MANAGERIAL ASPECTS OF INFORMATION SECURITY

Emina HADŽIJUSUFOVIĆ
International Burch University, 71000, Bosnia and Herzegovina
emina.hadzijusufovic@stu.ibu.edu.ba
Muamer BEZDROB
International Burch University, 71000, Bosnia and Herzegovina
muamer.berzdrob@ibu.edu.ba

Abstract
The increasing threat of unauthorized access, theft, and data breaches has become a significant challenge for individuals, businesses, and governments. This study investigates the current state of information security (ISec) in the United Arab Emirates (UAE), focusing on the roles of management commitment, organizational context, and IT department maturity in determining its effectiveness. The research includes a literature review and quantitative analysis, collecting real-world data on the effectiveness of information security practices from 171 participants across different organizations in the UAE. The findings confirm the proposed hypotheses, demonstrating statistically significant positive relationships between ISec Maturity and the independent variables: Organizational Context, IT Maturity, and Management Commitment. These insights offer valuable guidance for managers, IT personnel, and security experts, providing a roadmap for enhancing information security frameworks and ensuring resilient and secure operations across various organizational settings.

Key words: *information security; IT maturity; information security management system; management commitment; organizational context*

JEL Classification: *M15*

I. INTRODUCTION

Information security has become a top concern for organizations in today's digital age. The exponential growth of electronic storage and personal and sensitive information transmission has significantly increased the risk of unauthorized access, theft, and misuse of valuable data. Global business expansion is forced mainly by advancements in Information and Communication Technology (Henderson and Venkatraman, 1999; Lu and Ramamurthy, 2011). While organizations have greatly benefited from information systems in terms of efficiency and productivity, safeguarding sensitive information, valuable assets, and intellectual property against external and internal threats has become increasingly challenging (Solms and Niekrk, 2013). Information security addresses these challenges by protecting information from various threats to ensure cyber resilience and business continuity, reduce risks, and capitalize on business opportunities (Matar, 2018).

In the early 21st century, the primary goal of information security was to identify risks and threats for the organization, protect financial resources, maintain business reputation, and ensure compliance with regulations (Eloff and Solms, 2020). The field of information security is becoming increasingly complex, incorporating various new subjects such as threat intelligence, cloud computing, social engineering, the Internet of Things (IoT), and the risks associated with Artificial Intelligence (AI). This evolution is driven by continuous IT advancements and the expansion of globally interconnected businesses (Matar, 2018). This increased complexity requires organizations to comprehensively understand critical cybersecurity threats to effectively identify and mitigate vulnerabilities and ensure compliance with applicable security regulations.

The main objective of this research is to explore the various factors that contribute to effective information security, including the crucial role of management commitment. This encompasses setting comprehensive security policies and procedures, aligning security initiatives with the organization's overall strategy, and encouraging employees to adhere to best practices. The study also investigates the impact of the IT department's involvement and capabilities on the effective implementation and maintenance of information security measures within an organization in the UAE. Lastly, the study aims to investigate the impact of organizational context, including industry and ownership structure, on the effectiveness of implemented security measures. By examining different organizational contexts, this study aims to identify the key factors contributing to the success and usage of implemented security systems and the challenges organizations may face in different contexts. Given the UAE's proactive approach to embracing advanced technologies and its significant emphasis

on cybersecurity, this study aims to gain insights into the current information security landscape in the UAE and explore potential challenges and opportunities that entities are achieving in their information security management system.

II. LITERATURE REVIEW

Information security is defined as the "effective implementation of policies to ensure confidentiality, availability, and integrity of information and assets to protect from theft, tampering, manipulation, or corruption" (Smith and Jamieson, 2006, p. 25). While this definition primarily focuses on human-induced risks, it does not account for hazards such as environmental or technological disasters (Barton, 2014). Organizations aim to safeguard the confidentiality, integrity, and availability of their information, commonly referred to as the CIA triangle (Baskerville, 2005). Confidentiality ensures information is accessible only to authorized individuals; integrity maintains information's accuracy, consistency, and trustworthiness throughout its lifecycle; and availability ensures that information and systems are accessible and operational for authorized users when needed. The objective of information security is to protect information from threats. According to ISO 27002 (2022), the globally recognized standard for information security, threats are potential sources of unwanted incidents that jeopardize individuals, organizations, information systems, or data. These threats can come from various technological, environmental, or human-related factors and may result from malicious actors, natural disasters, accidents, or system failures. They pose risks to the confidentiality, integrity, and availability of information assets and can exploit vulnerabilities to cause harm. On the other hand, vulnerabilities refer to weaknesses in the implementation, design, operation, or management of an information system or its components. They represent characteristics that threats can exploit to compromise the security of information assets, systems, or entire organizations. Software, hardware, network configurations, processes, or human behaviors can be vulnerable (International Organization for Standardization, 2022). A study conducted by Moștean and Galea (2020) examines the role of Artificial Intelligence (AI) in information security. It underscores the persistent vulnerability posed by the human factor. Despite AI's potential effectiveness in countering threats, human error can undermine its efficacy. Identifying and addressing vulnerabilities is crucial to mitigate risks and prevent potential incidents or breaches, highlighting the importance of proactive security measures in safeguarding organizational assets and data.

Organizations employ various protective measures, known as controls, to safeguard their information from threats. These controls can be categorized into formal, informal, and technological (Alshaikh, 2018). Formal controls are developed based on risk assessment and audit findings, guiding the organization on how to minimize the risks and prevent potential information security incidents. They encompass policies and procedures that advise personnel on security best practices and outline the consequences of non-compliance. Informal controls, on the other hand, focus on influencing the culture of security through training and education. These controls create awareness and foster a security-conscious mindset among individuals within the organization. Lastly, technological controls are designed to restrict access and protect organizational systems, applications, data centers, and networks. Technological controls can include a range of measures, such as intrusion detection systems, strong access and authentication controls, network access control, data loss prevention, and various other mechanisms (Harris and Maymi, 2016). By implementing these diverse controls, organizations can establish a comprehensive security framework that addresses various aspects of information protection, ensuring the confidentiality, integrity, and availability of its valuable assets.

Several government agencies and organizations worldwide have established various standards and guidelines for information security management. These standards and guidelines provide general or specific guidance to organizations on developing, implementing, and maintaining an effective information security program. Some widely accepted and used standards and guidelines include the International Standard ISO 27000 series (International Organization for Standardization, 2022), the NIST Cybersecurity Framework (National Institute of Standards and Technology, 2024), and the Payment Card Industry Data Security Standard (PCI Security Standards Council LLC, 2022). The UAE has also established several rules and standards to guarantee the safety of sensitive data and information among enterprises, such as the Federal Law No. 34 of 2021 on Combating Cybercrimes (UAE Government, 2021), the UAE Information Assurance Standard (Telecommunications and Digital Government Regulatory Authority, 2020), the Information Security Regulation V3 by the Dubai Electronic Security Center (Dubai Electronic Security Center, 2024), and other similar measures. These local regulations aim to ensure data privacy, strengthen cybersecurity posture, and provide a secure digital world for people and businesses.

As an important aspect of information security, the Information Security Management System (ISMS) has been analyzed for this research. An ISMS provides a structured, documented process for managing information

security by defining policies and procedures, conducting risk assessments, enforcing access controls, training employees, and ensuring continuous improvement through regular audits and updates (Savola, Anttila et al, 2006). Governance of ISMS follows the ISO/IEC 27001 "Plan-Do-Check-Act" model, promoting a dynamic approach to security management. Studies highlight that an effective ISMS implementation requires active senior management involvement, which is crucial for resource allocation, policy enforcement, and fostering a security-aware culture. Additionally, they recognize that information security programs require a blend of managerial commitment and technological and non-technological controls (Dhillon, 2007; Hu, Hart et al, 2007; Whitman and Mattord, 2008). Authors claim that management commitment is crucial, as senior executives must view information security as a strategic concern and actively support it (AlGhamdi, Win et al, 2020). Significantly, in accordance with ISO 27001, the UAE Information Assurance Standard (UAE IA), the Information Security Regulation (ISR), and similar standards, management commitment is mandatory for organizations to achieve compliance.

Moreover, a study conducted by Barton et al. (2016) found that a lack of senior management commitment to information security can lead to insufficient resources and support for security initiatives, leading to employees not taking security seriously. Senior management plays a crucial role in influencing employee behavior and beliefs regarding cybersecurity and prioritizes cybersecurity within the organization (Karim and Tornqvist, 2023). Furthermore, the board and executives should understand security efforts and give their full support in order to develop strong security governance. This entails acknowledging the importance of security measures, actively participating in decision-making procedures, assigning enough resources, and promoting a security-aware culture inside the company (Auffret, Snowdon et al, 2017).

Furthermore, a study by Naumann, Olaru et al. (2023) suggests that top management's structured approach, including defining metrics to quantitatively measure its information security posture, significantly helps in decision-making. A structured approach not only quantitatively presents the level of information security but offers the decision-makers faster opportunities to implement and justify risk treatments or investments in information security (Naumann, Olaru et al, 2023).

In conclusion, the literature review emphasizes the critical role of senior management in information security. It emphasizes that top management's active engagement in prioritizing information security measures is critical for establishing and maintaining an effective ISMS within an organization.

III. RESEARCH MODEL

Through the review of the available literature and an in-depth analysis of information security, a research model has been developed to investigate the influence of management commitment, IT maturity, and organizational context as independent variables on the effectiveness of information security.

Organizational context refers to the various factors that characterize an organization, such as its ownership structure, industry, size, and age. These factors can influence the regulatory compliance requirements, data sensitivity, and threat landscape of the organization, affecting its information security needs and practices. According to the X-Force Threat Intelligence Index, different industries are prone to different security risks and are targeted by cyberattacks, indicating a higher need for information security (IBM, 2023). Therefore, the first hypothesis is proposed as follows:

H1: The organizational context has a direct and positive influence on the implementation and effectiveness of information security measures.

IT maturity reflects the IT department's level of involvement and capability in implementing and maintaining information security measures within an organization. It involves the use of advanced technologies, the continuous improvement of IT processes, employee training, and integrating security into all facets of IT operations. A mature IT department is essential for preparing for, identifying, and mitigating security threats, and enhancing the organization's overall security posture (Torten et al, 2018). Therefore, the second hypothesis is proposed as follows:

H2: The level of maturity and capability of the IT department within an organization will have a direct and positive influence on the effective implementation and maintenance of information security measures.

Management Commitment involves the extent to which the senior management supports and prioritizes information security within the organization. It includes allocating resources, establishing policies and

procedures, providing training and education, and fostering a security-conscious organizational culture. Management commitment can significantly enhance the effectiveness of information security programs, ensuring that security measures are comprehensive and well-integrated into the organization's operations (Liua, Wang et al, 2020). Therefore, the third hypothesis is proposed as follows:

H3: Higher levels of management commitment to information security will result in a more effective information security program within an organization.

The three above-stated hypotheses lay the foundation for the corresponding research design and the accompanying research model (Figure 1), which comprise three important determinants of organizational information security maturity.

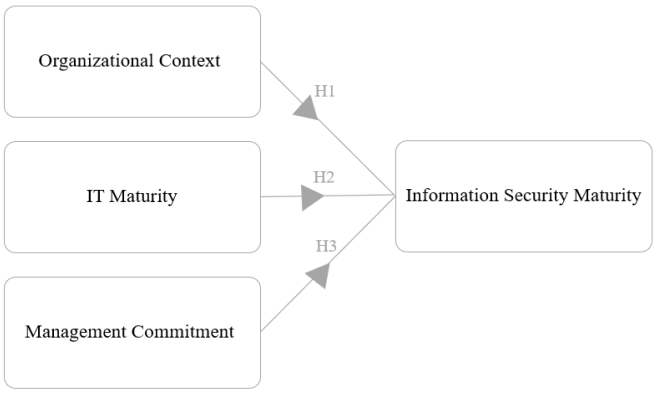

Figure 1 - Research model

IV. DATA AND METHODOLOGY

A questionnaire was developed and used as the primary instrument for data collection to test the research model and hypotheses. It was distributed to 200 employees from different organizations and industries in the UAE, targeting IT personnel, information security personnel, managers, and others involved in information security. The online survey method was chosen as it was easy and accessible, allowing respondents from diverse organizations or locations in the UAE to participate.

The survey achieved a high response rate of 85.50%, with a total of 171 respondents providing their valuable insights. Regarding the respondents' positions, 49.71% are employees in the IT sector, 22.81% hold the position of (Chief) Information Security Officer, and 22.22% hold managerial positions (Management), while the remaining 5.26% hold other positions within their organizations. Overall, the high response rate and the varied representation of respondents' positions within their organizations contribute to the credibility and validity of the study's results. By capturing insights from individuals in key information security roles and those in management and other positions, the study provides a well-rounded understanding of the relationship between management commitment, IT involvement and capabilities, and organizational context on the effectiveness of information security. Regarding the ownership structure of the respondents' organizations, 45.61% are private companies, 38.60% are government entities, and 15.79% are semi-government entities.

The questionnaire was organized into four sections that address information security effectiveness as the outcome variable (*ISec Maturity*) and its three corresponding determinants (predictors): *Organizational Context*, *IT Maturity*, and *Management Commitment*. The first section consists of demographic questions related to the respondents' positions within their organizations, ownership structure, industry, and organization age. The second section assesses the organization's information security practices and compliance. The third section focuses on the organization's IT department and its involvement in information security. The fourth section relates to the level of management commitment to information security within the organization. All model variables are latent and obtained as a linear combination of respective survey questions.

The confidentiality of participants' information was maintained to uphold ethical standards and data privacy regulations. The questionnaire was designed to be anonymous, and the data collected were used only for the purpose of this research. The participants' responses were treated with the utmost care and handled in a way that protected their anonymity. The aggregated data from the dataset were used to present the research results.

Data analysis was performed using SPSS software, with linear regression used to examine the relationships between the independent variables (*Organizational Context*, *IT Maturity*, and *Management*

Commitment) and the dependent variable (*ISec Maturity*). Initially, the dataset contained no missing values. However, three outliers were identified and excluded, resulting in a final sample size of 168. Multiple linear regression was used to test the hypotheses and determine the significance and strength of these relationships.

V. RESULTS AND DISCUSSION

Several assumptions were tested to ensure the validity and reliability of the results obtained from the regression analysis. First, the linear relationships between variables were confirmed using correlation coefficients and residual plots, indicating a proportional change between independent and dependent variables. Second, the independence of errors was assessed using the Durbin-Watson method, with a result of 1.57 (Table 3), suggesting moderate autocorrelation but still meeting the assumption of error independence. The constant variance of errors (homoscedasticity) was verified through residual plot analysis, confirming consistent error variance across all independent variable levels. Next, the normal distribution of errors was evaluated using normal probability plots, showing an approximately normal distribution. Lastly, the multicollinearity among independent variables was assessed using variance inflation factors (VIFs), with all VIF values below 10 (Table 5), indicating no significant collinearity issues.

Additionally, the descriptive statistics - central tendency, variation (Table 1), and correlation coefficients (Table 2), provide valuable insights into the characteristics of all dependent and independent model variables.

Table 1. Descriptive Statistics

Variables	Mean	Standard Deviation
ISec Maturity	10.55	3.71
Organizational Context	5.26	2.57
IT Maturity	14.84	5.94
Management Commitment	15.59	5.96

N = 168

The correlation analysis presents moderate to strong positive linear relationships between *ISec Maturity* and *Organizational Context*, *IT Maturity*, and *Management Commitment*. Notably, all these relationships were statistically significant ($p < 0.001$), emphasizing their importance in achieving the effectiveness of information security measures within organizations. In particular, there is a strong correlation between information security maturity and management commitment, which is a crucial factor in the research. This finding indicates that a higher level of management commitment positively influences the organization's information security maturity, as presented in Table 2.

Table 2. Correlations

Variables	ISec Maturity	Organizational Context	IT Maturity	Management Commitment
ISec Maturity	1.00	0.40 ***	0.66 ***	0.71 ***
Organizational Context	0.40 ***	1.00	0.16 *	0.40 ***
IT Maturity	0.71 ***	0.16 *	1.00	0.76 ***
Management Commitment	0.71 ***	0.40 ***	0.76 ***	1.00

*** - $p < 0.001$; * - $p < 0.05$; N = 168

The results also show that the model has a high R-squared value of 0.57, indicating that the independent variables can explain about 60% of the variation in the dependent variable (Table 3). This means that the model is a good fit and can account for most of the factors influencing *ISec Maturity*. The model has a low standard error of 2.46, indicating little variability in the observed data points around the regression line.

Table 3. Model Accuracy

Model	R	R^2	Adjusted R^2	Std. Error of the Estimate	Durbin-Watson
ISec Maturity	.75	.57	.56	2.46	1.57

Furthermore, the regression model used in the study significantly explains the variations in *ISec Maturity* (Table 4). The high F-statistic value of 72.14 and a high level of significance ($p < 0.001$) indicate a strong relationship between the independent variables (*Organizational Context*, *IT Maturity*, *Management Commitment*) and the dependent variable (*ISec Maturity*).

Table 4. ANOVA Analysis

	Sum of Squares	df	Mean Square	F	Sig.
Regression	1304.52	3.00	434.84	72.14	< 0.001
Residual	988.49	164.00	6.03		
Total	2293.02	167.00			

Table 5 displays the model's coefficients, providing valuable insights into the relationships between the predictor variables (*Organizational Context*, *IT Maturity*, and *Management Commitment*) and the outcome variable (*ISec Maturity*). The coefficient for *Organizational Context* is highly statistically significant (t-value = 3.62, $p < 0.001$), suggesting a positive relationship between *Organizational Context* and the outcome. There is also a significant influence of *IT maturity* on *ISec Maturity*, as indicated by the high statistical significance of the coefficient for *IT maturity* (t-value = 4.35, $p < 0.001$). Importantly, the main subject of this research, the relationship between management commitment and information security maturity, is further highlighted by the statistically significant coefficient associated with *Management Commitment* (t-value = 4.34, $p < 0.001$). This emphasizes how crucial managerial commitment and proactive involvement are in determining information security maturity.

Moreover, the standardized coefficients (Table 5) provide further insight, with *Management Commitment* demonstrating higher standardized coefficients than *Organizational Context* and *IT maturity*. This implies a stronger influence of *Management Commitment* on the dependent variable. With a significant coefficient associated with *Management Commitment*, the findings stress the importance of organizational leaders' proactive engagement in security planning and policy enforcement. Notably, the results indicate that all the independent variables have positive and statistically significant coefficients, suggesting a positive impact on the dependent variable, particularly evident in the significance of the *Management Commitment* variable. The model also has low Variance Inflation Factors (VIFs) for the independent variables, ranging from 1.21 to 2.74, indicating no problematic multicollinearity in the model. These results suggest that the model is valid and reliable and can be used to test the hypotheses.

Table 5. Model Coefficients

Coefficients	Unstandardized Model Coefficients	Standardized Model Coefficients	t-value	Significance	VIF
(Constant)	2.22	-	3.64	< 0.001	-
Organizational Context	0.29	0.20	3.62	< 0.001	1.21
IT Maturity	0.22	0.35	4.35	< 0.001	2.43
Management Commitment	0.23	0.37	4.34	< 0.001	2.74

N = 168

Based on the obtained linear regression results, the research model can be expressed as follows:

$$ISec\ Maturity = 2.22 + 0.29 \cdot Organizational\ Context + 0.22 \cdot IT\ Maturity + 0.23 \cdot Management\ Commitment$$

The results provide strong support for hypotheses H1, H2, and H3, confirming that *Organizational Context*, *IT Maturity*, and *Management Commitment* have positive and significant effects on organizational information security maturity. These findings are consistent with the literature review, which highlighted the importance of these factors in impacting the information security posture of organizations. The results also suggest that *Management Commitment* and *IT Maturity* have slightly stronger effects than *Organizational Context*, implying that these factors are more critical in determining the effectiveness of information security practices. Specifically, the significant impact of management commitment is emphasized, as it involves not only the strategic allocation of resources but also active engagement in security planning and policy enforcement, fostering a security-conscious organizational culture, driving significant improvements in an organization's security posture, and many others. These findings have important implications for managers, IT personnel, and security experts, as they provide a roadmap for enhancing information security frameworks and ensuring resilient and secure operations across various organizational settings.

VI. CONCLUSION

The primary objective of this study was to investigate management commitment and managerial aspects of organizational information security. Two other critical factors were examined, including IT maturity and capabilities and the organizational context. The study's findings emphasize the critical importance of *Organizational Context*, *IT Maturity*, and *Management Commitment* in impacting the maturity of information security (*ISec*) within organizations. The analysis provided strong evidence supporting hypotheses, demonstrating statistically significant positive relationships between *ISec Maturity* as the outcome variable and the independent variables: *Organizational Context*, *IT Maturity*, and *Management Commitment*. The organizational context influences the implementation and effectiveness of information security measures, encompassing elements such as an environment prioritizing security, regulatory requirements, ownership structure, and others. IT maturity emerged as a critical factor, with higher IT maturity correlating with more effective information security practices. This relationship highlights organizations' need to develop and maintain advanced IT capabilities to bolster their security posture. More importantly, management commitment was also a vital component, with strong correlations indicating that dedicated and proactive management significantly enhances the effectiveness of information security programs.

As the central topic of this research, management commitment encompasses several critical aspects that collectively impact the organization's information security posture. It involves strategically allocating resources and ensuring that sufficient budget and personnel are dedicated to information security initiatives. This includes investing in advanced security technologies, hiring skilled security professionals, and providing continuous training and development for existing staff. Additionally, proactive management actively engages in security planning, meaning that leaders are directly involved in developing and implementing security strategies, setting security priorities, and ensuring that the security policies align with the organization's overall strategy and objectives. Enforcing security policies is another crucial aspect of management commitment. Leaders must ensure that security policies are established and consistently applied. Effective leadership in information security is essential for building resilient security frameworks and mitigating potential threats and vulnerabilities. It encourages employees to prioritize security, follow protocols, and feel responsible for the organization's security posture. The study emphasizes that the managerial aspects of information security are crucial for ensuring effective information security within an organization. In conclusion, these findings emphasize the importance of a comprehensive approach to information security, where the organizational context, management commitment, and IT capabilities collectively contribute to achieving high levels of information security maturity.

The study also acknowledges its limitations and provides recommendations for future research. The limitations include the sample size and representativeness, the self-report nature of the data, and the lack of objective measures of information security performance. Future research may address these limitations by expanding the sample size and diversity, employing additional data collection methods, and incorporating objective measures, such as security audits or incident reports. Future research may also explore the implications of emerging technologies on information security practices, such as artificial intelligence, blockchain, cloud security, and the Internet of Things. By addressing these limitations and recommendations, future research could contribute to a more robust understanding of how different factors impact the effectiveness of information security.

VII. REFERENCES

1. AlGhamdi, S., Win, K. T., and Vlahu-Gjorgievska, E. (2020). Information Security Governance Challenges and Critical Success Factors: Systematic Review. Elsevier Ltd. doi:102030.doi: 10.1016/j.cose.2020.102030
2. Alshaikh, M. (2018). Information Security Management Practices in Organisations. Melbourne: The University of Melbourne.
3. Auffret, J.-P., Snowdon, J. L., Stavrou, A., Katz, J. S., Kelley, D., Rahman, R. S., and Warweg, P. (2017). Cybersecurity Leadership: Competencies, Governance, and Technologies for Industrial Control Systems. Journal of Interconnection Networks. doi:10.1142/s0219265917400011
4. Barton, K. A. (2014). Information System Security Commitment: A Study of External Influences on Senior Management. Nova Southeastern University. Retrieved from NSUWorks CEC Theses and Dissertations College of Engineering and Computing.
5. Barton, K. A., Tejay, G., Lane, M., and Terrell, S. (2016). Information system security commitment: A study of external influences. Computers and Security. doi: http://dx.doi.org/doi: 10.1016/j.cose.2016.02.007
6. Baskerville, R. (2005). Information warfare: a comparative framework for business information security. Journal of Information System Security, 1(1), 23-50.
7. Bassanti, H., and Shires, J. (2022). Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy. 29:90–103. doi: https://doi.org/10.1111/mepo.12616
8. Boehmer, W. (2008). Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. The Second International Conference on Emerging Security Information, Systems and Technologies. doi:doi:10.1109/securware.2008.7
9. Chang, S. E., Chen, S. Y., and Chen, C. Y. (2011). Exploring the relationships between IT capabilities and information security management. International Journal of Technology Management. 54(2/3). doi:doi:10.1504/ijtm.2011.039310
10. Cichonski, P., Millar, T., Grance, T., and Scarfone, K. (2012). Computer Security Incident Handling Guide. NIST Special Publication 800-61 Revision 2. doi:dx.doi.org/10.6028/NIST.SP.800-61r2
11. Dhillon, G. (2007). Principles of information systems security: text and cases. Hoboken, NJ: John Wiley and Sons.
12. Dubai Electronic Security Center. (2024, February). Information Security Regulation v3. (DESC) Dubai, UAE.
13. Eloff, M., and Solms, M. (2020). Information Security: Process Evaluation and Product Evaluation. Springer.
14. Flowerday, S. V., and Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who.
15. Grassegger, T., and Nedbal, D. (2021). The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. 181 (2021) 59–66. doi:doi:10.1016/j.procs.2021.01.103
16. Harris, S., and Maymi, F. (2016). CISSP All-in-One Exam Guide 7th ed. New York: McGraw Hill Education.
17. Help AG, a. e. (2023). State of Market Report 2023.
18. Henderson, J. C., and Venkatraman, H. (1999). Strategic alignment: Leveraging Information Technology for Transforming Organizations. IBM Systems Journal, 2, pp. 472-484.
19. Hu, Q., Hart, P., and Cooke, D. (2007). The role of external and internal influences on information systems security – a neo-institutional perspective. The Journal of Strategic Information Systems, 16(2), 153-172.
20. IBM. (2023). X-Force Threat Intelligence Index. IBM.
21. International Organization for Standardization. (2022). ISO 27001:2022, Information security, cybersecurity, and privacy protection — Information security management systems — Requirements. Geneva, Switzerland.
22. International Organization for Standardization. (2022). ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection, Information security management systems requirements. ISO, Geneva, Switzerland. Retrieved from www.iso.org
23. ITU, I. T. (2020). Global Cybersecurity Index (Vol. 4). International Telecommunication Union.
24. Jollans, A. (2018). Three ways to collaborate to improve cybersecurity. Retrieved from ibm.com/blogs: https://www.ibm.com/blogs/systems/three-ways-collaborate-improve-cybersecurity/

25. Karim, A., and Tornqvist, A. (2023). Guardians at the Gate: The Influence of Senior Management on Cybersecurity Culture and Awareness Training. Jönköping University.
26. Liua, C., Wang, N., and Liang, H. (2020). Motivating information security policy compliance: The critical role of International Journal of Information Management. doi:doi.org/10.1016/j.ijinfomgt.2020.102152
27. Lu, Y., and Ramamurthy, K. (2011). Understanding the link between information technology capability and organizational agility: an empirical examination. MIS Quarterly, Vol. 35, no. 4, 931-954.
28. Matar, A. (2018). Factors Influencing the Effectiveness of Information Security Practices in Organizations. University of Jyväskylä.
29. M.O.D, O. (2018). Management Commitment as a Determinant of Information Security Awareness. IOSRJEN, 73-81.
30. Moşteanu, N. R., & Galea, K. (2020). Artificial Intelligence and Cyber Security – Face to Face with Cyber Attack – A Maltese Case of Risk Management Approach. ECOFORUM, 9(2), 22.
31. National Institute of Standards and Technology. (2024, February). The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. doi:https://doi.org/10.6028/NIST.CSWP.29
32. Naumann, M. M., Olaru, S. M., Lampe, G. S., & Pitz, F. (2023). Measuring and Indicating The Level Of Information Security - An Analysis of Current Approaches. ECOFORUM, 12(2). The Bucharest University of Economic Studies.
33. Pavlov, G., and Karakaneva, J. (2011). Information Security Management System in Organization. Trakia Journal Of Sciences, 9.
34. PCI Security Standards Council LLC. (2022, March). The Payment Card Industry Data Security Standard (PCI DSS) v4.0.
35. Ruighaver, A., Maynard, S., and Chang, S. (2007). Organizational security culture: Extending the end-user perspective. Computers and Security, 26(1), 56-62.
36. Savola, R., Anttila, J., Sademies, A., Kajava, J., and Holappa, J. (2006). Measurement of Information Security in Processes and Products. In P. Dosnland, S. Furnell, B. Thuraisingham, and X. Wang, Security Management, Integrity, and Internal Control in Information Systems (pp. 249-265). Springer, US.
37. Smith, S., and Jamieson, R. (2006). Determining key factors in E-government information system security. Information Systems Management, 2, p. Page 25.
38. Solms, V. R., and Niekrk, V. J. (2013). "From information security to cyber security. Computer Security, 38(2), pp. 97-102.
39. Sulaiman, N. S., Fauzi, M. A., Wider, W., Rajadurai, J., Hussain, S., Harun, and Siti, A. (2022). Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review. doi:doi.org/10.3390/socsci11090386
40. Telecommunications and Digital Government Regulatory Authority. (2020, March). UAE Information Assurance Regulation v1.1. United Arab Emirates. Retrieved from www.tra.gov.ae
41. Torten, R., Reaiche, C., and Boyle, S. (2018). The impact of security awareness on information technology. Computers and Security. doi:https://doi.org/10.1016/j.cose.2018.08.007
42. UAE Government. (2021, September). Federal Decree-Law No. (34) of 2021 On Countering Rumors and Cybercrimes.
43. Whitman, M., and Mattord, H. (2008). Management of information security (2nd ed.). Boston, Massachusets: Thomson Course Technology.
44. Whitman, M., and Mattord, H. (2011). Principles of Information Security. Cengage Learning.
45. Wood, C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. Computer Fraud and Security, 2004(1), 16-17.