International Journal of Information Security
https://doi.org/10.1007/s10207-023-00786-9

REGULAR CONTRIBUTION

Fostering information security policies compliance with ISA-95-based framework: an empirical study of oil and gas employees

Rao Faizan Ali[1] · P. D. D. Dominic[2] · Sadaf Hina[3] · Sheraz Naseer[1]

Abstract

Oil and gas (O&G) organizations are progressively being digitalized in order to facilitate substantial information flow to remain competitive in the information age. This critical sector is spearheading the establishment of technical security measures to mitigate information security risks, yet employee behavioral influence remains an ongoing challenge in assuring information security. Existing studies of this domain primarily focus on employee behavior reshaping through multiple psychological theories. However, these studies ignore how these critical infrastructures implement information security. Most such infrastructures follow the International Society of Automation (ISA)-95 levels of automation and implement information security controls in line with these levels. This research paper proposed a theoretical framework to enhance information security policy compliance (ISPC) at level 4 to level 2 automation level in O&G organizations. To support the hypotheses, data were collected from 13 Malaysian O&G organizations. A total of 254 O&G employees participated in the survey and the structural equation modeling technique was used for data analysis. The study confirmed that ISA-95-based organizational governance factors and social bonding could enhance ISPC in O&G organizations. However, risk assessment and involvement factors have shown less support to the notion. For information systems practitioners, this study has shown how to enhance ISPC in O&G organizations through ISA-95-based organizational governance and social bonding.

Keywords Oil and gas organizations · ISA-95 · Organizational governance · Social bonding

1 Introduction

Oil and gas (O&G) organizations are considered process-oriented enterprises. To ensure smooth working processes, O&G organizations follow International Society of Automation (ISA)-95 standard automation guidelines. Most of the organizations in this sector implement information security according to ISA-95 levels of automation [36]. ISA-95 has five levels (4–0) of automation, from business layer to production layer (Fig. 1). On each level, different software and resources are deployed, respectively. For instance, at level 4 enterprise resource and planning (ERPs), at level 3, manufacturing enterprise systems (MES), level 2 supervisory control, and data acquisition (SCADA), level 1 programmable logic controller (PLC), and at level 0 sensors and actuators are deployed [39]. From level 4 to level 2, most of the information security activities require human involvement. Multiple studies suggested that the majority of the security attacks on these critical infrastructures occur due to mistakes from the internal employees [5, 36, 53]. To mitigate human mistakes, almost every critical infrastructure management has established comprehensive information security policies. Still, compliance with these policies is surprisingly low and in certain infrastructures its near to non-existence [5, 36, 53]. Periodically, policymakers and top managers in O&G organizations struggle to successfully implement information security policies by identifying deficiencies and issues in information security policies compliance [5]. However, it is

✉ P. D. D. Dominic
dhanapal_d@utp.edu.my

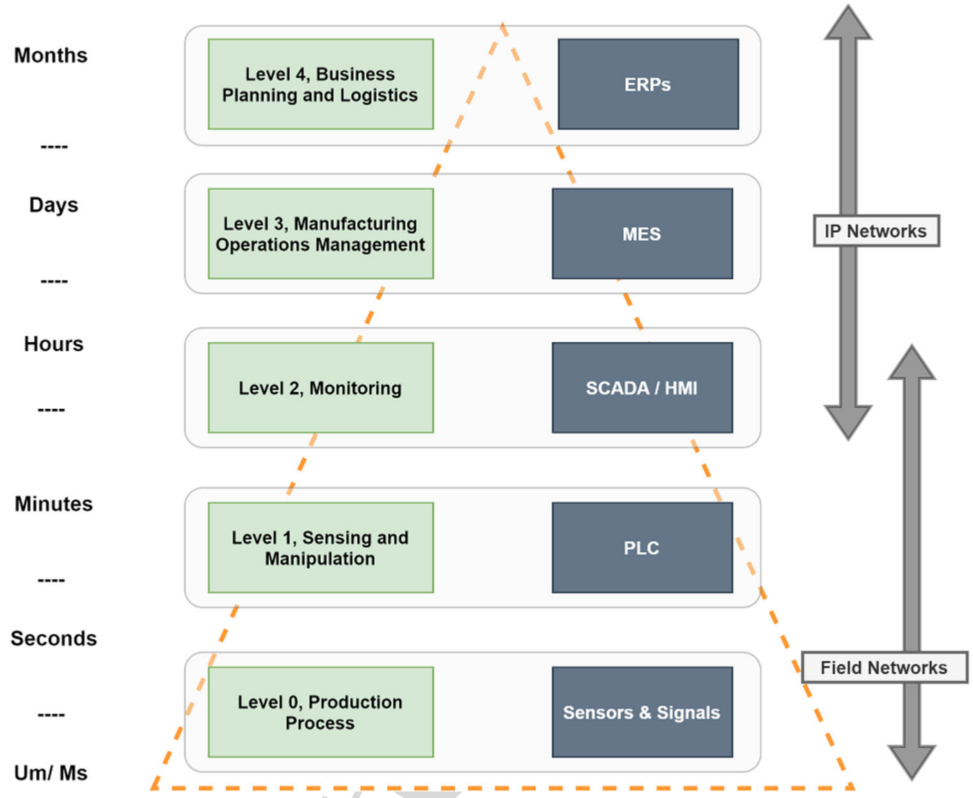
Rao Faizan Ali
faizan.ali@umt.edu.pk

Sheraz Naseer
sheraz.naseer@umt.edu.pk

[1] School of Systems and Technology, University of Management and Technology, Johar Town, Lahore 54782 C-II, Pakistan

[2] Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, 32610 Seri Iskandar, Perak Darul Ridzuan, Malaysia

[3] School of Science, Engineering and Environment, University of Salford, Manchester, UK


Months

Days

Hours

Minutes

Seconds

Um/ Ms
Level 4, Business Planning and Logistics
ERPs
Level 3, Manufacturing Operations Management
MES
Level 2, Monitoring
SCADA / HMI
Level 1, Sensing and Manipulation
PLC
Level 0, Production Process
Sensors & Signals
IP Networks
Field Networks

Fig. 1 ISA-95 levels of automation and O&G information security

essential to understand the factors that can motivate employees for the protection of organizational information assets, realize the need of information security mechanisms, and enhance employees' compliance with information security policies.

Non-compliance with information security policies in O&G organizations is identified by some research studies. Such as Albrechtsen and Hovden [9] and Jaatun et al. [32] in their research on Norwegian O&G organizations, concluded that there is a dire need to investigate the behavioral side of information security and its counter measures in O&G organizations. Likewise, [43] investigated information security problems in oil and gas organizations and demonstrated that O&G organizations have complex organizational structure. It is required to investigate information security lapses at each level of automation in the organization provided by ISA-95. Moreover, [32] found a mistrust issue in the IT staff and control staff of an O&G organization. Although multiple researchers attempted to solve behavioral information security problems in O&G organizations worldwide, still further research is required in certain neglected areas. Most of the studies focused on developed countries O&G organizations, and their findings cannot be generalized to developing countries employees. Furthermore, studies conducted in developed countries tried to solve problems related to information security, scarcely explored behavioral information security on each level of ISA-95.

To fill the aforementioned gaps, this research study focused on information security policies' compliance in Malaysian O&G organizations from Level 4–2 as classified in ISA-95. To enhance ISPC from level 4 to level 2 an overall security control enhancement is needed [4]. Studies suggested that to enhance security controls, organizational governance can play a vital role [5, 26]. Effective organizational governance should provide security education training, in-line security policies and procedures, adequate physical security monitoring at each level, and an enhanced risk assessment regarding information security-related issues [5, 26].

Research suggests that to reshaping employees' behaviors toward information security policies, social bonding is an effective method. Multiple researchers investigated that socially active information security culture leads to better information security policies compliance in organizations [29, 31]. Lack of organizational governance and social bonding among employees result in non-compliant behaviors [31]. Therefore a more holistic approach is required to deal with behavioral non-compliance with security policies in O&G organizations [36, 53].

No previous study has linked the aforementioned constructs to assess ISPC in a single research framework. Furthermore, none of the studies investigated ISA-95-based ISPC approach in a developing country's organizational culture. In brief, to the best of the authors' knowledge, this is

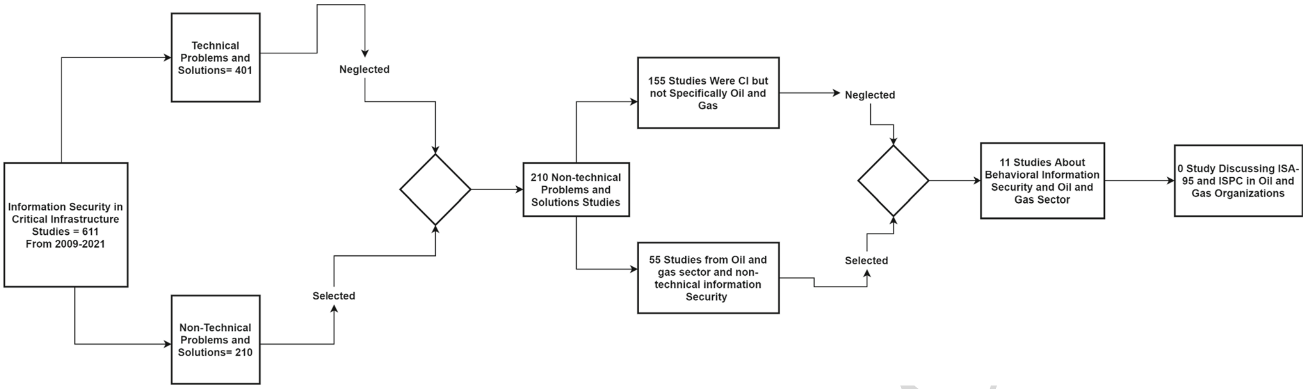

Information Security in Critical Infrastructure Studies = 611 From 2009-2021
Technical Problems and Solutions= 401
Non-Technical Problems and Solutions= 210
Neglected
Selected
210 Non-technical Problems and Solutions Studies
155 Studies Were CI but not Specifically Oil and Gas
55 Studies from Oil and gas sector and non-technical information Security
Neglected
Selected
11 Studies About Behavioral Information Security and Oil and Gas Sector
0 Study Discussing ISA-95 and ISPC in Oil and Gas Organizations

Fig. 2 Systematic literature review (identifying a research gap)

among first studies that attempts to address the ISPC problem for O&G organizations incorporating ISA-95 levels. It is believed that the integration and investigation of these constructs in the developing countries O&G industry will shed more light on the organizational governance, and social behaviors to enhance ISPC. Hence, this paper incorporates to investigate and answer the following research questions.

RQ1: What are the contributions of ISA-95-based organizational governance factors to shape employees' information security behavior to improve information security control in O&G organizations?

RQ2: How enhanced social controls can improve employees' attitude toward information security policies' compliance in O&G organizations?

2 Literature review

A rigorous systematic literature review was conducted on existing studies from 2009 to 2021 to gain a comprehensive insight. A step-by-step systematic literature review is presented in Fig. 2 ISPC and ISA-95 in O&G organizations have been scarcely discussed and analyzed in extant literature; still, some studies discussed behavioral information security in O&G organizations, shown in Table 1.

In a recent study [39], proposed a framework for network anomaly detection in O&G organizations, where the researchers tried to detect network anomalies in O&G industrial level 4 for ISA-95 with a deep learning-based model. Likewise [43] presented a study upon Norwegian O&G

Table 1 Literature review

Authors	Country	Study type	Findings	Limitations
[39]	N/A	Experimental/Technical	Attackers can attack on the O&G network and there is more research required to develop a network anomaly detection technique specifically for O&G sector	Partially related to ISPC, not addressing the behavioral problems related to information security Moreover, tested generic dataset not form O&G
[5]	Malaysia	Quantitative study/Survey research	ISPC can be enhanced with organizational governance and social bonding among employees	Study never discussed ISA-95 levels and implementation
[53]	N/A	Systematic Literature Review	The digitalization of O&G organizations systems will further increase attacks on O&G sector	Articles presented in the study may be not presenting the complete body of knowledge problems
[36]	N/A	Systematic Literature Review	Industry 4.0 is much necessary for O&G digitalization. O&G organizations still lagging to opt information security guidelines	Only systematic Literature Review. Addressing literature problems. Need further quantitative analysis
[54]	Norway	Empirical research	Threat Severity, and adoptive response policy are the predictors of cybercrime incident in O&G organizations	The study is related to O&G but not completely based on the behavioral information security

Table 1 (continued)

Authors	Country	Study type	Findings	Limitations
[40]	United Kingdom	Qualitative Research	Knowledge management systems can prevent operational issues in O&G organizations	The framework was developed using expert opinions but still need to be tested via a quantitative study
[58]	Malaysia	Case Study	There are multiple problems in control management of Malaysian O&G organizations	The study addressed fraud management not fully addressed behavioral information security problems
[43]	Norway	Experimental research	O&G organizations generally know about the risks associated with technology transformation but still investment in incident response capability is very scarce	Research was conducted only for risk assessment and analysis
[3]	Norway	Quantitative study/Survey research	The digital divide between security managers and employees still exists in O&G organizations	Study only discussing security management problems in O&G sector
[32]	Norway	Quantitative study/Survey research	There are some behavioral issues between IT and control staff which can increase the probability of risk	Study conducted in a developed country cannot be implicated on any developing country, moreover only for risk assessment and analysis

organizations and proposed a risk assessment model while adoption of new technology. They have described that O&G organizations generally know about the risks associated with technology transformation, but investment in incident response capability is very scarce. In another study [54] proposed a cyber-crime incident architecture with respect to ISA-95. A criminal case study was tested with the proposed architecture.

Furthermore, [54] provided a holistic, automated framework to handle cybercrime in O&G organizations. Likewise, [40] presented a qualitative study to evaluate knowledge management systems efficacy in O&G information security compliance and proposed a framework for effective information security management using knowledge management systems. In a recent study [53] presented a systematic literature review on incident assessment and attack patterns on O&G organizations. Although the systematic literature review's main theme was to synthesize all the available literature on cybersecurity attacks and their early assessment in O&G organizations, they still claimed that available literature is scarce on O&G and information security compliance.

In the same way, [36] presented a systematic literature review on the adoption of industry 4.0 in O&G organizations. The overall theme of the systematic literature review was to synthesize the available literature and provide the best policies to adopt industry 4.0 in O&G organizations. Their analysis showed that information security is an influential factor and that most O&G organizations compromise the security guidelines. On the other hand, [58] published a study on fraud management systems and detection in O&G organizations. Their study indicated an overall poor management control in O&G organizations in Malaysia.

Similarly, Albrechtsen and Hovden [3] presented an analysis based on their assumption that there is a digital divide that exists in information security managers and employees in O&G organizations. Their study proved that managers think employees are the weakest link, and employees believe that security tasks are irrelevant to their job. In another study, [32] presented a framework for incident response management for O&G organizations and found out that there are some behavioral issues between IT and control staff that can increase the probability of risk. Although there are very few studies available that directly addressing the ISPC issues in O&G organizations. [5] presented a research framework for information security policy compliance enhancement in Malaysian O&G organizations. They have used social bond theory and organizational governance factors to enhance the behavioral compliance among O&G employees.

In the light of related literature this study proposed a research framework to enhance ISPC at level 4–2 of O&G organizations. The conceptual representation of developed approach is illustrated in Fig. 3.

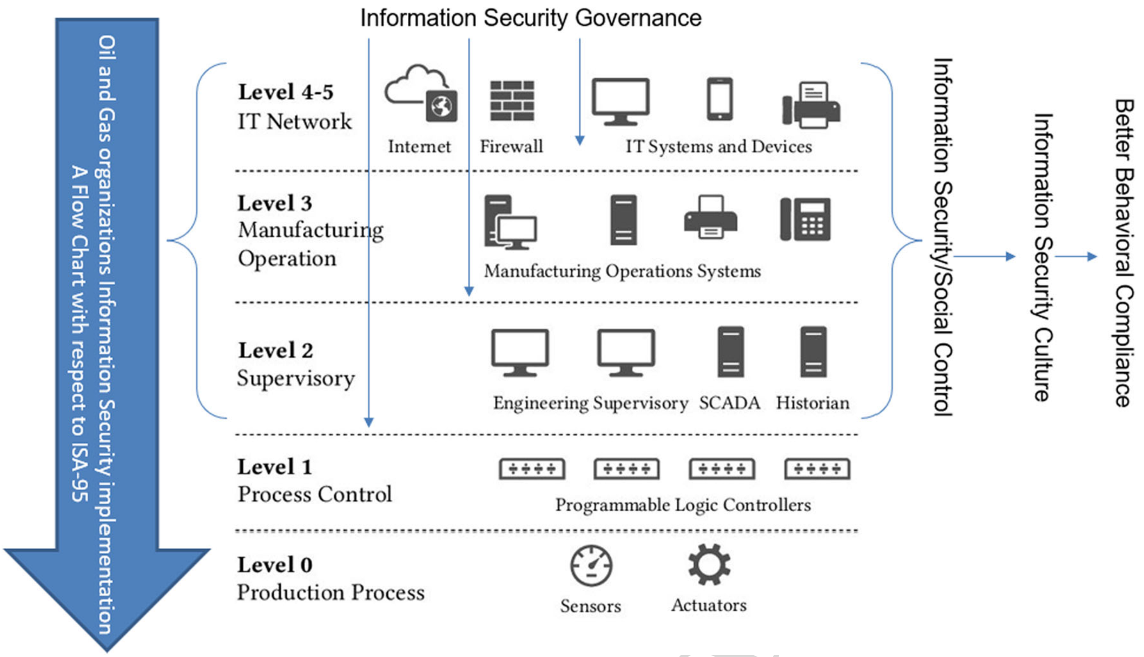

Information Security Governance
Oil and Gas organizations Information Security implementation
A Flow Chart with respect to ISA-95
Level 4-5
IT Network
Internet
Firewall
IT Systems and Devices
Level 3
Manufacturing
Operation
Manufacturing Operations Systems
Level 2
Supervisory
Engineering
Supervisory
SCADA
Historian
Level 1
Process Control
Programmable Logic Controllers
Level 0
Production Process
Sensors
Actuators
Information Security/Social Control
Information Security Culture
Better Behavioral Compliance

Fig. 3 Conceptual illustration of developed approach

3 Research model and hypotheses development

The researcher has performed an exhaustive literature review but very scarce literature available for ISA-95 levels in accordance with information security policies' compliance. The literature support for level 4 of the ISA-95 was available, but very few studies were discussing [40, 54]) factors involved in levels 3 and 2. ISA-95 level 4 describes the business and manufacturing layer, and enterprise resource planning (ERP) software was deployed at that level. As ERPs are special and complex software and for behavioral security of ERP's in-line security policies and procedures and formal information security awareness and training are required. Therefore, the researcher has chosen security policy and procedure and security education, training, and awareness constructs from the literature.

At level 3 of ISA-95, manufacturing and operations management dealt with Manufacturing execution systems (MES). The security of this software also required specialized security awareness and training and a clear policy to follow. Furthermore, a clear security control is also needed at this level as this level is inside the industry and employees who are using MES should know the security ethics. To assess the security at Level 3 of ISA-95 in the oil and gas industry researcher has chosen security policies and procedures, security education training and awareness, and clear security control inside the organizations. Level 2 of ISA-95 deals with monitoring and supervising, and at this level, supervisory control and data acquisition (SCADA) software is deployed. Again level-2 is the operational control of all the organizations' control; a security breach at this level can cause a huge loss. Employees working at this level also need strict physical security monitoring and a critical sense of risk assessment and analysis. For this purpose, the researcher chose physical security monitoring and risk assessment and analysis constructs from the literature and incorporate all these constructs into a single research framework.

ISPC is a behavioral problem and ensuring security policy compliance at root level is considered a difficult task for the management. In this research study, authors proposed that to ensure security policy adherence, O&G organizations must focus on social as well as security controls. However studies suggested social controls can be enhanced by good social bonding among employees and security controls can be enhanced by good security governance in organizations [28]. Four important features are investigated and explored under the umbrella of organizational governance. Providing parodic security education and training programs, establishment of comprehensive security policies, physical security monitoring of resources and timely risk assessment and analysis. In this study, the provision of inclusive resources and facilities to achieve the desired results from each of these factors is characterized as an organizational governance. As shown in Fig. 4, enhanced social and security controls can foster effective information security culture and good information security culture leads to better behavioral compliance with information security policies [48].

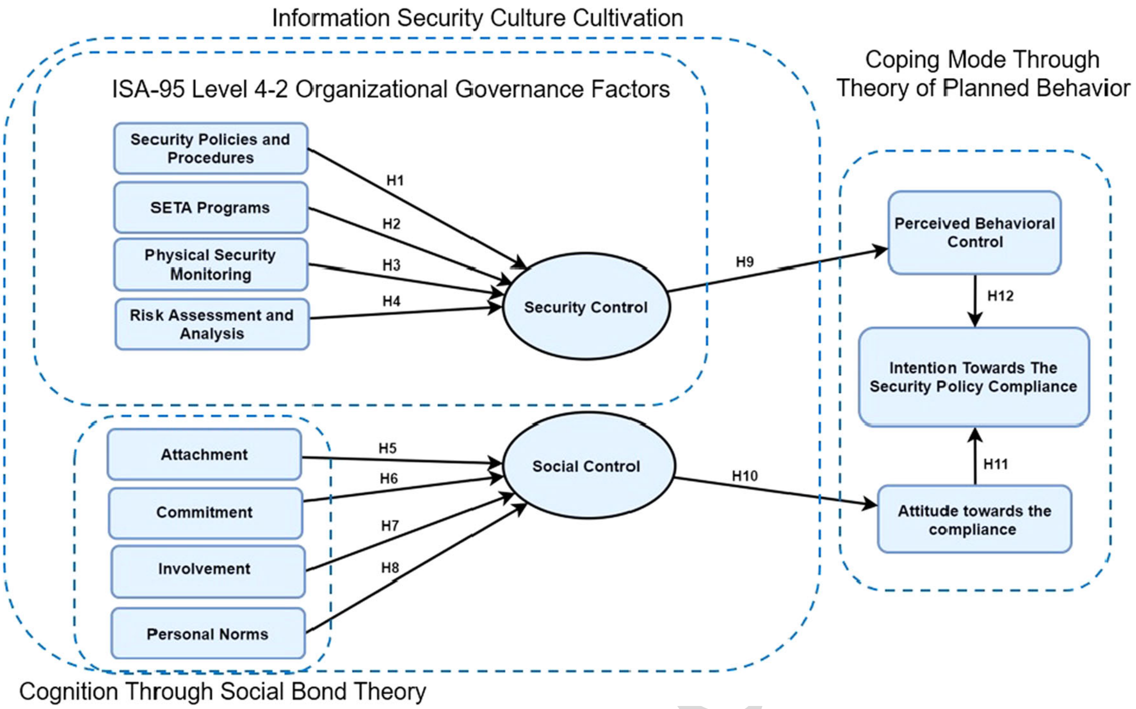

Information Security Culture Cultivation
ISA-95 Level 4-2 Organizational Governance Factors
Security Policies and Procedures
SETA Programs
Physical Security Monitoring
Risk Assessment and Analysis
H1
H2
H3
H4
Security Control
H9
Coping Mode Through Theory of Planned Behavior
Perceived Behavioral Control
H12
Intention Towards The Security Policy Compliance
H11
Attitude towards the compliance
Attachment
Commitment
Involvement
Personal Norms
H5
H6
H7
H8
Social Control
H10
Cognition Through Social Bond Theory

Fig. 4 Research framework

3.1 Organizational governance and security control

This section discussed the aspect of organizational governance and security control management. Researcher proposed an updated organizational governance in the context of ISA-95 levels which comprises of four constructs which are effective on each level of ISA-95.

3.1.1 Information security policies and procedures

Organizations that have proper policies and procedures for information security are effective at directing workers toward positive and complaint security behavior. Research has shown that compliance with organizational security policy can shape and minimize the risk of employee behavior as shown in [51]. However, [14] argued that the information security measures in place had to be understood to workers to provide an important factor in disruption. This ensures that not only must an organization's security policies and procedures be ready, it must also be adhered to and successfully enforced by its management. It is also a crucial factor to consider setting up a policy of ethical behavior [16] to build up the organization's security culture. Unclear policy can lead to poor governance that impedes employees from complying with security enforcement [16]. Thus, this study hypothesizes the following,

H1 Security policy and procedures have significant influence on security control management in the organization.

3.1.2 Security education training and awareness (SETA)

Security awareness is the most essential factor for inculcating the organization's security culture [16,41]. Employees must be aware that their actions must always be in compliance with the security rules and regulations to prevent accidental or deliberate security breaches. Security awareness is still lagging behind in today's technology innovation, whereas threats are growing almost from every angle [26]. In the corporate world, the lack of security knowledge causes non-compliant securitybehavior. In the critical organizational setups, information security is important and needs a great deal of attention from top management [7, 49]. People don't know if they have committed security violations without proper security training and education. Security governance also includes training staff to know what is acceptable and vice versa. Lack of awareness of security can reverse the efforts of successful implementation of information security within the organization [4]. Hence, this study hypothesizes the following.

H2 Security education training and awareness have significant influence on security control management in the organization.

3.1.3 Physical security monitoring

Multiple researchers concluded that to regulate the security conduct of employees in the company, physical security monitoring is necessary [3, 14, 21]. High-level protection includes access cards or biometrics-like finger print or eye retina scan that could control unauthorized users from invading private and sensitive locations. CCTV is also used to document digital proof of any activities of wrongdoing that take place within the organization. For security audit purposes, all users' online activities should be registered. Other forms of information and network security, such as firewalls and encryption, may often be used by the organization to ensure that the infrastructure is secure from technological and human attacks, within or outside the organization. Although it is easier to identify and rectify technical threats, however, human threats have proved to be challenging. The uses of physical monitoring practices are also said to be productive in regulating the employees' security behavior. Hence, this study hypotheses the following.

H3 Physical security monitoring has significant influence on security control management in the organization.

3.1.4 Risk assessment and analysis

Information is secured with the three triads of information system—confidentiality, integrity and availability. [7] argued that organizations that have security risk analysis and assessment management in place are more aware of probable losses due to security breaches. Similarly, Hina et al. [26] argued that despite the information technology governance framework like Control Objectives for Information and Related Technologies (COBIT) and Code of Connection (CoCo) being widely adapted by the organizations globally, these frameworks are found to be lacking in risk assessment and management functions. However, the authors mentioned that ISO 27001 seem to be promising in assessing security risks. With risk analysis assessment and management, organizations will be able to identify areas that are highly critical for information security and improve the security's effectiveness.

H4 Risk assessment and analysis have significant influence on security control management in the organization.

3.2 Employees behavior reshaping and social controls

This section discussed the aspect of employees behavioral reshaping through effective social bonding. Social bonding is a concept first introduced by Hirschi [27], and proposed social bond theory.

3.2.1 Attachment

Attachment refers to the strength of an individual's ties and interactions with his or her social surroundings. Relationships with parents, for example, are crucial, but other institutions and players, such as organizations or co-workers, also have a role [31, 51]. Studies suggested that, an employee who are more attached with organizational tasks will less likely to deviate with organizational policies [50]. Thus, this study hypotheses the following,

H5 An employees' attachment to organizational policies significantly influences social control in an organization.

3.2.2 Commitment

The amount of dedication spent in traditional norms and goals is referred to as commitment. [27] discusses that someone who has previously invested resources, time, and energy in obtaining compliant objectives, stands to lose more from deviant behavior than someone who has put less effort into achieving socially acceptable goals. For instance, an employee who has put in a lot of effort to get promotion, stands to lose more if he or she is rejected than a lazy employee who places less value on organizational tasks. In behavioral information security research multiple researchers empirically tested and concluded that committed employees are less likely to deviate from information security policies [31, 51]. Thus, this study hypotheses the following.

H6 An employees' commitment to organizational policies significantly influences social control in an organization.

3.2.3 Involvement

Travis [27] described involvement as a preventive measure from deviance. For example, a person who is intensively involved in constructive tasks and activities have less time to indulge in negative activities and deviant behaviors. This phenomenon is same in behavioral information security research. As [30, 31] described more involved employees less likely to violate the organizational information security policies. Thus, this study hypothesizes the following.

H7 An employees' Involvement in organizational policies significantly influences social control in an organization.

3.2.4 Personal norms

Personal norm is the last but very important factor of social bond theory. Social bond theory describes personal norms as the validation of mainstream norms of normal society.

It gets more difficult to disobey these values and standards as they become more internalized. In information systems research multiple researchers empirically tested the importance of personal norms toward ISPC [38, 57]. Hence this study proposed the following hypotheses,

H8 An employees' personal norms toward organizational policies significantly influence the social control of an organization.

3.3 Security/social controls and employees behavioral coping

In the light of above-mentioned organizational governance factors discussion this study proposed that, ISA-95-based organizational governance can enhance overall security control of an organization. On the other hand, multiple studies suggested employees of those organization which have effective organizational security control have better perceived behavioral control (Self-efficacy) than those who have poor security controls [6, 39]. Thus this study hypothesizes the following.

H9 Effective Security Control significantly influences employees perceived behavioral control.

Social controls on the other hand are another tool for employee's behavior reshaping, this study proposes that, better social bonding among employees can enhance an overall social control in organization. In the same way, effective social and security controls are very useful in fostering information security culture [15]. Existing literature suggested that, good information security culture leads to information security policies' compliance [48]. Hence this study hypothesizes the following.

H10 Effective social control positively influences employees' attitude toward security policy compliance.

An intention to perform a certain behavior based on various influencing factors leads to actual action for which behavior was conducted [26]. The intention refers to the degree to which people are willing to make efforts to engage in certain activities [2]. The theory of planned behavior categorized these factors as internal instincts (a person's attitude) and external perceived stimulus (subjective norms, perceived behavioral control). The social influence theory distinguishes the types and levels of commitment into the three processes (internalization, identification, and compliance), which will influence behavioral attitudes and intentions [5]. Thus, this study hypothesizes the following,

H11 Employees' attitude significantly influences intention to comply with information security policies of an organization.

H12 Employees perceived behavioral control significantly influences intention to comply with information security policies of an organization.

4 Research methodology

The design of this study is non-experimental and is based on quantitative survey. A questionnaire is used as a main survey instrument to acquire data for hypotheses testing.

4.1 Sample selection

According to existing literature, there are two most common sampling techniques used in studies; non-probability and probability [52]. Due to the absence of a sampling frame of the selected organization's O&G employees working at level 4–2, non-probabilistic sampling was used in this study. This method of sampling means that not all individuals in the population have an equal probability of being picked to participate. Therefore, purposive sampling was used in this research study, as it was very difficult to define the exact population of O&G employees from selected organizations. And the best of the researcher's knowledge there is no census and a complete list of employees working in selected departments of O&G organizations from Level 4–2. This method of sampling is usually used in technology adoption behavior experiments, as the exact number of adapters can be almost impossible to ascertain. As [10, 18] suggested the use of purposive sampling in IS behavior research as the theoretical predictions are more efficient for homogeneous groups. In this study, judgment-based sampling was used as respondents were chosen based on certain criteria.

4.2 Sample size and data collection

The G*Power software was used to calculate the minimum sample size. G*Power is an all-in-one power analysis application widely used in computer and social studies for statistical experiments [17]. For this study researcher followed [24] guidelines for correct sample selection for PLS-SEM. F test of multiple regression is used. According to Hair Jr et al. [24], to calculate the minimum limit of sample size, researcher must incorporate the research model independent variables or the maximum number of arrows pointing at a construct. For this study, the maximum number of arrows pointing at a construct is 4. The alpha value of 0.05, the power of 0.80, and the medium effect size ($f^2 = 0.15$) were used in the test. In most social sciences research, 80% is regarded as the minimum appropriate value [20, 24]. With the aforementioned values, the minimum sample size suggested by G*Power was 85. However, the research model for this study

Table 2 Full collinearity results

SETA	SPP	PSM	RAA	SCO	ATC	COM	INV	PN	SOC	ATT	ISPC
2.31	1.485	2.311	2.412	1.552	1.427	1.982	1.788	2.43	2.623	1.025	1.985

is complex and the researcher wants to acquire more statistical power for this research. As [34] stated that, SEM is a large sample technique and a small sample size may lead to certain errors (e.g. standard errors for latent construct effects). A total of 620 online questionnaires were distributed. Total, 254 usable responses were received with a response rate of 41%. This response rate is deemed acceptable as the domain and sector are very sensitive and questions are related to information security regarding personal and organizational practices [30, 31].

4.3 Measurement items

The measurement items were adopted from multiple studies such as Security Policies and Procedures (SPP = 5 items) adopted from [11, 26]). Security, Education, Training, and Awareness (SETA = 5 items) adopted from [26]. Physical Security Monitoring (PSM = 5 items) adopted from Abdul Hamid et al. [1]. Risk Assessment and Analysis (RAA = 3 items) adopted from [42]. Overall Security Control (SCO = 4 items) adopted from Abdul Hamid et al. [1]. Attachment (ATC = 4 items) adopted from [31]. Commitment (COM = 4 items) adopted from [30]. Involvement (INV = 3 items) adopted from [49, 51]. Personal Norms (PN = 4 items) adopted from [31]. Overall Social Control (SOC = 4 items) adopted from [28]. Attitude (ATT = 4 items) adopted from [26]. Perceived behavioral control (PBC = 4 items) adopted from Rajab et al. [44]. Information Security Policy Compliance (ISPC = 4 items) adopted from [29].

5 Results and analysis

Since the data in this study came from a single source, common method bias could be a potential issue, despite the fact that a few methodological precautions were considered in place before the questions were distributed, therefore a full collinearity test was executed. Full collinearity test provides scales whether any constructs had variance inflation factor (VIF) values of 3.3 or higher [35]. The pathological VIFs for all constructs range from 1.025 to 2.623, suggesting that common method bias was not a serious concern in this analysis; full collinearity results are presented in Table 2.

Table 3 Demographic analysis results

Demographic variable	Categories	Frequency (n = 254)	Percentage (%)
Gender	Male	170	67
	Female	84	33
Age (range in years)	20–30	88	35
	31–40	74	29
	41–50	52	20
	51–60	40	16
Education	Undergraduate	140	55
	Graduate	114	45
Years of experience	1–5	120	47
	6–15	75	30
	16–25	32	13
	26–35	27	10
Information Technology Competence	Low-moderate	112	44
	High-very high	142	56
Daily usage of computers (hours)	4–7	87	34
	8–11	139	55
	More than 11	28	11
Existence of ISPs	Yes	242	95
	No	12	5
Awareness of ISPs	Not aware	13	5
	Somewhat aware	157	62
	Very much aware	84	33

5.1 Demographic analysis

Table 3 shows the demographic profile of the respondents who took part in this research of information security policy compliance in Malaysian O&G organizations. For this study, 35% of the respondents belong to the 20–30 age categories. Moreover, 55% of the employees completed an undergraduate degree. The results also indicated that employees with 1–5 years of experience are more participative than other age groups. A large proportion is aware of security policy (62%) and 56% had high information and communications technology competency.

5.2 Measurement model analysis

Smart PLS 3.3 was used to test the research framework for this analysis [47]. The measurement model (validity and reliability of the measures) and the structural model were investigated using [8] two-stage analytical procedures (testing the hypothesized relationships). According to Table 4, the Cronbach alpha values in this study ranged from 0.803 to 0.923, which meet [22]'s recommended threshold. On the other hand, as a result of its shortcomings, McNeish [37] proposed the Composite Reliability Index as an alternative reliability measure. Table 4 shows that the composite reliability for all constructs surpassed the minimum cut-off value of 0.7, with a range of 0.872–0.917 for each category of results. These findings suggest that the measurement model was reliable enough.

5.2.1 Convergent validity

In contrast to indicators measuring other constructs, convergent validity refers to the degree to which individual indicators represent the constructs [55]. The Average Variance Extracted (AVE) is used to determine Convergent Validity. The AVE value should be greater than 0.5, explaining at least 50% of the variation in the given indicators [13, 24]. The AVE value is computed using the PLS Algorithm in SmartPLS 3.3. For each category of results, all constructs had AVE values greater than 0.5. Table 4 displays the complete measurement model results.

Table 4 Convergent validity

Constructs	Items	Loadings	Reliability and validity			
			Cronbach's Alpha > 0.7	rho_A > 0.7	CR > 0.7	AVE > 0.5
Security policies and procedures (SPP)	SPP1	0.760	0.842	0.844	0.888	0.613
	SPP2	0.808				
	SPP3	0.771				
	SPP4	0.774				
	SPP5	0.800				
Security education training and awareness (SETA)	SETA1	0.821	0.825	0.837	0.877	0.589
	SETA2	0.789				
	SETA3	0.689				
	SETA4	0.825				
	SETA5	0.702				
Physical security monitoring (PSM)	PSM1	0.759	0.852	0.855	0.895	0.630
	PSM2	0.842				
	PSM3	0.748				
	PSM4	0.835				
	PSM5	0.781				
Risk assessment and analysis (PSM)	RAA1	0.886	0.865	0.866	0.917	0.787
	RAA2	0.888				
	RAA3	0.888				
Security Control (SCO)	SCO1	0.862	0.822	0.825	0.883	0.656
	SCO2	0.762				
	SCO3	0.729				
	SCO4	0.877				
Attachment (ATC)	ATC1	0.867	0.867	0.878	0.915	0.729
	ATC2	0.821				
	ATC3	0.862				
	ATC4	0.864				
Commitment (COM)	COM1	0.792	0.791	0.796	0.865	0.615
	COM2	0.710				
	COM3	0.817				

Table 4 (continued)

Constructs	Items	Loadings	Reliability and validity			
			Cronbach's Alpha > 0.7	rho_A > 0.7	CR > 0.7	AVE > 0.5
	COM4	0.813				
Involvement (INV)	INV1	0.889	0.851	0.851	0.909	0.770
	INV2	0.865				
	INV3	0.878				
Personal norms (PN)	PN1	0.813	0.803	0.808	0.872	0.631
	PN2	0.794				
	PN3	0.704				
	PN4	0.858				
Social control (SOC)	SOC1	0.818	0.815	0.817	0.914	0.702
	SOC2	0.725				
	SOC3	0.693				
	SOC4	0.796				
Attitude (ATT)	ATT1	0.754	0.794	0.796	0.866	0.619
	ATT2	0.789				
	ATT3	0.769				
	ATT4	0.831				
Perceived behavioral control (PBC)	PBC1	0.795	0.826	0.832	0.884	0.657
	PBC2	0.803				
	PBC3	0.782				
	PBC4	0.860				
Intention to comply with information security policy (ISPC)	ISPC1	0.795	0.817	0.820	0.880	0.647
	ISPC2	0.803				
	ISPC3	0.782				
	ISPC4	0.860				

5.2.2 Discriminant validity

The heterotrait–monotrait ratio of correlations, HTMT technique, developed by [25], is used to assess discriminant validity in this analysis [34]. indicates that if the HTMT value is greater than 0.85, discriminant validity issues exist. As shown in Table 5, none of the respective constructs violate HTMT 0.85 while using the PLS algorithm, implying that construct validity is defined in the measurement model. As a result, all the reliability and validity criteria for this analysis have been met. The data can then be analyzed further for structural measurements.

5.3 Structural model assessment

The bootstrapping technique is used to generate results for each path relationship in the framework, to test the hypotheses. In PLS, bootstrapping is a nonparametric test that involves repeated random sampling with substitution from the original sample to generate a bootstrap sample and achieve standard errors for hypothesis testing [23]. Similarly [13] recommended bootstrapping with 5000 resamples when it came to the amount of resamples. For the constructs in this analysis, 13 hypotheses have been created. *t*-Statistics for all paths are created using the SmartPLS 3.3 bootstrapping feature to measure the significance level. The bootstrapping is set to 5000 subsamples, 0.05 significance stage, and one-tailed test. For the one-tailed test, the critical values for a significance level of 1% (= 0.01), 5% (= 0.05), and 10% (= 0.1) are 2.33, 1.645, and 1.28, respectively. Ramayah [45] indicated that the value of route coefficients has a standardized value between − 1 and + 1, according to the findings in Table 5 (values from − 0.004 to 0.646). According to Hair Jr et al. [24], estimated path coefficients close to + 1 indicate strong positive relationships, while estimated path coefficients closer to 0 indicate weaker relationships.

Next, the *t*-test results show that relationships have a *t*-value of greater than 1.645, indicating that they are meaningful at the 0.05 level of significance at 5000 subsamples. Security education training and awareness ($\beta = 0.351$, $t =$

Table 5 Discriminant validity

Latent construct	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)
1. SETA	–												
2. SPP	0.501	–											
3. PSM	0.455	0.602	–										
4. RAA	0.521	0.521	0.655	–									
5. SCO	0.501	0.301	0.519	0.521	–								
6. ATC	0.601	0.552	0.508	0.452	0.566	–							
7. COM	0.452	0.532	0.525	0.421	0.531	0.521	–						
8. INV	0.325	0.455	0.523	0.523	0.518	0.594	0.511	–					
9. PN	0.369	0.623	0.322	0.555	0.355	0.455	0.362	0.523	–				
10. SOC	0.559	0.355	0.456	0.528	0.451	0.485	0.451	0.458	0.355	–			
11. ATT	0.658	0.452	0.632	0.451	0.452	0.623	0.365	0.522	0.365	0.451	–		
12. PBC	0.623	0.366	0.562	0.521	0.485	0.511	0.558	0.335	0.651	0.552	0.325	–	
13. ISPC	0.521	0.455	0.542	0.362	0.521	0.510	0.596	0.385	0.452	0.491	0.582	0.456	–

Table 6 Structural model assessment

Hypotheses	Path	Beta-value	Std Error	*p*-value	*t*-value	BCI LL	BCI UL	Q^2	f^2	R^2	Result
H1	SPP → SCO	0.181	0.074	0.018	2.102	0.158	0.121	–	0.031	–	Supported
H2	SETA → SCO	0.351	0.085	0.000	3.223	0.223	0.401	–	0.104	–	Supported
H3	PSM → SCO	0.296	0.074	0.001	2.563	0.118	0.362	0.352	0.079	0.631	Supported
H4	RAA → SCO	0.058	0.089	0.189	0.867	−0.253	3.253	–	0.004	–	Not supported
H5	ATC → SOC	0.175	0.078	0.003	2.724	0.152	2.654	0.334	0.056	0.741	Supported
H6	COM → SOC	0.451	0.023	0.001	5.693	0.231	0.431	–	0.187		Supported
H7	INV → SOC	0.091	0.181	0.175	1.038	−0.198	0.250	–	0.008		Not supported
H8	PN → SOC	0.136	0.037	0.036	1.789	0.191	0.223	–	0.017		Supported
H9	SCO → PBC	0.675	0.021	0.000	10.391	0.152	0.419	0.221	0.838	0.453	Supported
H10	SOC → ATT	0.800	0.019	0.000	19.704	0.301	0.590	0.351	0.823	0.639	Supported
H11	ATT → ISPC	0.574	0.033	0.000	9.553	0.152	0.413	–	0.682	–	Supported
H12	PBC → ISPC	0.375	0.018	0.000	5.965	0.122	0.425	0.395	0.292	0.791	Supported

3.223, $p<0.01$), security policies and procedures ($\beta=0.181$, $t=2.102$, $p=0.018$), and physical security monitoring ($\beta=0.296$, $t=2.563$, $p<0.01$) are positively related to security control. Next, attachment ($\beta=0.175$, $t=2.724$, $p<0.01$), commitment ($\beta=0.451$, $t=5.693$, $p<0.01$) and personal norms ($\beta=0.136$, $t=1.789$, $p=0.037$) positively associated with social control. Furthermore, SCO ($\beta=0.675$, $t=10.391$, $p<0.01$) construct significantly associated with perceive behavioral control. Next, SOC ($\beta=0.800$, $t=19.701$, $p<0.01$) also shown a significant positive association with attitude. Moreover, attitude ($\beta=0.574$, $t=9.553$, $p<0.01$) and perceived behavioral control ($\beta=0.375$, $t=5.965$, $p<0.01$) have a positive association with intention to comply with security policies. On the other hand, risk assessment and analysis ($\beta=0.058$, $t=0.882$, $p=0.189$) showed no significant relationship with the security control construct. In the same way, involvement ($\beta=0.091$, $t=1.029$, $p=0.175$) has shown no significant relationship with social control. A detailed hypotheses analysis is shown in Table 6 and path analysis in Fig. 5.

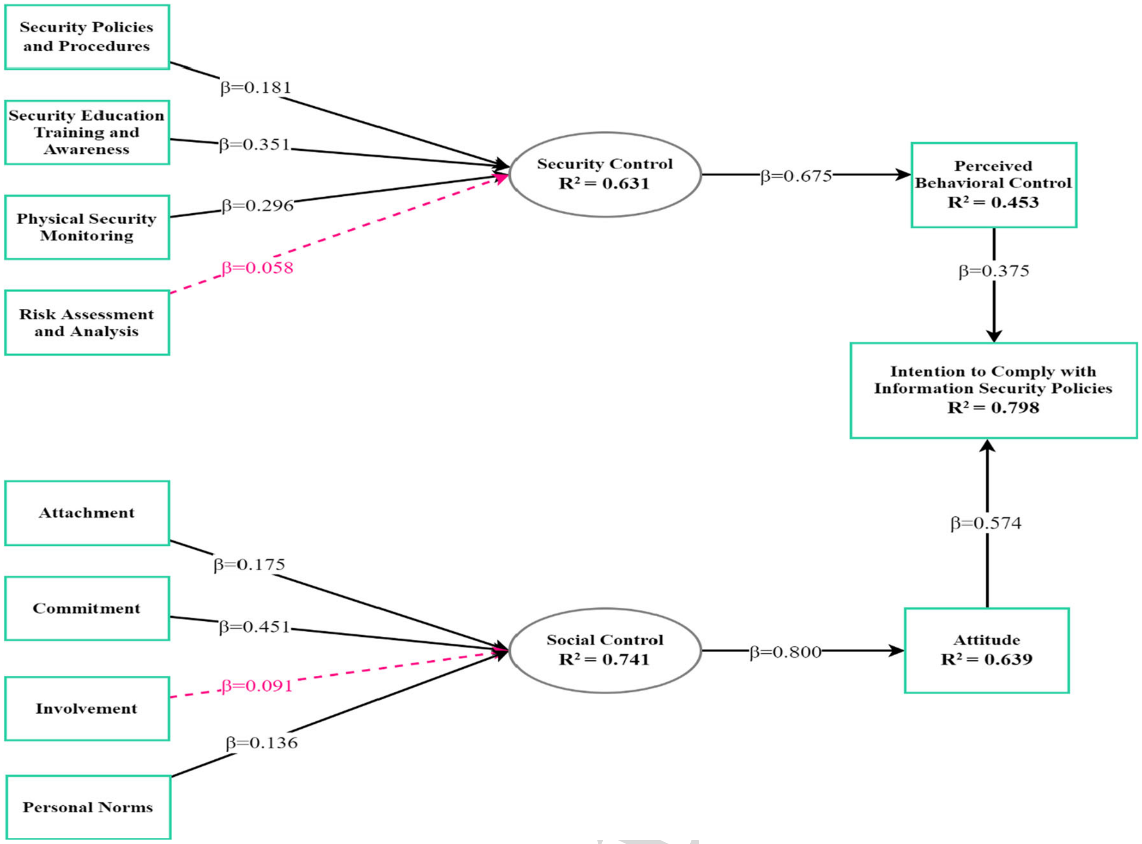

Security Policies and Procedures
Security Education Training and Awareness
Physical Security Monitoring
Risk Assessment and Analysis
β=0.181
β=0.351
β=0.296
β=0.058
Security Control R² = 0.631
β=0.675
Perceived Behavioral Control R² = 0.453
β=0.375
Intention to Comply with Information Security Policies R² = 0.798
β=0.574
Attachment
Commitment
Involvement
Personal Norms
β=0.175
β=0.451
β=0.091
β=0.136
Social Control R² = 0.741
β=0.800
Attitude R² = 0.639

Fig. 5 PLS Results (red and dotted line indicates non-significance effects)

6 Discussion and conclusions

Study's first research question was about organizational governance effects on security control of O&G organizations to enhance perceived behavioral control of employees.

Organizational governance serves as a knowledge source provided by organizational management. In this study, organizational governance was described as an organization's effort to provide the required resources and tools to motivate employees to protect and prevent potential information security threats. Four critical organizational governance elements emerged from the literature review. It was validated to instill a philosophy of information security in organizations. These aspects were regarded as primary sources of information for employees on a variety of information security matters. Furthermore, organizational governance factors were defined based on ISA-95 levels. According to ISA-95, level 4 deals with the business layer means knowledge sources should be behavioral-based like SETA programs. Levels 3 and 2 deal with the factors related to monitoring and risk assessment. Therefore, the researcher selected four major factors in organizational governance SETA, SPP, PSM, and RAA. Thus, organizational factors were collectively seen as sources of knowledgeAs consistent with [14], the results show that inline security policy and procedures are important to enhance the security control of an organization. The presence of a document that contains rules and regulations for workers employed in an organization is referred to as security policies and procedures [11]. Roles and responsibilities are described in policies, as well as the implications of non-compliance. This accepted hypothesis verified the impact of policies on employees' perceptions of organizational security control, which is in line with a recent study [5]. Likewise, the standard regression weight for the path from security education, training, and awareness to security control was calculated as $\beta = 0.351$, with a significance of $p < 0.001$ and CR = 0.877. These findings backed up the hypothesis, implying that security education and awareness programs have a significant impact on employees' perceptions of organizational security control. Results further showed that physical security monitoring has a strong impact on organizational security control, this finding indicates that management should place a greater emphasis on security monitoring because it is an important deterrent factor in preventing security breaches. This may include a regular audit as well as continuous monitoring via computer surveillance [46].

Risk assessment and analysis was the final component of organizational governance toward security control management. The results revealed that risk assessment and analysis showed no substantial impact as a security control factor. This demonstrates that most O&G organizations employees' do not recognize the importance of risk assessment and analysis in protecting data from natural disasters and human error or they do not perceive the concept of the current study; that risk assessment and analysis can enhance overall organizational security control. Furthermore, results indicated that O&G organizations employees are unaware that risk assessment and analysis plans exist in their organizations. This finding is in line with [9], who explained that most of the O&G organizations lack in risk assessment and analysis and there are loopholes in the risk assessment practices in O&G organizations. Future data analysis showed that enhanced security control in an organization significantly improve perceived behavioral control (self-efficacy) of employees; these findings are consistent with [14]. The result from structural equation modeling confirmed the contribution of organizational governance factors in enhancing overall security control. The influence among hypothesized factors was found positive and highly significant. The later analysis confirmed that enhanced security control led to better behavioral control, which can guarantee a positive intention to comply with information security policies.

The second research question was about how social bonding and social controls effect employees' attitude toward organizational information security policies. ISPC is a behavioral action that is triggered by external and internal simulants. This research study focused on social bonding factors and overall social control to enhance the employees' perceptions about information security policies compliance. Current research findings highlighted the significant contribution of social bonding factors to enhance overall social control, which leads to a better attitude toward information security policies. The standard regression weight for the path from attachment to social control was calculated as $\beta = 0.175$, with a significance of $p < 0.001$ and $CR = 0.915$; these values supported the hypothesis. As suggested by Safa et al. [51], employees with better attachment perform their daily tasks better along with information security tasks. Ifinedo [30] showed that better attachment employees are less likely to deviate from organizational policies, which later enhance overall organizational security culture. Commitment to organizational information security policies is considered as an essential construct to enhance social control in organizations. The results indicate that O&G employees are well committed to their organizational information security policies and procedures, and they want to protect their organizational assets from any information security incident. These findings are consistent with [31, 51]. These researchers showed that employees with better commitment toward information security policies are less likely to harm their organizational assets.

The standard regression weight for the path from involvement to social control was calculated as $\beta = 0.095$, with a significance of $p > 0.05$ and $CR = 0.909$; these values did not support the hypothesis. These resulted values indicated that O&G employees are attached and committed to their organizations' information security policies, but there is a need to enhance the employee involvement toward organizational information security control. The reasonable reason for the failure of this hypothesis was found from the literature described by [33]. They have discussed that organizational, administrative control over the IS security issues should be based on the motivations and acceptable training methods. In contrast, if the organizations are not using exact motivation methods to control the IS issues, they may not be involved in IS-related activities as required. The results showed that O&G employees want to comply with organizational information security policies. likewise, the above-mentioned values indicated that personal norms are contributing toward the enhancement of the overall social control of an organization. These findings are in line with [26, 31, 51]. Furthermore, results indicated that social control has a significant influence ($R^2 = 0.639$) on the employees' attitude toward ISPC. Overall, social control explains 63 percent of the variance in the attitude of O&G organizations employees.

6.1 Theoretical and practical implications

This research provides some important theoretical implications to the current body of knowledge. To the best of author's knowledge, this study is among the first studies which incorporated ISA-95 automation levels and designed organizational governance according to the ISA-95 levels. The ISA-95-based organizational governance can help O&G employees to better understand the information security policies.

Second, this study empirically tested social and security controls effects on employees planned behavior. To the best of authors' knowledge, this is first study which empirically tested social and security controls effects on employees behavioral coping (planned behavior). Results indicated that both controls can significantly enhance information security culture in an organization. Moreover, it is easy for employees to cope with organizational information security policies in a good information security culture [16, 48].

Third, this study is complimentary to previous well-known studies based on the protection motivation theory and general deterrence theory. Furthermore, this study backs up social bond theory ideas about group effects and social/personal standards which can serve to discourage deviant conduct in terms of ISPC. Furthermore, this study provided support to the argument that protection motivation and deterrence approaches are not enough to enforce ISPC in organizations. As previous research indicated that organizational punishments have negative effects on employees' attitude which leads them to violate form organizational ISPs [56].

The study also provides various implications for practice. Current research is conducted in a developing country setting. The study is among the first studies which incorporates ISA-95 and information security policy compliance in a developing country. The practical implications mostly generalize toward developing countries First, the designed research framework is based on ISA-95 levels, which almost every manufacturing industry adopts for automation. The current study's results are not only beneficial to O&G industry, it can also be helpful to whole manufacturing industry in fostering ISPC. Second, as social bonding appeared to be a very useful tool for fostering information security culture, practitioners must put some efforts to enhance social bonding among employees. Finally, practitioners must focus on enhancing compliance through improvement of information security culture. Practitioners must follow some non-deterrence-based methods to cultivate good information security culture in the organizations.

6.2 Limitations and future research

Like all empirical studies this study also have some limitations, first of all current research is an empirical study on O&G organizations which are considered as critical infrastructure. The collection of the data from these organizations is near to impossible. Furthermore, this research was conducted during the Covid-19 phase which hinders the data collection phase of this research. Therefore, researcher collected data through judgment sampling which is a non-probability sampling and has less generalizability power. Future research may overcome this limitation by testing this model with a different sampling and population to enhance the generalization of the results. Second, research only took four organizational governance factors, future research may propose some more useful organizational governance factors like workplace capabilities, managerial leadership etc.

Author contributions Conceptualization, RFA and PDDD; methodology, RFA and SN; software, SH; validation, RFA and SH; formal analysis, RFA, PDDD and SN; data curation, RFA and PDDD; writing—original draft preparation, RFA and PDDD; writing—review and editing, PDDD and SH; visualization, RFA and SH; supervision, PDD Dominic; project administration, RFA and PDDD; funding acquisition, PDDD.

Funding This work was supported in part by YUTP-FRG Grant 015LCO-171. PETRONAS Govt of Malaysia.

Research data policy/Data availability statement The data that support the findings of this study are available from PETRONAS Malaysia Sdn Bhd, but restrictions apply to the availability of these data, which were used under license for the current study and so are not publicly available. The data are, however, available from the authors upon reasonable request and with the permission of PETRONAS Malaysia Sdn Bhd.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Ethical statement Authors consciously assure that, this is authors' own original work, which has not been previously published elsewhere. The paper is not currently being considered for publication elsewhere. The paper reflects the authors' own research and analysis in a truthful and complete manner. The paper properly credits the meaningful contributions of co-authors and co-researchers. The results are appropriately placed in the context of prior and existing research. The results are appropriately placed in the context of prior and existing research. All authors have been personally and actively involved in substantial work leading to the paper and will take public responsibility for its content.

References

1. Abdul Hamid, H., Mohd Dali, N.: Curbing misbehaviour with information security measures: an empirical evidence from a case study. AL-ABQARI: J. Islam. Soc. Sci. Human. **17**(1), 28–38 (2019)
2. Ajzen, I.: The theory of planned behavior. Organ. Behav. Hum. Decis. Process.Behav. Hum. Decis. Process. **50**(2), 179–211 (1991)
3. Albrechtsen, E., Hovden, J.: The information security digital divide between information security managers and users. Comput. Secur. Secur. **28**(6), 476–490 (2009). https://doi.org/10.1016/j.cose.2009.01.003
4. Albrechtsen, E., Hovden, J.: Improving information security awareness and behaviour through dialogue, participation and collective reflection: an intervention study. Comput. Secur. **29**(4), 432–445 (2010). https://doi.org/10.1016/j.cose.2009.12.005
5. Ali, R.F., Dominic, P., Ali, K.: Organizational governance, social bonds and information security policy compliance: a perspective towards oil and gas employees. Sustainability **12**(20), 8576 (2020)
6. Ali, R.F., Dominic, P., 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. **11**(8), 3383 (2021)
7. Alnatheer, M. A.: Information security culture critical success factors. Paper presented at the 2015 12th International Conference on Information Technology-New Generations (2015)
8. Anderson, J.C., Gerbing, D.W.: Structural equation modeling in practice: a review and recommended two-step approach. Psychol. Bull. **103**(3), 411 (1988)
9. Bergh, L.I.V., Leka, S., Zwetsloot, G.: Tailoring psychosocial risk assessment in the oil and gas industry by exploring specific and common psychosocial risks. Saf. Health Work. Health Work **9**(1), 63–70 (2018)
10. Calder, B.J., Phillips, L.W., Tybout, A.M.: Designing research for application. J. Consum. Res. Consum. Res. **8**(2), 197–207 (1981)
11. Chen, Y., Ramamurthy, K., Wen, K.-W.: Impacts of comprehensive information security programs on information security culture. J. Comput. Inf. Syst. Comput. Inf. Syst. **55**(3), 11–19 (2015)
12. 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. **39**(7), 447–459 (2013). https://doi.org/10.1016/j.cose.2013.09.009

13. Chin, W.W.: How to write up and report PLS analyses. In: Esposito Vinzi, V., Chin, W., Henseler, J., Wang, H. (eds.) Handbook of Partial Least Squares, pp. 655–690. Springer, Berlin (2010)
14. D'Arcy, J., Hovav, A., Galletta, D.: User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Inf. Syst. Res. **20**(1), 79–98 (2009). https://doi.org/10.1287/isre.1070.0160
15. Da Veiga, A.: The influence of information security policies on information security culture: illustrated through a case study. Paper presented at the Proceedings of Ninth international Symposium on Human Aspects of Information Security & Assurance (HAISA 2015) (2015)
16. Da Veiga, A., Martins, N.: Defining and identifying dominant information security cultures and subcultures. Comput. Secur. **70**(3), 72–94 (2017). https://doi.org/10.1016/j.cose.2017.05.002
17. Erdfelder, E., Faul, F., Buchner, A.: GPOWER: A general power analysis program. Behav. Res. Methods Instrum. Comput.. Res. Methods Instrum. Comput. **28**(1), 1–11 (1996)
18. Etikan, I., Musa, S.A., Alkassim, R.S.: Comparison of convenience sampling and purposive sampling. Am. J. Theor. Appl. Stat.Theor. Appl. Stat. **5**(1), 1–4 (2016)
19. Furnell, S., Rajendran, A.: Understanding the influences on information security behaviour. Comput. Fraud Secur. **2012**(3), 12–15 (2012). https://doi.org/10.1016/S1361-3723(12)70053-2
20. Gefen, D., Rigdon, E.E., Straub, D.: Editor's comments: an update and extension to SEM guidelines for administrative and social science research. MIS Q. **35**, iii–xiv (2011)
21. Gwebu, K.L., Wang, J., Hu, M.Y.: Information security policy noncompliance: an integrative social influence model. Inf. Syst. J. **30**(2), 1350–1917 (2019). https://doi.org/10.1111/isj.12257
22. Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E., Tatham, R.L.: Multivariate Data Analysis, 7th edn. Hoboken, Pearson Prentice Hall (2010)
23. Hair, J.F., Ringle, C.M., Sarstedt, M.: PLS-SEM: indeed a silver bullet. J. Mark. Theory Pract. **19**(2), 139–152 (2011)
24. Hair, J.F., Jr., Hult, G.T.M., Ringle, C., Sarstedt, M.: A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), vol. 2, 2nd edn. Sage Publications, Thousand Oaks (2017)
25. Henseler, J., Ringle, C.M., Sarstedt, M.: A new criterion for assessing discriminant validity in variance-based structural equation modeling. J. Acad. Mark. Sci. **43**(1), 115–135 (2015)
26. Hina, S., Selvam, D.D.D.P., Lowry, P.B.: Institutional governance and protection motivation: theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. Comput. Secur. **87**, 101594 (2019)
27. Hirschi, T.: Social bond theory. Criminological theory: past to present. Roxbury, Los Angeles (1998)
28. 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. **26**(2), 282–300 (2015)
29. Ifinedo, P.: Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput. Secur.**31**(1), 83–95 (2012)
30. Ifinedo, P.: Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Inf. Manag. **51**(1), 69–79 (2014)
31. Ifinedo, P.: Roles of organizational climate, social bonds, and perceptions of security threats on IS security policy compliance intentions. Inf. Resour. Manag. J.Resour. Manag. J. **31**(1), 53–82 (2018)
32. Jaatun, M.G., Albrechtsen, E., Line, M.B., Tøndel, I.A., Longva, O.H.: A framework for incident response management in the petroleum industry. Int. J. Crit. Infrastruct. Prot.Infrastruct. Prot. **2**(1–2), 26–37 (2009)
33. Kessler, S.R., Pindek, S., Kleinman, G., Andel, S.A., Spector, P.E.: Information security climate and the assessment of information security risk among healthcare employees. Health Inform. J. **26**(1), 461–473 (2020)
34. Kline, R.B.: Principles and Practice of Structural Equation Modeling. Guilford Publications, New York (2015)
35. Kock, N., Lynn, G.: Lateral collinearity and misleading results in variance-based SEM: an illustration and recommendations. J. Assoc. Inf. Syst. **13**(7), 1–40 (2012)
36. Lu, H., Guo, L., Azimi, M., Huang, K.: Oil and Gas 4.0 era: a systematic review and outlook. Comput. Ind.. Ind. **111**(3), 68–90 (2019). https://doi.org/10.1016/j.compind.2019.06.007
37. McNeish, D.: Thanks coefficient alpha, we'll take it from here. Psychol. Methods **23**(3), 412–433 (2018)
38. Merhi, M.I., Ahluwalia, P.: Examining the impact of deterrence factors and norms on resistance to information systems security. Comput. Hum. Behav.. Hum. Behav. **92**(March), 37–46 (2019)
39. 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 **12**(11), 1882 (2020)
40. Ochieng, E.G., Ovbagbedia, O.O., Zuofa, T., Abdulai, R., Matipa, W., Ruan, X., Oledinma, A.: Utilising a systematic knowledge management based system to optimise project management operations in oil and gas organisations. Inf. Technol. People **31**(2), 527–556 (2018)
41. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C.: Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Comput. Secur. **42**, 165–176 (2014)
42. Qassim, Q.S., Jamil, N., Daud, M., Patel, A., Jaaffar, N.: A review of security assessment methodologies in industrial control systems. Inf. Comput. Secur. **27**, 47–61 (2019)
43. Qian, Y., Fang, Y., Gonzalez, J.J.: Managing information security risks during new technology adoption. Comput. Secur. **31**(8), 859–869 (2012)
44. Rajab, M., Eydgahi, A.: Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. Comput. Secur. **80**, 211–223 (2019)
45. Ramayah, T., Cheah, J., Chuah, F., Ting, H., Memon, M.A.: Partial least squares structural equation modeling (PLS-SEM) using smartPLS 3.0 Handbook of Market Research. In: 2nd edn Kuala Lumpur: Pearson Malaysia Sdn Bhd (2018)
46. Ren, K., Wang, C., Wang, Q.: Security challenges for the public cloud. IEEE Intern. Comput. **16**(1), 69–73 (2012)
47. Ringle, C., Wende, S., & Becker, J. (2019). *SmartPLS 3*. Retrieved from http://www.smartpls.com
48. Ruhwanya, Z., & Ophoff, J. (2019). Information security culture assessment of small and medium-sized enterprises in Tanzania. Paper presented at the International Conference on Social Implications of Computers in Developing Countries.
49. 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. Fut. Gener. Comput. Syst. **97**(5), 587–597 (2019). https://doi.org/10.1016/j.future.2019.03.024
50. 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. **40**(June), 247–257 (2018)
51. Safa, N.S., Von Solms, R., Furnell, S.: Information security policy compliance model in organizations. Comput. Secur. **56**(1), 70–82 (2016)

52. Sekaran, U., Bougie, R.: Research Methods for Business: A Skill Building Approach. Wiley, New York (2016)
53. Stergiopoulos, G., Gritzalis, D.A., Limnaios, E.: Cyber-attacks on the Oil & Gas sector: a survey on incident assessment and attack patterns. IEEE Access **8**(1), 128440–128475 (2020)
54. Tsakalidis, G., Vergidis, K., Petridou, S., Vlachopoulou, M.: A cybercrime incident architecture with adaptive response policy. Comput. Secur. **83**, 22–37 (2019)
55. Urbach, N., Ahlemann, F.: Structural equation modeling in information systems research using partial least squares. J. Inf. Technol. Theory Appl. **11**(2), 5–40 (2010)
56. Vance, A., Siponen, M.T., Straub, D.W.: Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. Inf. Manag. **57**(4), 103212 (2020)
57. Yazdanmehr, A., Wang, J.: Employees' information security policy compliance: a norm activation perspective. Decis. Supp. Syst. **92**(December), 36–46 (2016)
58. Zakaria, K.M., Nawawi, A., Salin, A.S.A.P.: Internal controls and fraud–empirical evidence from oil and gas company. J. Financ. Crime **23**(4), 1154–1168 (2016)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Journal: 10207
Article: 786

Author Query Form

Please ensure you fill out your response to the queries raised below and return this form along with your corrections

Dear Author

During the process of typesetting your article, the following queries have arisen. Please check your typeset proof carefully against the queries listed below and mark the necessary changes either directly on the proof/online grid or in the 'Author's response' area provided below

Query	Details required	Author's response
1.	Kindly check the city and state are correct in affiliations 1 and 2 and amend if necessary.	
2.	Please confirm if the author names are presented accurately and in the correct sequence (given name, middle name/initial, family name). Author 1 Given name: [Rao] Last name [Faizan Ali]. Also, kindly confirm the details in the metadata are correct.	
3.	Please check the H6 is repeated three times, we have changed H6, H7 and H8, respectively. Please confirm the this changes and correct if necessary.	
4.	References [12, 19] were provided in the reference list; however, this was not mentioned or cited in the manuscript. As a rule, if a citation is present in the text, then it should be present in the list. Please provide the location of where to insert the reference citation in the main body text. Kindly ensure that all references are cited in alpha numerical order.	