International Journal on Engineering, Science and Technology

2022, Volume 4, Issue 4 ISSN: 2642-4088 (Online)

Investigating Benefits Realization of Information Security Policies for Palestine Higher Education: An SEM – ANN Approach

Yousef Mohammad Iriqat

Al-Quds Open University, Palestine

Abstract: In essence, Information Security Management (ISM) is a real-life situation based on its characteristics; confidentiality, integrity, and availability. To generate knowledge based on eight key concepts of ISM supported by popular management theory that uses the core principles of planning, organizing, leading and controlling (PLOC). The research will investigate benefits realization for IS Policies (ISP) by integrating Cranfield Benefits Management Model CBMM. A conceptual research model will be developed from extant academic literature, standards, and the examination of interrelationships between the objectives and practices, and refined via survey data from managers and security professionals based in Palestine higher education institutions. A benefits realization plan BRP is used to define the benefits of the overall ISM work and responsibilities for their realization, measurement and reporting for the ISP realization. Building on these previous efforts, the purpose of this study is to investigate the conceptual theoretical model to recognize benefits realization in the ISP based on the many guidelines and standards available in both academia and practice. Such a conceptual model could provide educational institutions with a favoured benefits realization approach to ISP and future research activities for Palestine higher education institutions. In the context of applied research, the research will use a quantitative method research paradigm using a grounded theory that employs quantitative data. The model used in this research was analysed in two steps. In the first step, Structural Equation Modelling (SEM) was used to determine significant determinants that affect the adoption of PLOC in the ISP realization. In the second step, a Neural Network Model ANN was applied to validate the findings in step 1 and establish the relative importance of each determinant to the adoption of ISP realization. The expected achievable benefits attributes from ISP implementation may include the following; It is beneficiary, gain, attributable and discernible.

Keywords: Benefits management model, Information security policies, Benefits realization, SEM, ANN

Introduction

Information Security Management ISM is defined as that part of the overall management system, based on a corporate risk approach, to create, implement, operate, monitor, review, preserve and improve information security (Whitman & Mattord, 2022; Dhillon, 2007). The ISM includes organisational structures, *policies*, planning, responsibilities, practices, procedures, processes and resources (Whitman & Mattord, 2022). Many organization realizes the benefit of having a fully working ISM unit that will be in charge of Information Security InfoSec matters from the implementation of InfoSec standards like ISO 27000 to benefits acquired from aspects of InfoSec to protect the organizational information assets (Herath et al., 2022). As a whole, organisations should question is the assets (including employees) appropriately protected in terms of loss of confidentiality, integrity and/or availability ((Whitman & Mattord, 2022). Has the known InfoSec vulnerability (e.g. accidental or malicious intent by employee's behaviour) that could affect the organisation been managed systematically? In general, everyone in an organization has to realize his responsibility on protecting information assets and more specifically organization managers (Herath et al., 2022).

Benefits management is often defined as "the process of organizing and managing such that the potential benefits arising from the use of InfoSec are realized" (Ward et al.,1996; Dolan, 2018). An ISM is not a defensive mechanism, it's a holistic way to manage and protect all aspects of InfoSec, it should raise benefit realization throughout the organization for InfoSec risks and involve all employees and users throughout an organization to lower the overall risk and maintain a highly available Information system (Ward et al., 2007).

ISM may provide a better fit with organizational processes and increased chances of benefits realization if the research explores the relationship between InfoSec Policies awareness and benefits realization. A significant challenge will face many organizations when customizing or implementing an InfoSec policy that will cover all aspects of organization processes, and deliver benefits by implementing a benefits realization model to improve coordination and customization across all units of an organization and put employees into perspective (Ward et al., 2007).

Examining this relationship between the soft approach of the Benefits Realization Management Model BRMM (Badewi, 2016) and InfoSec policies realization may be useful as it may explain why some implementations are more successful in realizing benefits than others. However, while each of these aspects has been studied concerning ISM models few studies consider them about the delivery of benefits realization (Love, 2014). In specific, few researchers have observed whether benefits realization differs by the type of customization assumed. For example, a more tailored system may provide a better fit with organizational processes and hence increase the chance of benefits being realized (Love, 2014). The problem has many aspects, such as; Inability to manage InfoSec policy benefits or unawareness of what these are, the employees must first know what they are, accordingly, to realize the potential benefits of InfoSec policy (i.e. identified, planned, owned, and reviewed). Furthermore, benefits management as an approach to realising InfoSec policy benefits has not been investigated yet. Therefore, this research aims to investigate how InfoSec policy benefits can be realized.

The soft school of BRMM, in which the "practice" of benefits is the major driver of success, takes "practice" as the cornerstone in its theories; the better the practice, the more benefits will be realized and, therefore, the more the "accomplishment" (Badewi, 2016; Love, 2014). Therefore, the researchers consider the "practice" variable as a mediating factor between what can be done and the success of the structure. This soft school of BRMM is involved in perception, attitude, behaviour, motivation, and intention. Therefore, the soft school can be examined by means of objective techniques (Badewi, 2016).

Certainly, benefits do not come from deploying a technology; rather they come from changing an organization's way of doing things (employee behaviour). It follows from this argument that "employees" are the main reason for the failure of an InfoSec-enabled business transformation changing employee culture and their behaviour toward a specific assessable objective (Davenport, 2000; Badewi, 2016).

Research Background: Palestine Higher Education

The Palestine Economy Portal PEP (2016) recommends extensive reforms to the rules and regulations surrounding government and institutional InfoSec policies. PEP (2016) argues for laws and legislation to facilitate the protection and security of information; it sees this as an urgent necessity to prevent the risks of cybercrime and InfoSec threats (PEP, 2016). Using the Global Cybersecurity Index (2017), the researcher sees that the GCI index in Palestine is below the 33rd percentile; only three of 25 indicators are above the 65th percentile (cybercriminal legislation, government certification and international participation). A clear gap exists between developing countries in terms of awareness, understanding and knowledge of InfoSec practices.

Recently, there has been a rising number of publications focused on cybercrime and InfoSec policies in Palestine (Abdelwahed et al., 2017; Iriqat et al., 2019). According to Amro (2018), the majority of people in Palestine are connected to the internet and are generally affected by technology. However, knowledge of cybercrime, including identity theft, financial fraud and defamation, does not match up with the high level of connection. In Palestine, for example, cybercrime laws and regulations are weak and must be reviewed (Amro, 2018).

Researchers have, in recent years, showing an increased interest in Palestine Higher Education PHE InfoSec policies (Abdelwahed et al., 2017; Iriqat et al., 2019). Alshare et al. (2018) recommend the establishment of university-level InfoSec units and the formalisation of InfoSec policy documents to avoid the risk of cybercrimes or penetration into the university information system. According to a recent study on Palestinian universities in Gaza by Abdelwahed et al. (2017), universities should support the InfoSec policies from the process of risk assessment and creation of InfoSec policies to the process of continually reviewing and updating InfoSec policies.

Numerous research initiatives (da Veiga et al., 2020; Iriqat et al., 2019; Aurigemma & Mattson, 2017; Ahlan et al., 2015) on InfoSec behaviour and awareness have focused on theory verification and validation or have simply been literature reviews of theory comparisons used in InfoSec or InfoSec policy compliance, and, as such, may present a biased viewpoint. Many researchers propose (da Veiga et al., 2020; Iriqat et al., 2019; Aurigemma & Mattson, 2017; Ahlan et al., 2015) that a theoretical model without empirical evidence of employee InfoSec policy compliance does not offer any evidence to support their models.

Furthermore, to put this study in the context of PHE, the researcher uses an investigation of the Benefits Management Model into InfoSec countermeasures. The study could significantly contribute by integrating the BRMM into InfoSec awareness (Ahlan et al., 2015). Also, by exploring employee realization of InfoSec policies in PHE and realising the collaboration of BRMM with InfoSec to achieve and innovate benefits realization resourcefully. Benefits should be managed by identifying, planning and auditing the benefits by exploring InfoSec realization potentials, as a critical success factor that may improve the benefits realization process of

InfoSec policies (Alshare et al. ,2018; Badewi, 2016; Davenport, 2000). Moreover, the benefit of employee realization InfoSec policies for the organization is to improve the overall governance structure in managing InfoSec and preserve a structured and inclusive model for identifying and evaluating InfoSec risks, selecting and applying applicable controls, and determining and improving their effectiveness (Alshare et al., 2018).

Because combining the BRMM process factors of Planning, Leading, Organizing, and Controlling PLOC perception and ISP Awareness constructs cover a few different sides of the ISP realization to strengthen the human factor, which is the weakest link in the security chain (Abdul Molok et al., 2010), more consideration should be given to employee's awareness of InfoSec policy agreement (Ahlan et al., 2015). PHE like other universities in the Middle East that are not oil-rich nations have a heavy burden on their spending on highly new high-tech InfoSec progressions. Therefore, our ***drive*** for this research:

- Promote and gain insights on employee's ISP Awareness (ISPA), and understand employee's perceptions of extrinsic soft BRMM process factors (PLOC) that drive their behaviour for ISP realization.
- To develop a novel model for the intention of this study that best highlights several factors that were extracted from well-known theories in the context of PHE.

The research question and objective for the intention of this study; The research *Question*: Are there any relationships between employee perception of the BRMM process factors antecedent to ISP awareness with perceived ISP realization? The research *Objective*: To determine the consequence of employee perception of PLOC antecedent to ISP awareness with perceived ISP realization**.** To answer the research question related to the InfoSec policy and perception factors by drawing on well-known theories such as the soft approach of BRMM, and InfoSec awareness related to employees benefit realization with InfoSec policy using data collected from 119 management employees for exploring this study through a research instrument of six constructs with several measurement variables each. The paper is organized by presenting a brief literature review, theoretical framework, research methodology, empirical data analyses and results, followed by a discussion.

Literature Review

The existing literature (Yerby & Floyd, 2018; Alshare et al., 2018) on InfoSec countermeasures is extensive and focuses particularly on four types: Preventative (such as anti-virus, firewall, security education and training awareness (Alshaikh et al., 2018; da Veiga et al., 2020). Reactive (such as to incidents), a detective (system /computer monitoring), and administrative (use ISP to protect our information asset, to ensure compliance with policies and procedures) (Alshaikh et al., 2018; Alshare et al., 2018; da Veiga et al., 2020). One of the most cited studies is that of Whitman & Mattord (2022) who see three general categories of countermeasures- policies through setting documented rules for employees' behaviour, programs are activities to improve employee InfoSec -education, training and awareness programs, and technical countermeasures.

According to Dhillon (2007), "InfoSec has three levels of control: technical, formal, and informal". He argues that any disagreement between the three levels may result in potential security problems. By protecting technical systems, controls are usually assigned in the area of access control and authentication (Dhillon, 2007).

Nevertheless, InfoSec risks cannot be dealt with by mere technical controls. For example, perpetrators may find it easier to acquire information from documents left in the trash rather than accessing the information system (da Veiga et al., 2020; Dhillon, 2007). Organisations can no longer trust solely process and technology for risk mitigation of security problems and need a more significant consideration towards employees' integration with process and technology (da Veiga et al., 2020; Dhillon, 2007; Herath et al., 2022). In the subsequent review, it will be shown that the ability to provide a secure and trusted information system by employee compliance with ISP is a business necessity.

Much of the current literature (Herath et al., 2022; da Veiga et al., 2020; Iriqat et al., 2019), on insider actions, pay particular attention to what causes direct or indirect threats to organisational assets and classify it into two categories; intentional (deviant behaviour): includes sabotage, theft, and industrial espionage, unintentional (misbehaviour): includes using an organisation's computers to browse non-work-related websites, posting secure information onto untrusted websites by accident, or carelessly opening phishing links on emails and Websites.

Internal threat is a problem that all universities are facing, as staff action or ignorance can potentially lead to potential security risks (Herath et al., 2022). Although some researchers accentuate the idea that an internal threat is more pressing than an external threat (Herath et al., 2022; Yerby & Floyd, 2018), others see only insider personnel who have access to the information assets, who do not comply with security countermeasures such as ISP would jeopardize the information assets and cause many risks (Alshaikh et al., 2018).

Higher education constitutes from universities have very data-rich vulnerabilities, and they store large amounts of student records of information that are replenished recurrently by multiple departments (Ahlan et al., 2015). The vast amount of data, accessed by many staff; academic, administrative, and others, makes a significant threat to securing university assets. The decentralisation of storage, access, and usage of information assets creates duplication, lax security controls, and chances for potential attackers (da Veiga et al., 2020). University campus, the information technology infrastructure constitutes several different computer systems and applications which should protect the privacy of staff and student records. It is common practice for employees to have access to these systems, and employees do not always comply with security policies and protocols. These diverse computer systems have possible to be demoralised or have information sharing that may lead to an obliteration of InfoSec policies compliance (Yerby & Floyd 2018; Alshare et al., 2018). Where staff transition between special committees and different roles within the university. Universities fall under various compliance and security requirements which raises the problem of the type of information that they are accountable for as well as adhering to the requirements and laws (Yerby & Floyd 2018).

A key element of InfoSec awareness is the human factor or the employee within the university (Yerby and Floyd, 2018; Ahlan et al., 2015). InfoSec awareness is an essential element of every university since the human factor is often the weakest link (Yerby & Floyd, 2018). Ahlan et al. (2015), defined InfoSec awareness as a "state where users in an organisation are aware of and preferably committed to their security mission (often expressed as in end-user security guidelines)”. More specifically, Yerby & Floyd (2018), described InfoSec awareness as one's acquaintance of InfoSec threats and the countermeasures to prevent such threats.

Additionally, awareness of InfoSec policies is vital for InfoSec perception and behaviour, and it plays a crucial role in employee policy behaviour compliance (Kolosenia et al., 2018). InfoSec awareness is considering employees' cognitive state by being conscious about the state of information protection from external and internal threats that face their institution, they understand the risk, and participate in the overall effort to keep the institution secured (Xu & Guo, 2019). InfoSec awareness is considered the general platform as InfoSec is the responsibility of everyone within an institution; researchers specify employee security awareness as a problematic issue, and that most employees lack awareness of policies, security issues and procedures (Alshare et al., 2018).

Benefits Management and realising the benefits from investments made especially by those in information systems became an important area in the late 20s (Badewi, 2016). The concept of benefits realization is not new and neither is the awareness of the links between project and benefits management as evidenced by several types of research that explore the origin of information system failure to be the imprecise statement of benefits, leading to an indeterminate provision of responsibility for managing their conveyance. The increase of importance in benefits realization has coincided with the increasing use and complexity of information systems, thus it defines as the process of organizing and managing, such that the potential benefits arising from the use of information systems are realized (Cresswell et al., 2022; Breese, 2012). The newly identified research points out that the organisation and its business context determine the benefits and the organisation must be proactive in realising benefits (Breese, 2012).

Planning benefits realisation key issues are how the roles and responsibilities are perceived by HE employees for realising business benefits and planning business changes. In particular, the role of the manager was explored. Questions were asked as to how the HE organization perceived benefits delivery plans and the extent to which process and organizational changes are addressed. Benefits realisation comprises confirming that the benefits outlined in the benefits realisation plan are realised (Breese, 2012). This involves the realised benefits to the benefits outlined in the perceived plan. External and internal factors can affect whether or not benefits are realised by the InfoSec policies. The external factors include organizational regulations and changes in the technological environment (Breese, 2012). The internal factors include the extent to which management promotes the implementation and usage of the InfoSec policies.

Organizing can be defined as the process by which the recognised plans are realized (Al-Mashari et al., 2003; Breese, 2012; Cresswell et al., 2022). It is intentional in the sense of making sure that all the responsibilities necessary to attain aims are allocated to employees who can do the best in ISP compliance, to create an environment for the best employee performance. The skill of influencing employees for a particular purpose or reason is *leading*. Leading is considered to be the most important and challenging of all managerial activities, by influencing the organization's employees to work together in the interest of the organization. And by creating a positive attitude towards InfoSec policies realization and goals among the members of the organization is called leading (Al-Mashari et al., 2003). It is required to oblige the objective of use and competence by changing the behaviour of the employees.

Controlling is monitoring the organizational progress toward goal fulfilment. Thus, monitoring advancement is vital to confirm the accomplishment of organizational goals. Therefore, outcomes are controlled by controlling what employees ensure, and controlling empowers the achievement of the plan. Controlling is the last but not least significant management function process (Al-Mashari et al., 2003; Breese, 2012; Badewi, 2016).

The BRMM is suitable in the sense its approach clearly shows how the intended InfoSec policies will contribute to the organization's overall performance of ISP compliance. The BRMM was designed to start with an understanding of the drivers and the organization's overall strategic direction (Scheepers et al., 2022). The BRMM provides limited guidance in this but remains the most comprehensive and flexible framework available. HE Organisations should use the best practices guidelines offered as guidance to identify their own set of benefits and overcome this shortcoming (Scheepers et al., 2022; Breese, 2012).

The Conceptual Research Model

The benefit of InfoSec policies is by delivering the perception of the outcome not by delivering outputs. The delivering outcomes (the benefits from an ISP) have been examined in many works of literature, such as Ward and Daniel (2006), which have addressed the main steps required for obtaining benefits from IT investments. The developed conceptual research model shown in figure 1, integrates the employee's perception of PLOC with ISP Awareness of InfoSec countermeasure's effect on the employee's perception of ISP realization.

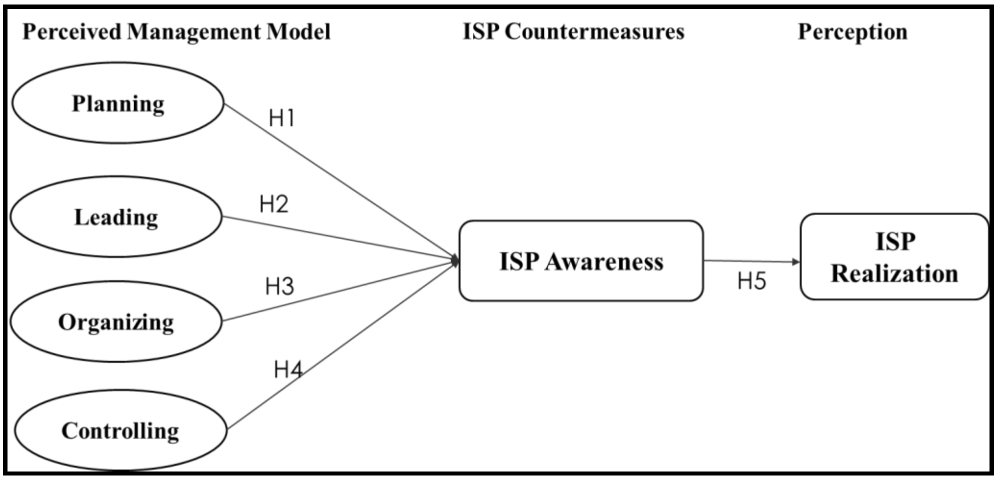

Figure 1: Conceptual Research Model (BRMM- ISP Realization)

Based upon the above discourse around Planning, Organizing, Leading, and Controlling, it is possible to postulate a clear relationship between these four constructs, and envisage how they might be configured in the context of benefits realization through ISP. From this analysis, the benefits realization skill will be enacted through a coherent set of benefits realization skills. As demonstrated in Figure 1, each construct has an indirect effect by employee's ISP realization mediated by ISP countermeasures. As consequence, the study postulate that, based on the unique characteristics of ISM that the most likely benefits realization model that should be explored in an ISP context is the Model of Benefits Management. To examine the impact of the perceived PLOC of the BRMM and the ISP realization through the InfoSec Countermeasures, thus the hypotheses are:

H1: *The relationship between the perceived planning of the BRMM and the ISP realization is moderated by the Information Security Countermeasures.*
H2: *The relationship between the perceived leading of the BRMM and the ISP realization is moderated by the Information Security Countermeasures.*
H3: *The relationship between the perceived organizing of the BRMM and the ISP realization is moderated by the Information Security Countermeasures*.
H4: *The relationship between the perceived controlling of the BRMM and the ISP realization is moderated by the Information Security Countermeasure*.
H5: *Information Security Countermeasures are positively related to the perceived ISP realization*

Research Methodology

Several published studies in InfoSec (Scheepers et al., 2022; Ward & Daniel, 2006; Yerby & Floyd, 2018; Alshaikh et al., 2018) and BRM show that empirical and case studies are the most popular methods used in InfoSec research. Accordingly, in the context of empirical study, this study uses part of an extensive established research instrument to collect the primary empirical dataset (Iriqat et al., 2019). This part represents this study to answer the posed research questions and objectives of the study, which constitute the BRMM operationalised factors and the research hypothesis. The research methodology includes the research methods and research instrument validation.

Research Methods and Statistical Tool

The purpose of this study is to recognise the impact of perceived PLOC of the management process on the benefits realization of ISP and the mediating role of ISP awareness. To test the proposed conceptual model, data were collected using a research instrument to gather information into SPSS V23. A Partial Least Square PLS Structural Equation Modelling (SEM) was chosen as the quantitative tool of analysis to perform multivariable regression and exploratory research questions because it provides flexibility in terms of the type of data and the examination of complex associations (Rahman et al., 2020) using SmartPLS 4. PLS-SEM is a technique that practises the weighted composites of construct variables to interpret for the measurable error without prior distributional expectations about the data. Moreover, PLS-SEM provides the relationship significance of the constructs to evaluate the performance of the model (Ali et al., 2018).

To acquire more insights regarding the importance of each construct regarding the realization of ISP, Importance-Performance Map Analysis (IPMA) was also reported. According to Ringle & Sarstedt (2016), combining PLS-SEM with IPMA offers profound insights into the impacts of certain constructs on explicit behaviour (Ringle & Sarstedt, 2016; Hair et al.,2011). IPMA enables us to investigate the importance and performance at the construct level, which helps identify the critical factors for the improvement of the antecedent constructs (Ali et al., 2018). IPMA is a two-dimension matrix that considers the construct's average latent variable score for the performance and the total effect of the importance of the construct (Ringle & Sarstedt, 2016).

In the second stage, an Artificial Neural Network (ANN) was applied to validate the findings and establish the relative importance of each factor to the realization of ISP. ANN approach bears a resemblance to the structure of the human brain encompassing the neuron, synapse, and axon. It can enhance knowledge through the learning process (Dinh et al., 2018). ANN possess the capability to address nonlinearity and to learn by building input-output mapping (Dinh et al., 2018). The key benefit of employing ANN is to measure the complicated linear and non-linear associations between interpreters and the acceptance decision and to prioritize the constructs based on their relative importance (Dinh et al., 2018). Moreover, ANN is more vigorous and has superior prediction accuracy than the usual regression methods (Dinh et al., 2018).

Henseler et al. (2009) stated: ‘‘In research settings with predictive scope, weak theory, and no need for an understanding of underlying relationships, artificial neural networks (ANN) may be useful’’. In the second phase, ANN is applied to examine the accompaniment and confirm the PLS-SEM analysis and measure the effectiveness of independent constructs on the dependent construct.

Research Instrument

Since this study is exploratory, we opted to use an exploratory survey for the data collection, the survey addresses the issues which affect the capacity of PHE by targeting several universities to realise the benefits of InfoSec policies, to address how HE organizations do or do not ensure that benefits claimed are actively managed through to realisation. To do this a developed research model based on the BRMM, and ISP Awareness (Al-Alawi et al., 2016) was used to structure a questionnaire to elicit details of how effective HE organizations are in addressing benefits management ISP realization by employees. The total respondent from the management division acting as head of sections or departments from six HE universities responded to the survey were 129, thus providing a reasonable set of data for the analysis of the exploratory study.

In this study, definitions of the perceived factors from the developed theoretical model were initially proposed based on reviews of ISP awareness, and the PLOC factors related to employee realization intention with InfoSec policies. The measurement items (variables) were expansively reviewed and developed from previous research in the InfoSec and process management disciplines. Furthermore, the developed items so the “expected” perceived process management (PLOC) and “expected” perceived realization intention of ISP is suitable in the context of Palestine, to understand Staff “perception” realization and to an extent their awareness of ISP’s to mitigate security threats explicitly from insiders as emphasised in the literature review.

The research survey underwent content and face validity. Content validity is assessed by examining the process by which scale items are generated (Straub, 1989). While Straub (1989) defined content validity as the degree to which a measure's items represent an appropriate sample of the theoretical content domain of a construct. Face validity; according to (Creswell & Creswell, 2017), signifies few content experts, consequently; a total of two professionals provided reviewed content. Modifications and recommendation sentence rephrasing by the professional, also only a few items were replaced as suggested by reviewer's face validation.

The Dataset validity and reliability of the collected datasets 129 surveys, where 16 collected surveys have been disregarded based on partially answered by participants with an estimated percentage of (16/129) %12. Furthermore, a few missing datasets were treated by the Expectation-Maximisation method (Field, 2009) using SPSS. Furthermore, testing for *Response Bias* (Field, 2009), did not exhibit response bias based on the collected dataset. The final dataset comprises 113 participants. Moreover, the *Common-Method Variance* (CMV) based on the Harman on-factor test (Field, 2009), the total variance explained should be less than 50%. The total variance explained in the study shows a value of 32.3%. This indicates the survey displays no bias in terms of multicollinearity or bias introduced from the survey, which causes the variance.

Results Analysis

This paper presents some of the key results of that analysis. From the survey, it is clear that many PHE organizations believe that current methods are far from satisfactory in ensuring that the perceived benefits are properly identified and realised. The analysis encompassed a descriptive of demographic variables, assessment of the measurement model and structural models were tested using partial least square-structural equation modelling (PLS-SEM) using SmartPLS 4 software. The sample of 113 was a group of 11% IT experts, 89% division managers, and 75% who have less than 15 years of experience. With 58% male, and 42% female participants.

Assessment of Measurements Model

Construct reliability and validity: Convergent Validity (factor items "measurement variables" loadings) of the outer model was assessed by examining the reflective constructs, which consist of several measurement variables for each construct. Four of the measurement variables were removed (IC1-IC3, AISP5) that have loading below 0.7. The rest of the measurement items and their reflective constructs as shown in table 1 with an outer loading above 0.7. Meanwhile, according to (Ringle & Sarstedt, 2016), the reflective item loadings for exploratory research should be more than 0.5, although the item loadings above 0.7 will be assessed in the structural model.

Internal consistency was confirmed based on Cronbach's alpha CA and RhoA values above 0.7 (Ringle & Sarstedt, 2016) for all constructs as shown in table 1. The Composite reliability CR values (greater than 0.7) for all constructs in the measurement model were also greater than Cronbach's alpha values, signifying that all constructs had acceptable reliability assessment values. Therefore, the evaluation of the measurement model based on evaluating its reliability and validity is confirmed according to (Ringle & Sarstedt, 2016). Meanwhile, the *convergent validity* of the constructs was confirmed by measuring the constructs' Average Variance

Extracted AVE and CR values for the threshold score of 0.5 and 0.7 respectively as indicated by (Ringle & Sarstedt, 2016). Furthermore, constructs are within the range of acceptable Variance Inflation Factors VIF < 5, a VIF value of 5 consider minor collinearity and a VIF of 10 is considered major collinearity (Hair et al., 2010).

Discriminant validity: the cross-loading criterion (Fornell & Larcker, 1981). Subjective independence can help reduce the presence of multicollinearity amongst the latent variable denoting that the AVE of a latent variable should be higher than the squared correlation between the latent variable and all other variables (Hair et al.,

Table 1. Measurement Model

Factor		Outer loading	Measurement Model Reliability Scores				VIF
			CA	(Rho-A)	CR	AVE	
ISP Realization			0.887	0.918	0.921	0.743	
	IC4	0.879					
	IC5	0.873					
	IC6	0.855					
	IC7	0.841					
ISP Awareness			0.793	0.858	0.863	0.614	
	AISP1	0.882					
	AISP2	0.713					
	AISP3	0.778					
	AISP4	0.750					
Planning			0.840	0.853	0.885	0.607	1.049
	P1	0.774					
	P2	0.810					
	P3	0.789					
	P4	0.777					
	P5	0.742					
Leading			0.872	0.962	0.910	0.716	2.670
	L1	0.780					
	L2	0.874					
	L3	0.890					
	L4	0.837					
Organizing			0.913	0.892	0.929	0.725	3.030
	O1	0.830					
	O2	0.881					
	O3	0.881					
	O4	0.796					
	O5	0.867					
Controlling			0.884	0.906	0.911	0.631	2.334

C1	0.719
C2	0.833
C3	0.806
C4	0.821
C5	0.774
C6	0.806

2010). The square root of the AVE for every construct should exceed the correlation range among all constructs by using Fornell-Larcker's criterion. Table 2 presents the results of cross-loading criteria, with the diagonal values exceeding other values in its column or row. Additionally, all these values confirm the square root of AVE values for each latent variable presented in table 2.

An alternative approach is by using the Heterotrait-Monotrait (HTMT) ratio of correlation. As a criterion – the HTMT value needs to be higher than $HTMT_{0.85}$, a value of 0.85, or $HTMT_{0.90}$, a value of 0.90 (Kline, 2011). The HTMT is an estimate of the correlation between the constructs, its interpretation is straightforward: if the indicators of two constructs exhibit an HTMT value that is smaller than one, the actual correlation between the two constructs is most likely different from one, and they should differ (Henseler et al., 2009). Adopting HTMT as a criterion involves comparing it to a well-defined threshold. If the value of this threshold is lower than the HTMT, one can conclude that there is a lack of discriminant validity (Table 3).

Table 2. Fornell-Larcker criterion

	Controlling	ISP Awareness	ISP Realization	Leading	Organizing	Planning
Controlling	**0.794**					
ISP Awareness	0.322	**0.783**				
ISP Realization	0.301	0.389	**0.862**			
Leading	0.677	0.309	0.421	**0.846**		
Organizing	0.720	0.098	0.242	0.771	**0.852**	
Planning	0.194	0.355	0.223	0.100	0.073	**0.779**

Table 3. Heterotrait-Monotrait Ratio (HTMT).

	Controlling	ISP Awareness	ISP Realization	Leading	Organizing	Planning
Controlling						
ISP Awareness	0.356					
ISP Realization	0.329	0.397				
Leading	0.794	0.315	0.447			
Organizing	0.787	0.104	0.253	0.885		
Planning	0.244	0.422	0.261	0.175	0.184	

Assessment of Structural Model

The structural model shows the inner-path relationships between constructs in figure 2. It highlights the casual relationships and coefficients between the latent constructs that will be examined using SEM-PLS analysis. According to Hair et al. (2011), "Testing the structural model determines whether there is empirical evidence for the hypothesised relationship between the constructs".

Path Coefficients (β) figure 2, determine the strength of the relationship between latent constructs, the strength of individual inner path (β) as suggested by Hair et al. (2011), ($\beta < 0.2$ is weak; $0.2 \leq \beta \leq 0.5$ is moderate; $0.5 < \beta$ is strong). Beta values the strength of individual inner path in the structural model shown in figure 2, is moderate and positive, except for organizing construct it has a value of 0.505 but in the other direction (-0.505) which means its formative indicator rather than a reflective indicator as the other construct.

To check the ability of variance explained in the constructs criteria, the shown R^2 results in Table 4, indicate the amount of explained variance based on Hair et al. (2010), criteria of R^2 should be above 19%. The shared variance in ISP Awareness construct as a mediator that is explained in the perceptions of PLOC constructs is significant (0.496). Hence, it indicates that the shared variance of the ISP Awareness construct has an amount of 49.6% explained variance from the perceived PLOC constructs. Also, the dependent variable ISP realization has an amount of 55.1% explained variance.

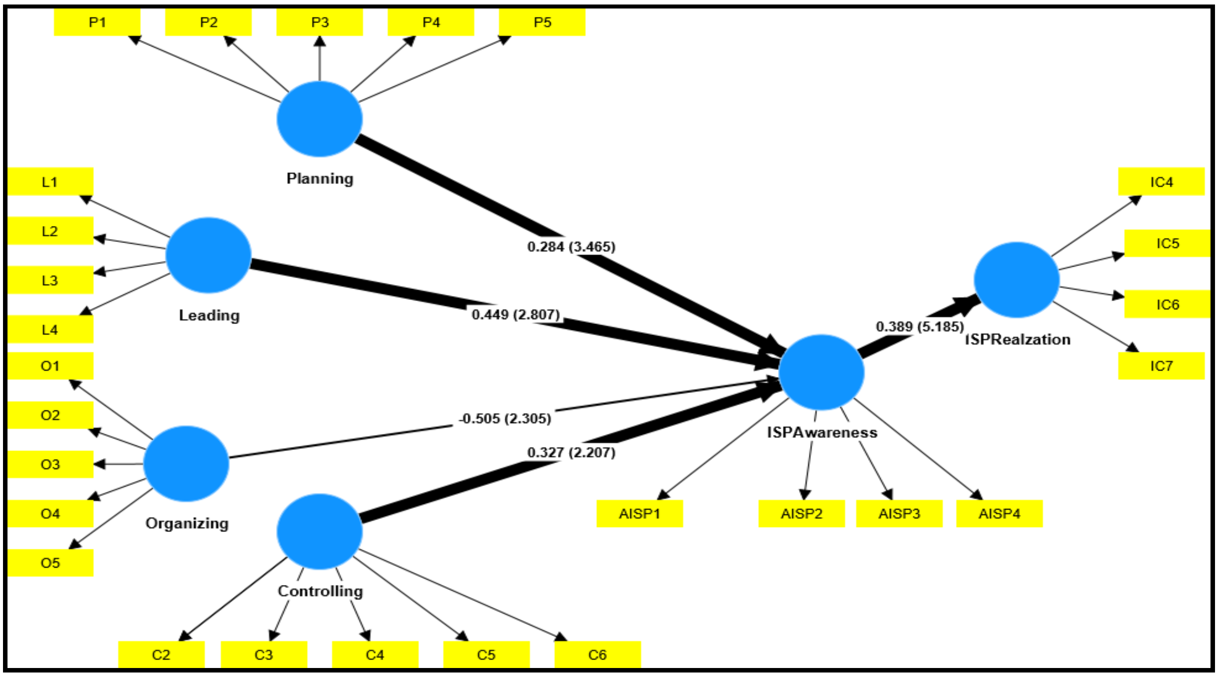

Figure 2. Structural Model (Path Coefficients (β), t-statistics)

Table 4 presents the path coefficients' significance relationships associated with ISP realization through indirect relation via the ISP awareness as mediator such as; Planning, Leading, Organizing, and Controlling perception constructs are significant and contribute to the research model. The p-values are less than 0.05 at 90% confidence intervals with two tails for all construct and its statistically significant, based on a t-statistics value above 1.645 and a significant level (for interval 5%-95%). Meanwhile at 95% confidence intervals two tails (2.5%-97.5%) H1 and H5 are statistically significant. Consequently, hypotheses H1-H4 “The relationship between the perceived PLOC of the BRMM and the ISP realization is moderated by the Information Security Countermeasures”, are supported at the 90% confidence intervals. Therefore, ISP realization by employees was affected by perceived PLOC constructs antecedent to ISP awareness. Also, H5 is supported as the direct effect of ISP awareness on ISP realization.

Table 4. Path Analysis Results

Path (Hypothesis)	Mean	StDev	T	P values	Confidence intervals	
					2.5%	97.5%
H1: Planning -> ISP Awareness -> ISP Realization	0.120	0.042	2.599	0.009**	0.045	0.209
H2: Leading -> ISP Awareness -> ISP Realization	0.155	0.078	2.226	0.026*	0.021	0.322
H3: Organizing -> ISP Awareness -> ISP Realization	-0.153	0.097	2.033	0.042*	-0.325	0.061
H4: Controlling -> ISP Awareness -> ISP Realization	0.117	0.064	1.994	0.046*	0.002	0.255
H5: ISP Awareness -> ISP Realization	0.399	0.075	5.185	0.000**	0.247	0.537
ISP Awareness (R^2= 0.496); ISP Realization (R2= 0.551)						

** significance at 95%, * significance at 90%

In conclusion, as seen in figure 2; All perceived constructs constitute the novel model and contribute to the whole theoretical model despite that one constructs Organization is formative and contribute to the employee’s ISP realization by testing the path statistical significance, while these constructs have shown a significant positive relationship with ISP realization as an antecedent to ISP awareness. Therefore, the model is novel and coherent based on these constructs, as shown by values of R^2 amount of explained variance in table 4. And, β, the correlation strength of (figure 2) for the five significant paths are of moderate values.

Importance Performance Map Analysis

An importance-performance matrix analysis (IPMA) as a post-hoc procedure in PLS using ISP Realization as the outcome construct was performed. The objective of running IPMA is to estimate the importance of the predecessor constructs (PLOC and Awareness) and their performance in describing the target construct. This analysis recognizes factors that have a relatively weak to moderate total effect (importance) for the target variable but a relatively high performance (Hair et al., 2011). These factors represent the potential scope for improvement and these factors need high attention.

In IPMA, the total effects of predecessor constructs represent the importance of shaping the target construct, while the average latent variable scores of predecessor constructs represent their performance (Ringle et al., 2016). The performance scores were computed by rescaling the latent constructs scores to a range of 1 to 100 (1 = lowest performance; 100 = highest performance) (Ringle et al., 2016). More specifically, instead of only analysing the path coefficients (i.e. the importance dimension), the IPMA also considers the average value of the latent variables and their indicators (i.e. performance dimension)".

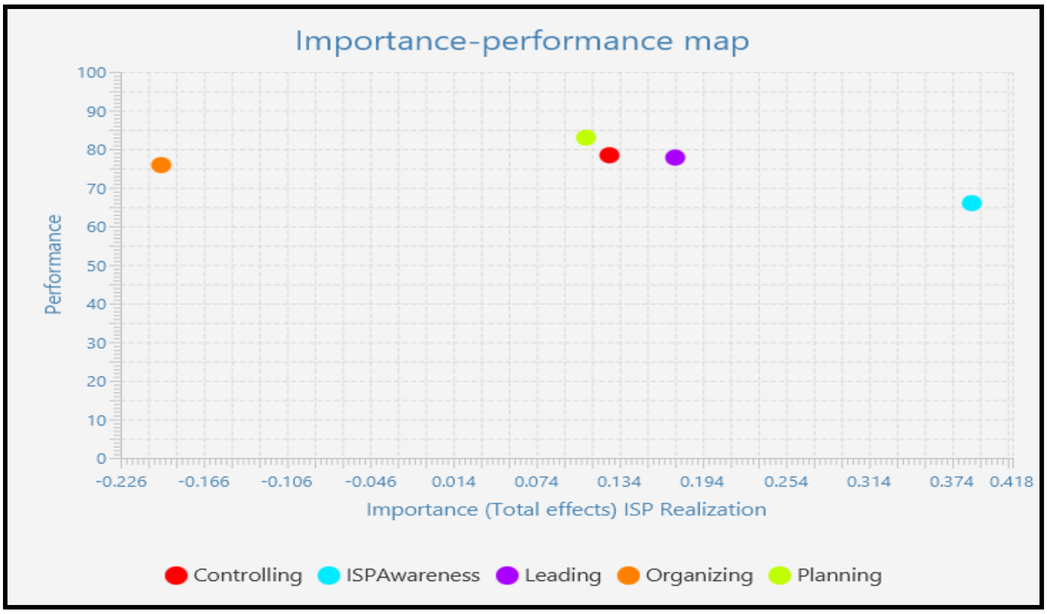

Figure 3. IPMA

Figure 3 shows the values of predecessor constructs' importance (total effects) and performance scores target constructs. Further, we developed a priority map (as shown in Figure 3) by plotting the predecessor constructs' total effects value and performance scores. From the map, it is observed that the ISP awareness construct is a very important factor in determining ISP realization despite its average performance because of its relatively higher total effects (importance) compared to other factors in the proposed model.

Nonetheless, the performance of Planning, Leading, and Controlling were of high performance and average importance than other factors. The organizing factor show average performance with low importance as also specified in figure 2 as a formative construct (β=-0.505). In sum, to enhance the adoption of soft PLOC factors in employee perception of InfoSec policies, the managerial activities should concentrate on improving the performance of functional organizing factors, with increased effort on the other PLOC factors.

Artificial Neural Network Analysis

This study achieved neural-network analysis by using the SPSS V23 software package. The neural-network model was developed employing a multilayer perceptron training method. This study uses an active hidden layer since a continuous function can be represented adequately by one hidden layer (Talukder et al., 2020). A benefit of proposing an ANN model that can recognize non-linear correlations is that the ANN may learn multifaceted linear and non-linear correlations between predictors and adoption choice (Talukder et al., 2020). Further, neural networks do not test hypotheses and analyse causal relationships due to their 'black-box' nature. As a result, a two-stage strategy is adopted in this work, similar to those (Talukder et al., 2020). In the first stage, an SEM is employed to evaluate all the hypotheses and excerpt important predictors in the model that are further incorporated as inputs to the ANN in the second stage to measure the status of each piece of evidence.

At this stage, the statistically authoritative essentials from the SEM were included in the model. Five hypotheses have been identified as critical for imminent investigation based on the SEM discoveries. As a result, these elements were characterized as input variables in the input layers; in this case, the output layer's dependent variable was ISP realization.

Table 5. Root Mean Square Error

Sample	N	%	RMSE
Training	83	73.5	0.033
Testing	30	26.5	0.031
Hidden/output layer activation Sigmoidal Function			

In this study, we allocated 73.5% of data for training the neural network model and the rest 26.5% of data for testing the prediction precision of the trained model, Meanwhile, the hidden/output layer activation espoused is the sigmoidal function (Talukder et al., 2020). The five significant constructs of PLOC and Awareness with ISP realization as output layer (see Figure 4). The RMSE values for training and testing were 0.033 and 0.031 respectively (see Table 5). These low RMSE values denote that the neural-network model is consistent in explaining the numerical relationships between the predictors and output.

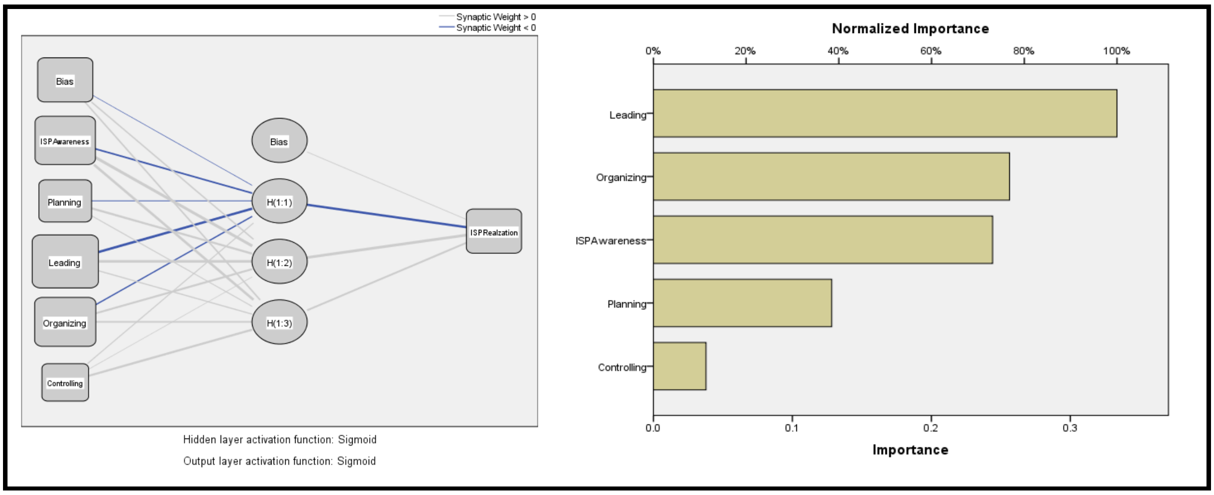

Figure 4. ISP Realization Normalized Importance

To determine the sensitivity analysis for the average of the significance of the independent construct that benefits to predict the dependent construct (Talukder et al., 2020). As per the findings from ANN analysis shown in figure 4, it is seen that Leading was the most important forecaster of ISP realization adoption by the employees. The other important variables in predicting ISP realization were organizing and ISP Awareness.

Discussion and Conclusions

This study has offered and conferred the background of the research. It presents information, inferences, and recommendations obtained from an evaluation of the current ISP realization based on the BRMM PLOC process model perception of the PHE organization. It is from this information that a clear picture emerges of the present role of InfoSec policy realization, and it explained why ISP realization is vital for the HE computing environment. Moreover, the research problem was discussed, as this study set to develop a model to understand and gain more insights on employee's realization behaviour of ISPs facilitated by factors from BRM theories, and ISP awareness as an InfoSec countermeasure at a university information system environment in the context of Palestine Higher education.

A comparative analysis of results gained from PLS-SEM and ANN is presented to identify similarities and differences in determining the importance of predictors. According to SEM results (Table 4), the most and least significant determinants of BRMM PLOC process perception were the Leading and Planning factors respectively. Meanwhile, all hypothesis was supported which shows that PLOC as antecedents to ISP awareness as one of the InfoSec countermeasures has an indirect effect on ISP realization. All perceived constructs constitute the novel model and contribute to the whole theoretical model despite that one constructs Organization is formative and contributes to the employee's ISP realization by testing the path statistical significance, while these constructs have shown a significant positive relationship with ISP realization mediated by ISP awareness. Therefore, the model is novel and coherent.

The IPMA gives researchers the prospect to develop their PLS-SEM analysis and, thereby, gain further results and findings. More specifically, instead of only analysing the path coefficients (i.e. the importance dimension), the IPMA also considers the average value of the latent variables and their indicators (i.e. performance dimension). From the IPMA figure 3, it is observed that the performance of planning, leading, and controlling were of high performance and average importance than other factors. Nonetheless, the organizing factor show above-average performance with low importance which indicates a need for prodigious attention by managers and IS experts. Furthermore, the ISP awareness construct is a very important factor in determining ISP realization despite its average performance because of its relatively higher total effects (importance) compared to other factors in the proposed model. The IPMA is particularly useful for generating additional findings and conclusions by combining the analysis of the importance and performance dimensions in practical PLS-SEM applications. Thus, the IPMA allows for prioritizing factors to improve a certain target-dependent factor. Expanding the analysis to the indicator level enables identifying the most important areas of specific activities. These results are, for example, predominantly important in practical studies identifying the differing impacts that certain construct dimensions have on phenomena such as ISP compliance, and ISP realization for example.

In contrast, ANN (shown in table 5, and figure 4) identified the leading factor as the most important and controlling as the least important factor in predicting ISP realization by PHE employees. However, leading was ranked equally in both SEM and neural network results. These findings indicate the superiority of using machine learning tools, e.g., artificial neural networks, for the measurement of non-linear relationships over conventional statistical methods, e.g., PLS-SEM that can only analyse the linear relationship (Chan and Chong 2012). This finding provides additional insights to the practitioners about the relative importance of the predictors in exploring PHE employees' ISP realization.

In conclusion, based on the analysis, strong support for the research model was achieved. The study introduces theoretical, methodological and practical contributions. It makes important theoretical contributions to the evolving body of knowledge about how Palestinian employees perceived planning, leading, organizing, and controlling of BRMM theory antecedent to motivational factors that direct their benefit behaviour of perceived realization of ISP, but to the best of our knowledge, this is the first study that, illustrate on the perceived PLOC factors, offers a theoretical exploratory and empirical support for the consequence of perceived benefit realization of ISP by university employees in Palestine. Furthermore, using ISP awareness as InfoSec practices as antecedents to four perceived factors that were extracted from established theories such as BRMM helps us to comprehend employees' awareness of practical ISP on the road to securing the information they work with. The research model determined more insights into how university employees perceive the ISP from their views on the perceived PLOC.

Secondly, the InfoSec countermeasure as ISP awareness contributed as the antecedent to the PLOC model factors to confirm employees' benefits realization of ISPs in the context of Palestine universities as these policies may or may not have been published to university employees *so that* it could offer a sense of consideration by employees on ISP's, therefore methodological contribution. Also, practical contribution as it involves the management process and IT expert in the formation of best InfoSec policies and practices.

Further Studies and Research Limitations

The study's limitation is in the assessment of only four BRM perception factors from well-known theory and using moderation and mediation effects to explore the performance of the research model with participants' profiles. Datasets could cover more organizations and expand significantly in numbers. Meanwhile, the research model results are promising, hence, more empirical quantitative analysis is needed by collecting more data from other Higher Institutions in Palestine. As the IPMA assumes linear relationships, future research could focus on non-linear IPMA results, since the aim is to identify antecedents that have a relatively high importance for the dependent factor, but also have a relatively low performance. Furthermore, future work could identify mixed-mode analysis by incorporating the eight areas of ISM and the BRM theory for further exploration of the benefits realization of InfoSec.

Acknowledgements

My appreciation for the continued support of Al-Quds Open University. This paper and the research behind it would not have been possible without the participation of the university employees of Palestine Higher education. I am grateful to Dr Abd. Rahman Ahlan of the International Islamic University Malaysia for

providing me with a wealth of help and support during the original study on ISP. Thank you for your time and effort.

References

Abdelwahed, A. S., Mahmoud, A. Y., & Bdair, R. A. (2016). Information Security Policies and their Relationship with the Effectiveness of the Management Information Systems of Major Palestinian Universities in the Gaza Strip. *International Journal of Information Science and Management (IJISM)*, *15*(1).

Abdul Molok, N. N., Ahmad, A., & Chang, S. (2010). Understanding the factors of information leakage through online social networking to safeguard organizational information. In *Proceedings of the 21st Australasian Conference on Information Systems*.

Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information security awareness at the knowledge-based institution: its antecedents and measures. *Procedia Computer Science*, *72*, 361-373.

Al-Alawi, A. I., Al-Kandari, S. M. H., & Abdel-Razek, R. H. (2016). Evaluation of information systems security awareness in higher education : An empirical study of Kuwait University. Journal of Innovation and Business Best Practice, 2016. http://doi.org/10.5171/2016.329374

Ali, F., Rasoolimanesh, S. M., Sarstedt, M., Ringle, C. M., & Ryu, K. (2018). An assessment of the use of partial least squares structural equation modeling (PLS-SEM) in hospitality research. *International Journal of Contemporary Hospitality Management*, *30*(1), 514-538

Al-Mashari, M., Al-Mudimigh, A., & Zairi, M. (2003). Enterprise resource planning: A taxonomy of critical factors. *European journal of operational research*, *146*(2), 352-364.

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018, January). An exploratory study of current information security training and awareness practices in organizations. In *Proceedings of the 51st Hawaii International Conference on System Sciences*. DOI: 10.24251/HICSS.2018.635

Alshare, K. A., Lane, P.L., Lane, M.R. (2018) "Information security policy compliance: a higher education case study", Information & Computer Security, Vol. 26 Issue: 1, pp.91-108, https://doi.org/10.1108/ICS-09-2016-0073

Amro, B. (2018), “Cybercrime as a Matter of the Art in Palestine and its Effect on Individuals”, I.J. Wireless and Microwave Technologies, 2018, 5, 19-26**,** DOI: 10.5815/ijwmt.2018.05.03.

Badewi, A. (2016). Investigating benefits realisation process for enterprise resource planning systems.

Breese, R. (2012). Benefits realisation management: Panacea or false dawn?. *International Journal of Project Management*, *30*(3), 341-351.

Cresswell, K., Sheikh, A., Franklin, B. D., Hinder, S., Nguyen, H. T., Krasuska, M., ... & Williams, R. (2022). Benefits realization management in the context of a national digital transformation initiative in English provider organizations. *Journal of the American Medical Informatics Association*, *29*(3), 536-545.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Davenport, T. H. (2000). *Mission critical: realizing the promise of enterprise systems*. Harvard Business Press.

Dhillon, G. (2007). *Principles of information systems security: Texts and cases*. John Wiley & Sons Incorporated.

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE transactions on knowledge and data engineering*, *30*(7), 1366-1385.

Dolan, K. (2018). Embedding Benefits Realization Management into Organizations. In *Implementing Project and Program Benefit Management* (pp. 253-268). Auerbach Publications.

Field, A. (2009). Discopering statistics using SPSS, thrid edition.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, *18*(1), 39-50.

Global Cybersecurity Index [GCI] (2017). GCI Website http://www.itu.int/en/ITUD/Cybersecurity/Pages/GCI.aspx

Hair, J. F., Anderson, R. E., Babin, B. J., & Black, W. C. (2010). Multivariate data analysis: A global perspective (Vol. 7).

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice*, *19*(2), 139-152.

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. In *New challenges to international marketing*. Emerald Group Publishing Limited.

Herath, T. C., Herath, H. S., & Cullum, D. (2022). An Information Security Performance Measurement Tool for Senior Managers: Balanced Scorecard Integration for Security Governance and Control Frameworks. *Information Systems Frontiers*, 1-41.

Iriqat, Y. M., Ahlan, A. R., Abdul Molok, N. N., & Abd Rahim, N. H. (2019). Exploring staff perception of InfoSec Policy Compliance: Palestine Universities Empirical Study. *2019 First International Conference of Intelligent Computing and Engineering (ICOICE)*. https://doi.org/10.1109/icoice48418.2019.9035133

Kline, R. B. (2011). *Principles and practice of structural equation modeling*: Guilford press. ISBN-13: 978-1606238769

Kolosenia, D., Leeb, C. Y., & Leec, G. M. (2018). Security Policy Compliance in Public Institutions: An Integrative Approach. *Journal of Applied Structural Equation Modeling: 2(1),13-28*

Love, P. E., Matthews, J., Simpson, I., Hill, A., & Olatunji, O. A. (2014). A benefits realization management building information modeling framework for asset owners. *Automation in construction, 37,* 1-10.

Palestine Economy Portal [PEP] (2016). Conference on Information Security and Combating Cybercrime Security – Ramallah, https://www.palestineeconomy.ps/ar/Article/8648

Rahman, M. F. W., Kistyanto, A., & Surjanti, J. (2020). Flexible work arrangements in COVID-19 pandemic era, influence employee performance: The mediating role of innovative work behavior. *International Journal of Management, Innovation & Entrepreneurial Research*, *6*(2), 10-22.

Ringle, C. M., & Sarstedt, M. (2016). Gain more insight from your PLS-SEM results: The importance-performance map analysis. *Industrial management & data systems*.

Scheepers, H., McLoughlin, S., & Wijesinghe, R. (2022). Aligning stakeholders perceptions of project performance: The contribution of Business Realisation Management. *International Journal of Project Management*.

Sternad Zabukovšek, S., Kalinic, Z., Bobek, S., & Tominc, P. (2019). SEM–ANN based research of factors' impact on extended use of ERP systems. *Central European Journal of Operations Research*, *27*(3), 703-735.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS quarterly*, 147-169.

Talukder, M. S., Sorwar, G., Bao, Y., Ahmed, J. U., & Palash, M. A. S. (2020). Predicting antecedents of wearable healthcare technology acceptance by elderly: A combined SEM-Neural Network approach. *Technological Forecasting and Social Change*, *150*, 119793.

Ward, J., & Daniel, E. (2006). *Benefits management: Delivering value from IS & IT investments* (Vol. 30). Chichester: John Wiley & Sons.

Ward, J., De Hertogh, S., & Viaene, S. (2007, January). Managing benefits from IS/IT investments: An empirical investigation into current practice. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 206a-206a). IEEE.

Ward, J., Taylor, P., & Bond, P. (1996). Evaluation and realisation of IS/IT benefits: an empirical study of current practice. *European Journal of Information Systems*, *4*(4), 214-225.

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security*. Cengage.

Xu, Z., & Guo, K. (2019). It ain't my business: a coping perspective on employee effortful security behavior. *Journal of Enterprise Information Management*. Vol. 32 No. 5, pp. 824-842. https://doi.org/10.1108/JEIM-10-2018-0229

Yerby, J., & Floyd, K. (2018). Faculty and Staff Information Security Awareness and Behaviours. In *Journal of The Colloquium for Information System Security Education* (Vol. 6, No. 1, pp. 23-23).