OPEN ACCESS Freely available online

ISSN: 2315-7844
Review of Public Administration and Management

Perspective

Evaluation of Information Security in Government

Luo Yan*

Department of Economics and Social Science, Xiamen University, Fujian, China

DESCRIPTION

The extensive use of IT gives a wide range of options for the automation of management systems and an improvement in the effectiveness and calibre of delivered services. In addition, the adoption of IT solutions in the public sector indicates the requirement for service realization security. In order to secure an institution's information resources and ensure the continuous accomplishment of its objective, the Information Security Management System (ISMS) is being deployed within public administration institutions. It is based on risk management of information risks that might have a negative impact on how well a public administration institution functions. ISMS cover a range of planning and organizational endeavours. Therefore, the effectiveness, dependability, and quality of the completed public duties are impacted by cyber security management in the public sector administration. Many nations and companies recognize the necessity of creating effective solutions that enable an improvement in the degree of information security. Multiple instances of scientific research, assessment, and reports, including the findings of control published by the Polish Supreme Audit Office, show that the mentioned requirements regarding information security in public organizations.

The Personal Data Protection Act and the Act on National Cyber Security were among the European Union documents that were enacted in Poland. The level of information security and privacy protection increased as a result of the adoption of European solutions into Polish law. Improvements to the organizational structure and security protocols were impacted by European legal actions. Additionally, there are now more efficient technical and physical protection methods available. Regular staff skill development and training were also significant changes. There are still various information threat weaknesses prevalent in some public administration institutions. Further, as a result of the expansion of specialized equipment and cyber-attacks, the threat landscape is always changing. The environment described suggests that additional study on information security in public administration is required in order to evaluate and enhance the current solutions. Additionally, the research priorities of the European Union in the area of cyber security are included in this research.

The public sector is composed of numerous subsystems that together constitute a complicated mega-system. An interdisciplinary area of study is the organizational and functional complexity of public administration with reference to information security management. IT solutions by themselves are insufficient to guarantee IS protection. Since management and behavioural factors are essential to establishing ISMS in organizations, this address the difficulties of IS Management (ISM) in institutions. The human aspect of security should also be maintained in order to safeguard organizational assets, such as user data and systems, as is particularly clear in social engineering attacks. In modern organizations, the human factor is crucial to the successful implementation of IS, and employee risk perceptions have a big impact on security behaviours. However, with increasing awareness and undergoing IS training, these views can be altered. Intuition tells us that implementing security measures alone is insufficient. Without the need for knowledge of the motivations behind the measures and their intended outcome, they frequently fail or are disregarded. If not, this results in a lack of adoption of IS measures. The cyber security, security objectives, and security strategy of the institution must be understood in the real world of work.

Human Social Engineering (SE) attacks that serve as a springboard for additional cyber-attacks on institutions are one growing concern. Criminals frequently use SE since the chances of success are high and awareness levels are low. In SE, one could be both the producer and the victim simultaneously, depending on the viewpoint perpetrator because one may have made a mistake and broken one's own organization's security policy; victim since such a revelation is always the consequence of deception or manipulation. All things considered, there exist disconnects between human knowledge and attitudes as well as between attitudes and actual human behaviours. Human ISA and IS behaviours is significantly influenced by psychological variables, behavioural control, and the sociocultural, gender, and age environment in nonlinear and complicated interactions. Higher-level ISA abilities are required for this, as well as the

Correspondence to: Luo Yan, Department of Economics and Social Science, Xiamen University, Fujian, China, Email: luoyan@gmail.com

Received: 06-Jun-2022, Manuscript No. RPAM-22-17304; **Editor assigned:** 09-Jun-2022, PreQC No. RPAM-22-17304 (PQ); **Reviewed:** 24-Jun-2022, QC No. RPAM-22-17304; **Revised:** 01-Jul-2022, Manuscript No. RPAM-22-17304 (R); **Published:** 08-Jul-2022, DOI:10.35248/2315-7844.22.10.349

Citation: Yan L (2022) Evaluation of Information Security in Government. Review Pub Administration Manag. 10:349

motivational element of intention. Employees themselves must determine how to adopt IS in their own unique work environments. The senior management has a duty to serve as an example in this situation. In order to ensure that employees follow IS behaviours, management must take the initiative. The goals of the company should be supported by advice as an enabler. This includes comprehending the spirit and purpose of security measures, as well as knowledge of how security mechanisms must be operated.