DOI: https://doi.org/10.31341/jios.43.2.1 UDC 004.056
Open Access Original Scientific Paper

Key Success Factors of Information Systems Security

Krunoslav Arbanas *karbanas@foi.hr*
Paying Agency for Agriculture, Fisheries and Rural Development
Zagreb, Croatia

Nikolina Žajdela Hrustek *nikolina.zajdela@foi.hr*
Faculty of Organization and Informatics
University of Zagreb, Varaždin, Croatia

Abstract

The issue of information systems security, and thus information as key resource in today's information society, is something that all organizations in all sectors face in one way or another. To ensure that information remain secure, many organizations have implemented a continuous, structured and systematic security approach to manage and protect an organization's information from undermining individuals by establishing security policies, processes, procedures, and information security organizational structures. However, despite this, security threats, incidents, vulnerabilities and risks are still raging in many organizations. One of the main causes of this problem is poor understanding of information systems security key success factors. Identifying and understanding of information security key success factors can help organizations to manage how to focus limited resources on those elements that really impact on success, therefore saving time and money and creating added value and further enabling operational business. This research, based on comprehensive literature review, summarizes most cited key success factors of information systems security identified in scientific articles indexed in relevant databases, of which the top three success factors were management support, information security policy and information security education, training and awareness. At the end, article states identified research gaps and provides readers with possible directions for further researches.

Keywords: information security, information systems, success, success factors

1. Introduction

In the late 1990s attacks on information systems evolved from the use of Trojan horses and viruses to sophisticated attacks such as distributed denial-of-service, embedded malicious code in email messages or various forms of malicious software intended for extortion and blackmail. Entering into the 21st century, attacks are no longer just the result of the attackers' desire to show their knowledge, but they aim at achieving financial gain [1]. As a result, there is a certain shift in security countermeasures, from purely technical protection measures that have shown insufficient [2] to a proactive strategic approach that includes other elements of information security, especially

those from the organizational or sociological aspect, since even the best security technology cannot stop the social engineering based attack [1]. One of the first and the foremost challenges faced by information security executives is to successfully balance the need to protect information assets on the one hand and enable operational operations on the other, because over-strict protection can lead to business performance barriers while loose controls can create unacceptable risks for information assets [3]. A modern view of information security requires that an effective information security strategy must be balanced, i.e. designing and implementing security solutions should emphasize the importance of technology, but also the socio-organizational context within the organization [3] and observe information security also as business and social question, not just technical [3], [2].

National Institute of Standards and Technology (NIST) [4] defines *information security* as "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability"; *information systems security* as "the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats" and *cyber security* as "the ability to protect or defend the use of cyberspace from cyber-attacks" where *cyberspace* represents "a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers". As we can see, there are just minor differences between "information security" and "information systems security" so, in this paper they are considered as synonyms. On the other hand, although the terms "information security" and "cyber security" are also often used interchangeably in the literature [5] the mere look on the above definition tells us that there are some differences between these terms.

Accordingly, von Solms and van Niekerk [5] argue that, although there is a major overlap between information and cyber security, these two concepts are not completely analogous. The part that is overlapping is protection of information based assets stored or transmitted using information and communication technology (ICT). The part that differs information from cyber security is the fact that focus of information security are also information based assets stored or transmitted without ICT while the focus of cyber security are non-information based assets that are vulnerable to threats via ICT [5]. Similarly, von Solms and von Solms [6] argue that cyber security is "*a part of information security which specifically focuses on protecting the confidentiality, integrity and availability of digital information assets against any threats, which may arise from such assets being compromised via (using) the Internet*" based on the definition of information security ("*preservation of the confidentiality, integrity and availability of information*") from ISO/IEC 27000 and the definition of cyber security ("*preservation of the confidentiality, integrity and availability of information in Cyberspace*") from ISO/IEC 27032 [6]. Baring that in mind, in this research cyber security will be observed as the part of overall information security.

The main contribution of this research is an overview of the scientific researches in the information systems security domain with identified critical success factors for managing information security as well as suggestions of possible further research. As such, this paper includes only scientific papers regarding information security indexed in ACM Digital Library, IEEE Xplore Digital Library, SCOPUS, Web of Science (WoS) or Google Scholar and does not take into consideration national/international initiatives towards information or cyber security (e.g. Cybersecurity Strategy of the European Union).

Regarding the organization of the rest of the article, it consists of three main parts: the first part deals with general review of researches of information security in organizations, the second part focuses on researches related to the information systems security success while the third part is reserved for critical review and conclusion with suggestions for further research.

2. Information Security in Organizations

Information, i.e. data that has a meaning in a given context and a value for a person in certain circumstances, should be considered as an asset by an organization [7], due to the fact that possessing specific, relevant and accurate information can make a huge difference in organization's performance [8]. Saying that, it is clear that the protection of confidentiality, integrity and availability of information cannot be overemphasized. Confidentiality reflects the protection of data from unauthorized disclosure by sharing this information only among authorized users; integrity refers to the accuracy of information, including the maintenance of origin, completeness and exactness, while accessibility implies providing users with timely information [9].

Organizations are challenged to make information security an everyday practice [10], however, it is often the case that organizations are led by thought "business first, then security" [11] due to perception among employees that security is just on the way and hampers the ability of employees to accomplish tasks [8], [12]. This results with viewing information security as a burden and not wanting to spend money on it [13] and, because of this, organizations often do nothing about security as long as everything is fine, but when things go wrong, they suddenly pay attention, but then one must make much more to recover from an unwanted situation, and complete recovery is sometimes impossible [8]. Employees in charge of information security then become "firemen" to restore operational operations [11], because organizations realize the real value of effective information security only after the negative consequences of security breaches [14].

At a time when many organizations reduce their budget, and thus proactive security spending [15], the organization facing the cost of security decision should first consider the need for spending, bearing in mind that the value of information should justify the cost of protection [16], and only then determine how much and on what to

spend in order to avoid inefficient spending [17]. The economic perspective naturally recognizes that, although investments in information security are good, a higher level of security does not always worth more, since the system cannot be completely secure regardless of the amount of investment [18] and, eventually, will end up under attack, but at least investing in security measures should postponed that. Therefore, the organization should its limited resources, instead of the information with the highest vulnerability due to potentially very high protection costs, focus on medium-vulnerability information using "moderate protection" principle [11], and the optimal investment should not exceed half of expected loss without investing in security [18].

It is emphasized today that information security is no longer a purely technical issue, but primarily a management problem [7], [8], which requires involvement of senior management to incorporate policies, procedures, organizational structures and education, training and employee awareness [2]. Accordingly, since technical solutions are insufficient to address the challenges of information security [19], ever-increasing security needs have expanded the attention of researchers to research of the role of management in information security management [2]. Effective information security management requires a combination of technical and managerial controls for information risk management [2] with an emphasis on people as an essential element of information security [19], [20], [21] where, despite sophisticated technologies and technical measures, employee inattention may continue to jeopardize the organization's security which depends on its users [8], [22], [23].

The literature on information security systems consistently suggests that employees represent the greatest threat to information security and are therefore the weakest link in the information security management process [2], [24], [22], [25], [26]. However, although employees are part of information security issues, they are also part of the solution since education, training and awareness raising increase security compliance with the security policy, and thus the level of security in the organization [2], [27]. Failure to understand the factors that contribute to the success of information systems security implies that implemented information security measures in organizations are less effective, and organizations are difficult to precisely and consistently state the benefits provided by implemented information security as well as ensure optimal use of resources in the future [28].

Security requirements or data sensitivity are nothing lesser in small and medium-sized organizations than large, but small and medium-sized businesses face the challenge of lacking support for information security management due to insufficient awareness of its importance [10]. That is why they, instead of proactive, take reactive attitude according to information security, and consider security technologies as business costs rather than strategic potentials [29] resulting in greater resource constraints and education and training shortages in information systems security

domain [30]. Due to the limited number of employees and technical constraints, small and medium-sized companies often have system administrator who is responsible for system configuration as well as system security management i.e. security settings, as well as security oversight are their responsibilities, which leads to too many rights for the same person [11].

3. Information Systems Security Success

When we talk about the information systems success, we can say that there are several information systems success models, from which the most notably is DeLone & McLean (D&M) success model [31], first developed in 1992 and, after many testing, updated 10 years later. This model is so widespread and widely accepted that it has been cited hundreds of times and is considered one of the most influential theories in contemporary research of information systems domain [32]. The updated version consists of six dimensions (system quality, information quality, service quality, use, user satisfaction, and net benefits). The final construct of "net benefits" (or "net impacts" as the authors call it in the last iteration) measures the outcomes of the system and is inevitably compared to the system goal, and the authors define it as "*the extent to which information systems are contributing (or not contributing) to the success of individuals, groups, organizations, industries, and nations*" [31]. For that reason, the construct "net impacts" is the most contextually dependent and variable of all D&M model elements. For example, net impacts can be: improved decision making, improved productivity, increased sales, reduced costs, increased profits, consumer benefits, and job creation. The same authors still recognize the fact that, as information systems alter and evolve, the interested parties in different contexts alter its purpose and expectations as well as the definition of success. Just economic performance evaluation measures are no longer sufficient and a balanced value definition is needed, which, along with economic, also includes sociological value i.e. tangible and intangible benefits [31].

Accordingly, parallel can be drawn with the *information systems security success*; it is not possible to simply and unambiguously define it since there is a different understanding of this concept in different contexts and in different organizations. For example, the success of an information systems security for an organization that builds its business on classified information can be no data leakage in the past year; for another organization, it can be compliance with regulatory requirements, while for third organization success may be employee satisfaction because the organization is well protecting their personal information. Accordingly, and taking into account D&M's comment on combination of tangible and intangible benefits, Dunkerley & Tejay [28] define the information systems security success as "*cumulative effect of the relationship between information systems experience and user experience* ".

Furthermore, along with the necessary technical controls, researches show growing awareness of the need to emphasize the non-technical side. Thus Al Kalbani et al. [9] cited three contexts for observing the success of information security: technological, which includes security technologies; organizational, which includes communication and management support in promoting information security; and the environment context related to security initiatives due to environmental pressures. The conceptual model developed by Tu & Yuan [33] consists of six constructs: business alignment, organizational support, IT competence, organizational awareness, security control development, and performance of information security management. Norman & Yasin [34] argue that there are four main classes of success factors in information systems security management, which consist of organizational structure, security management practices, environmental impacts and values. Human, technological and process elements needed for construction of the control mechanism have been identified as crucial for successful implementation of information systems security management, while the impact of the environment is seen as contributing to successful security management [34]. Similarly, Zammani & Razali [35] also summarize the factors of success in three aspects: people, organization and process. *People* aspect are key security management players (senior management, security management team, audit team, employees, third parties); *organization* aspect lists important documents that need to be established and monitored (security policies and procedures), while the *process* aspect describes key information security management practices and activities that key players must carry on (e.g. awareness raising, resource planning or risk management [35]).

Giving the above mentioned, some of the key success factors in implementing, accepting or managing information security in organizations found in the literature are: *senior management support* [2], [7], [8], [9], [36], [24], [12], [33], [19], [35], [13], [37], [26], *defined security policy* [8], [7], [9], [36], [24], [12], [19], [35], [38], [37], [26], *education, training and awareness* [7], [8], [9], [36], [24], [12], [33], [19], [35], [2], [13], [38], [37], [39], [26], *defined roles and responsibilities* [7], [9], [10], *information security and business alignment* [24], [33], [13], *information security culture* [10], [24], [19], *budgeting* [8], [36], [37] and *legislative pressure* [7], [9], [19]. Other factors found in the literature include risk assessment [24], [35], security controls [33], [13], improvement of efficiency and productivity [9], [33], security incident management [19], [38], asset management [19], social pressure [9] and ethical behavior [24].

Some of the above-mentioned key success factors recognized by the academia, have been recognized for some time also by the industry, in international security-related standards, such as ISO/IEC 27000 family of standards [40] or the NIST Special Publications (SP) 800 series from the National Institute of Standards and Technology

[41][1]. For the ISO 27000 family, it is most important to mention ISO/IEC 27001:2013 (requirements for Information security management systems), ISO/IEC 27002:2013 (Code of practice for information security controls), ISO/IEC 27005:2018 (Information security risk management), ISO/IEC 27014:2013 (Governance of information security) or ISO/IEC 27035:2016 (Information security incident management). From the NIST SP 800 series that counts over one hundred documents, some of them are, just to mention a few, the NIST SP 800-12 which represents an introduction to computer security, NIST SP 800-53 which contains the master list of security controls, NIST 800-50 which deals with security awareness and training, NIST SP 800-61 which is about incident response or NIST 800-39 which is about managing information security risk.

Despite the fact that the area of information security as well as information systems success has resulted in numerous studies, these two domains are generally treated separately, resulting in the identification of only 4 authors in a total of 3 articles linking the D&M success model with information security while other researches emphasize individual dimensions and not their interaction. Thus, Montesdioca & Macada [42] suggest measuring customer satisfaction using the quality dimensions of D&M model in the context of information security and testing the relationship between quality and customer satisfaction variables through a survey of 176 information system users on their satisfaction with the information security practice. The results showed that the information quality was positively correlated with the user satisfaction; the system quality was negatively related to the user satisfaction, while the service quality was not related to the user satisfaction. Therefore, the relationship between quality variables has shown a positive relationship between them, except in the case of information quality and service quality [30].

Dunkerley's model [28], [14] rests on the same foundations as the D&M model [31], i.e. it starts from the work of scientists Shannon and Weaver, who identified in 1949 three constructs that make a successful communication, whose work Mason in 1978 customized and linked with the information systems domain that provides 3 levels. First level is *technical*, which represents the accuracy and efficiency of the system that produces the information and consists of 3 constructs (information integrity, information system assurance and operations enablement). Second level, *semantic*, represents the success that information has in transmitting intended meaning from sender to recipient, which consists of 2 constructs (user intention and user knowledge). Finally, *effectiveness* level represents the effect of information on user behavior and is also the final construct, the information system security success [28].

[1] All the NIST SP-800 publications were available on https://csrc.nist.gov/ until 21st of December 2018 when, due to the lapse in government funding, csrc.nist.gov and all associated online activities became unavailable until further notice.

As stated before, top three recognized key success factors of information security are *management support*, *information security policy* and *information security education, training and awareness*.

3.1. Management Support

Numerous researches show that management support is a key factor for success in adopting information security in organizations [33], [43], [30]. This support can highlight information security as an important function at the organizational level in many ways, including financing information security awareness education and training, human and financial resources allocation or promoting the importance of security for other employees within the organization [12], [33]. Without the support and involvement of senior management, the creation, training and implementation of security policies are generally not taken seriously [8], [9]. However, the management will not act as support for information security if they do not see that it supports the organization's core business activities and, for that reason, security experts have to explain the needs of security and convince management in its importance in business assurance [8]. In addition, it is important to state that inconsistent management support gives a confusing message to employees, affecting their behavior in terms of compliance. For this reason, for each organization, a documented security policy with clearly defined goals, roles and responsibilities and acceptable behavior towards organizational information assets is necessary [19].

3.2. Information Security Policy

Information security policy describes employee's roles and responsibilities as well as solving specific security issues in protection of organization's resources [22] and is a fundamental tool that translates security expectations into clear, specific and measurable goals and responsibilities [12] linked to organizational goals.

On compliance with the security policy, significant impact has employees' attitudes depending on their level of awareness of information security and conflict of individual interest between security and functionality [12], compliance cost and benefit analysis, management support and beliefs and the severity of sanctions [25]. Siponen et al. [44] point out that employees have to understand that their noncompliance with security policy will be exposed and sanctioned [9], and argue that social pressure by senior management, superiors, colleagues and information security personnel is crucial to boost employee compliance with security policies stating the importance of respecting the security policy. So if an employee perceives a consistent behavior of their colleagues that matches the expectations of a superior, it is more likely that they will follow what other colleagues are doing [12], [21].

Although organizations are making significant efforts to make use of information security policies to improve information security, their impact and efficiency are questionable as employees' compliance with security policy staff remains problematic [12]. Problematic, because, if organizations explicitly do not recognize the various steps required to develop a security policy, there is a risk in policy development that security policy will be poorly designed, incomplete, redundant and irrelevant, and which users will not fully support [43]. Information security policy can be effective in guiding employee behavior by encouraging a strong information security culture, but only if employees know, understand and accept the necessary precautionary measures [45]. Since ambiguous policies can lead to noncompliance because of wrong interpretation due to possible ambiguities in the document itself, clearly explicitly statements, written in simple sentences are desirable [46].

3.3. Information Security Education, Training and Awareness

Through education, training and awareness mechanisms, employees in organizations of different shapes and sizes become aware of information security for making informed decisions while doing their jobs [27]. While education involves learning basic concepts and theoretical concepts from work materials, the training serves to provide employees with skills and knowledge related to information security that are specific to their roles and responsibilities through the use of seminars and workshops. On the other hand, raising awareness serves for focusing employee attention on information security in order to ensure their understanding of their roles and responsibilities in the protection of information [27] that can easily be overlooked if information security is considered as solely IT department's responsibility [23]. The greatest emphasis from these three components is awareness raising, which functions as a tool to familiarize employees with the understanding and acceptance of the information security policy developed by the organization [12]. The ultimate goal of these methods is to change the habits of employees in the organization [8], [39].

4. Conclusion and Further Research

Information security has become one of the key strategic issues in managing an organization, and effective information security management for a long time attacks attention to both professional and academia experts [33]. However, although information security is a recognized problem, it often happens that organizations have little or no understanding of what to do or how. What they need to keep in mind is the fact that information security cannot be achieved without its acceptance in the daily work of the organization [8], [47] since this is a problem that every employee has to face with [11]. It is important to point out that there is no "silver bullet" for effective

information security since today no stand-alone mechanism or technology is not anymore sufficient to ensure success. Instead, effective information security can be achieved by holistic approach that apply multiple mechanisms for aligning organizational and sociological factors within the organization combined with technological competencies [2], [3].

This research reveals that, although the information system success model is considered to be one of the most influential theories in modern researches of information system domain [32], there is not enough researches that link the domains of information security and information system success. There is also a lack of empirical evidence of proposed theoretical frameworks or models of information systems security success. Vast majority of identified success factors are either theoretical or validated only via case study(ies) which calls for action in the information security research field.

Based on previously stated, several possible directions regarding further researches are identified. Namely, future research may explore additional critical factors of information systems security success and include additional relationships in order to get a complete picture of the mechanism that leads to information security success. Second, empirically validation of proposed theoretical models is particularly necessary. Third, it would be interesting to show what leads to establishment of identified critical success factors (e.g. management commitment) within an organization i.e. what affects them or what are its antecedents. Fourth, validated models in one organization/country can be validated in other organization/country and results compared to show if there are any differences regarding industries, size of the organization, political environment in the observed country, etc. Fifth, one of the possible directions is also a literature review about information security key success factors which will take into consideration national/international initiatives towards information or cyber security (e.g. Cybersecurity Strategy of the European Union). Finally, there is a need for more research into the success factors and security challenges associated with new or emerging technologies, such as Internet of Things, cognitive computing, smart cars, smart cities and other new opportunities that bring along new threats.

Identifying the key success factors of information system security and validating its effectiveness within the organization will ultimately enable the organization to make better use of its resources [14] by distinguishing the controls they need from those less important [33] and at the same time create added value and further enable operational business.

References

[1] M. Dlamini, J. Eloff, and M. Eloff, "Information security: The moving target," *Comput. Secur.*, vol. 28, no. 3–4, pp. 189–198, 2009.

[2] Z. A. Soomro, M. H. Shah, and J. Ahmed, "Information security management needs more holistic approach: A literature review," *Int. J. Inf. Manage.*, vol. 36, no. 2016, pp. 215–225, 2016.

[3] T. Kayworth, D. Whitten, M. Q. Uarterly, and E. Xecutive, "Effective Information Security Requires a Balance of Social and Technology Factors," *MIS Q. Exec.*, vol. 9, no. 3, 2010.

[4] R. Kissel, "Glossary of Key Information Security Terms," 2011.

[5] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, 2013.

[6] B. von Solms and R. von Solms, "Cyber Security and Information Security – What goes where ?," *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 2–9, 2018.

[7] Mehdi Kazemi, "Evaluation of information security management system success factors: Case study of Municipal organization," *African J. Bus. Manag.*, vol. 6, no. 14, pp. 4982–4989, 2012.

[8] M. Al-Awadi and K. Renaud, "Success Factors In Information Security Implementation in Organizations," in *IADIS International Conference e-Society*, 2007.

[9] A. Alkalbani, H. Deng, and B. Kam, "A Conceptual Framework for Information Security in Public Organizations for E-Government Development," in *25th Australasian Conference on Information Systems*, 2014.

[10] A. AlHogail and A. Mirza, "A proposal of an organizational information security culture framework," in *Proceedings of International Conference on Information, Communication Technology and System (ICTS) 2014*, 2014.

[11] W. Jin and Z. Yu, "The Analysis of Information System Security Issue Based on Economics," in *2016 International Conference on Information Engineering and Communications Technology*, 2016.

[12] J. Goo, M. S. Yim, and D. J. Kim, "A path to successful management of employee security compliance: An empirical study of information security climate," *IEEE Trans. Prof. Commun.*, vol. 57, no. 4, pp. 286–308, 2014.

[13] C. E. Tu, C. Z., Yuan, Y., Archer, N., & Connelly, "Strategic Value Alignment for Information Security Management: A Critical Success Factor Analysis," *Inf. Comput. Secur.*, vol. 26, no. 2, pp. 150–170, 2018.

[14] K. Dunkerley and G. Tejay, "Developing an Information Systems Security

Success Model for eGovernment Context," *Am. Conf. Inf. Syst.*, vol. Paper 346, pp. 1–8, 2009.

[15] A. Aminnezhad, R. Mahmod, and M. T. Abdullah, "Survey on Economics of Information Security," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 16, no. 7, pp. 99–116, 2016.

[16] K. Haufe, R. Colomo-Palacios, S. Dzombeta, K. Brandis, and V. Stantchev, "A process framework for information security management," *Int. J. Inf. Syst. Proj. Manag.*, vol. 4, no. 4, pp. 27–47, 2016.

[17] A. Stewart, "Can spending on information security be justified? Evaluating the security spending decision from the perspective of a rational actor," *Inf. Manag. Comput. Secur.*, vol. 20, no. 4, p. 312–+326, 2012.

[18] R.-Y. Ye and L.-J. Feng, "Technical and Economic Models of Information Security," in *2015 International Conference on Computer Science and Applications Technical*, 2015, pp. 329–332.

[19] A. N. Singh, M. P. Gupta, and A. Ojha, "Identifying factors of 'organizational information security management,'" *J. Enterp. Inf. Manag.*, vol. 27, no. 5, pp. 644–667, 2014.

[20] J. Anttila and K. Jussila, "Challenges for the Comprehensive and Integrated Information Security Management," *Proc. - 13th Int. Conf. Comput. Intell. Secur. CIS 2017*, pp. 586–589, 2017.

[21] D. P. Snyman, H. Kruger, and W. D. Kearney, "I shall, we shall, and all others will: paradoxical information security behaviour," *Inf. Comput. Secur.*, vol. 26, no. 3, pp. 290–305, 2018.

[22] S. Aurigemma and R. Panko, "A composite framework for behavioral compliance with information security policies," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2012.

[23] Z. Ahmad, M. Norhashim, O. T. Song, and L. T. Hui, "A typology of employees' information security behaviour," in *2016 4th International Conference on Information and Communication Technology, ICoICT 2016*, 2016.

[24] M. A. Alnatheer, "Information Security Culture Critical Success Factors," in *2015 12th International Conference on Information Technology - New Generations*, 2015, pp. 731–735.

[25] P. Ifinedo, "Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance With IS Security Policy Guidelines?," *Inf. Syst. Manag.*, vol. 33, no. 1, pp. 30–41, 2016.

[26] M.-D. Mclaughlin and J. Gogan, "Challenges and Best Practices in Information Security Management," *Mis Q. Exec.*, vol. 17, no. 3, pp. 237–262, 2018.

[27] E. Amankwa, M. Loock, and E. Kritzinger, "A conceptual analysis of information security education, information security training and information security awareness definitions," in *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, 2014.

[28] K. D. Dunkerley and G. Tejay, "A Confirmatory Analysis of Information Systems Security Success Factors," in *Proceedings of the 44th Hawaii International Conference on System Sciences*, 2011, pp. 1–10.

[29] S. Dojkovski, S. Lichtenstein, and M. J. Warren, "Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia," *Ecis*, pp. 1560–1571, 2007.

[30] K. A. Barton, G. Tejay, M. Lane, and S. Terrell, "Information system security commitment: A study of external influences on senior management," *Comput. Secur.*, vol. 59, no. 2016, pp. 9–25, 2016.

[31] W. H. DeLone and E. R. McLean, "IS Success Measurement," *Found. Trends Inf. Syst.*, vol. 2, no. 1, pp. 1–116, 2016.

[32] T. D. Nguyen, T. M. Nguyen, and T. H. Cao, "Information Systems Success: A Literature Review," in *FDSE 2015. Lecture Notes in Computer Science*, 2015, vol. 9446, pp. 242–256.

[33] Z. Tu and Y. Yuan, "Critical Success Factors Analysis on Effective Information Security Management: A Literature Review," in *Twentieth Americas Conference on Information Systems*, 2014, pp. 1–13.

[34] A. A. Norman and N. M. Yasin, "Information systems security management (ISSM) success factor: Retrospection from the scholars," *African J. Bus. Manag.*, vol. 7, no. 27, pp. 2646–2656, 2013.

[35] M. Zammani and R. Razali, "An Empirical Study of Information Security Management Success Factors," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 6, no. 6, pp. 904–913, 2016.

[36] P. Choejey, D. Murray, and C. C. Fung, "Exploring Critical Success Factors for Cybersecurity in Bhutan'S Government Organizations," no. December, pp. 49–61, 2016.

[37] V. Bolek, A. Látecková, A. Romanová, and F. Korcek, "Factors affecting information security focused on SME and agricultural enterprises," *Agris On-line Pap. Econ. Informatics*, vol. 8, no. 4, pp. 37–50, 2016.

[38] S. E. Choi, J. T. Martins, and I. Bernik, "Information security: Listening to the perspective of organisational insiders," *J. Inf. Sci.*, vol. 44, no. 6, pp. 752–767, 2018.

[39] D. Tse, Z. Xie, and Z. Song, "Awareness of information security and its implications to legal and ethical issues in our daily life," *IEEE Int. Conf.*

Ind. Eng. Eng. Manag., pp. 1236–1240, 2017.

[40] "International Organization for Standardization." [Online]. Available: https://www.iso.org/ics/35.030/x/. [Accessed: 29-Dec-2018].

[41] "The Federal Risk and Authorization Management Program (FedRAMP)." [Online]. Available: https://www.fedramp.gov/nist-publications/. [Accessed: 29-Dec-2018].

[42] G. P. Z. Montesdioca and A. C. G. Macada, "Quality Dimensions of the DeLone-McLean Model to Measure User Satisfaction: An Empirical Test on the Information Security Context," in *2015 48th Hawaii International Conference on System Sciences*, 2015, pp. 5010–5019.

[43] S. V. Flowerday and T. Tuyikeze, "Information security policy development and implementation: The what, how and who," *Comput. Secur.*, vol. 61, pp. 169–183, 2016.

[44] M. Siponen, S. Pahnila, and M. A. Mahmood, "Compliance with Information Security Policies: An Empirical Investigation," *Computer (Long. Beach. Calif).*, pp. 64–71, 2010.

[45] A. Da Veiga, "Comparing the information security culture of employees who had read the information security policy and those who had not," *Inf. Comput. Secur.*, vol. 24, no. 2, pp. 139–151, 2016.

[46] M. P. Buthelezi, J. A. Van Der Poll, and E. O. Ochola, "Ambiguity as a Barrier to Information Security Policy Compliance: A Content Analysis," in *2016 International Conference on Computational Science and Computational Intelligence Ambiguity*, 2016, pp. 1360–1367.

[47] J. Abbas, H. K. Mahmood, and F. Hussain, "Information Security Management for Small and Medium Size Enterprises," *Sci.Int.(Lahore)*, vol. 27, no. 3, pp. 2393–2398, 2015.