. Pattinson, M.; Parsons, K.; Butavicius, M.; McCormac, A.; Calic, D. Assessing information security attitudes: A comparison of two studies. *Inf. Comput. Secur.* **2016**, *24*, 228–240. [CrossRef]
65. Jeon, S.; Kim, Y.G.; Koh, J. An integrative model for knowledge sharing in communities-of-practice. *J. Knowl. Manag.* **2011**, *15*, 251–269. [CrossRef]
66. Reitz, H.J.; Jewell, L.N. Sex, Locus of Control, and Job Involvement. H. Joseph Reitz, Faculty, University of Florida, and Linda N. Jewell, Faculty, University of California-Irvine. Abstract from Academy of Management Journal, March 1979, p. 72. *Int. Exec.* **1979**, *21*, 17–18. [CrossRef]
67. Workman, M.; Bommer, W.H.; Straub, D. Security lapses and the omission of information security measures: A threat control model and empirical test. *Comput. Hum. Behav.* **2008**, *24*, 2799–2816. [CrossRef]

68. Pi, S.-M.; Chou, C.-H.; Liao, H.-L. A study of Facebook Groups members' knowledge sharing. *Comput. Hum. Behav.* **2013**, *29*, 1971–1979. [CrossRef]
69. Shibchurn, J.; Yan, X. Information disclosure on social networking sites: An intrinsic–extrinsic motivation perspective. *Comput. Hum. Behav.* **2015**, *44*, 103–117. [CrossRef]
70. Tamjidyamcholo, A.; Bin Baba, M.S.; Shuib, N.L.M.; Rohani, V.A. Evaluation model for knowledge sharing in information security professional virtual community. *Comput. Secur.* **2014**, *43*, 19–34. [CrossRef]
71. Lee, W.-K. The temporal relationships among habit, intention and IS uses. *Comput. Hum. Behav.* **2014**, *32*, 54–60. [CrossRef]
72. Astington, J. *The Child's Discovery of the Mind*; Harvard University Press: Cambridge, MA, USA, 1993.
73. Shropshire, J.; Warkentin, M.; Sharma, S. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Comput. Secur.* **2015**, *49*, 177–191. [CrossRef]
74. Park, J.H.; Gu, B.; Leung, A.C.M.; Konana, P. An investigation of information sharing and seeking behaviors in online investment communities. *Comput. Hum. Behav.* **2014**, *31*, 1–12. [CrossRef]
75. Bagozzi, R.P.; Yi, Y. Specification, evaluation, and interpretation of structural equation models. *Acad. Mark. Sci.* **2011**, *40*, 8–34. [CrossRef]
76. Hair, J.F., Jr.; Black, W.C.; Babin, B.J.; Anderson, R.E. *Multivariate Data Analysis*; Pearson Prentice Hall: Upper Saddle River, NJ, USA, 2010; p. 785.
77. Arbuckle, J.L. *Amos 16.0 User's Guide*; SPSS, Inc.: Chicago, IL, USA, 2007.