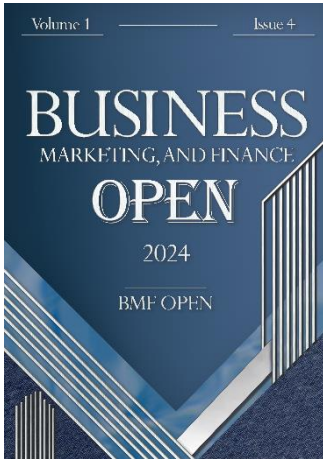# Presenting the Dimensions of the Information Security and Privacy Model for the Audience of Government Communication Offices and the Validation of the Obtained Model

IHAB ABDALWAHID SAGBAN AL- KHAFAJI[1], Hamid Davazdahemami[2,*], HATEM BDAIWI OBAID ALSHAMMARI[3] and Saeid Sharifi[4]

[1] PhD student, Department of Media Management, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran;

[2] Assistant Professor, Department of Management, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran;

[3] Assistant Professor, Faculty of Arts, Media Department, University of Babylon, Iraq;

[4] Assistant Professor, Department of Management, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran;

* Correspondence: h.12emami@khuisf.ac.ir

Abstract: The present study aims to present the dimensions of the information security and privacy model for the audience of government communication offices and to validate the obtained model based on a grounded theory study. This study falls within the category of qualitative research and was conducted using the emergent grounded theory approach. In data analysis, a total of 252 initial conceptual codes, 7 main conceptual codes, and 26 sub-conceptual codes were identified to explain the primary concepts. The findings indicated that the mean scores for each component were above 3, signifying an overall positive evaluation. The degrees of freedom, which equal 374, correspond to a sample size of 375 and are used in the calculation of the t-value. The significance level indicates the probability of observing the data if the null hypothesis is true, and values below 0.05 indicate statistical significance. Overall, the data demonstrated that the components were positively evaluated, and the results were statistically significant. The findings of this study suggest that the dimensions of information security and privacy are perceived as highly important by the audience of government communication offices. These positive evaluations also indicate that the audience expects these offices to continue improving and enhancing their security systems. Given the increasing cyber threats, the importance of these dimensions is felt more than ever before.

Keywords: modeling dimensions, information security, privacy, government communication offices, model validation

1. Introduction

In today's world, information security and privacy are among the primary concerns of organizations and governments at all levels. Particularly in government communication offices, which handle sensitive and critical information related to public and governmental affairs, ensuring information security and protecting privacy are considered key priorities. In this regard, designing appropriate models for managing information security and privacy plays a crucial role in safeguarding personal data and preventing cyber threats [1, 2].

To fully understand these challenges, it is essential to examine the requirements, constraints, and specific risks associated with information security and privacy in government communication offices. These offices manage a vast volume of confidential information, ranging from classified government documents to personally identifiable information (PII) [3, 4].

Government communication offices typically deal with sensitive and classified information, considering information security and privacy as critical concerns. To protect sensitive government data from unauthorized access or leakage, both internally and externally, these offices need to implement proper security practices based on the aforementioned theoretical and research foundations. Additionally, adherence to privacy frameworks ensures that personal data collected and processed by government communication offices are managed in a manner that respects citizens' privacy rights. The audiences of government communication offices, including government officials, employees, and the general public, benefit from the application of these frameworks to maintain trust, confidentiality, and the integrity of communication channels [5].

Due to their continuous interactions with citizens, various organizations, and government institutions, government communication offices have access to a vast amount of sensitive information. Consequently, security threats and risks—particularly from hackers, cyber-attacks, and privacy breaches—have significantly increased. Therefore, information security and privacy models must consider various dimensions, including access control, encryption, monitoring and transparency, employee security training, and risk management to ensure data security and the privacy of citizens and government employees. Information security and privacy provide a framework for understanding and implementing measures to protect sensitive data from unauthorized access, disclosure, alteration, and destruction. These frameworks are crucial for ensuring the confidentiality, integrity, and availability of information across different sectors [6, 7].

In this regard, various security models, such as the Bell-LaPadula model, the Biba model, and the Clark-Wilson model, provide theoretical foundations for structuring and implementing access control policies. These models define rules and principles for managing information security based on factors such as confidentiality, integrity, and separation of duties [8, 9]. Moreover, cryptographic techniques form the cornerstone of secure communications and information protection. The fundamentals of cryptography include concepts such as encryption algorithms, hash functions, digital signatures, and key management. Research in this area continuously explores new algorithms, protocols, and methods to enhance information security [10, 11].

In addition, risk management processes, such as risk assessment, risk analysis, and risk mitigation, form the basis for informed decision-making regarding information security. Theoretical frameworks such as ISO 27005 and NIST SP 800-30 guide organizations in identifying, assessing, and mitigating the risks associated with information assets [12, 13].

However, it should be noted that information security is not solely a technical issue. Human factors significantly impact an organization's security posture. Models such as the Protection Motivation Theory and the Theory of Planned Behavior help in understanding and addressing the human aspects of information security, including user awareness, behavior, and compliance. On the other hand, privacy frameworks such as Fair Information Practice Principles (FIPPs) and the General Data Protection Regulation (GDPR) establish principles and guidelines for managing the privacy of personal information. Research in this area focuses on privacy-enhancing technologies, anonymization techniques, consent management, and privacy-preserving data sharing [2, 14, 15].

Despite significant advancements in the field of information security and privacy, many government communication offices still face considerable challenges in protecting their sensitive data. These challenges arise

due to various reasons, including technical complexities, a lack of adequate training, and the absence of comprehensive and up-to-date models for assessing and managing security and privacy in government organizations. In many cases, existing security models fail to address the specific threats and security needs of these organizations. This research gap highlights the need to develop and validate specific information security and privacy models for government communication offices that can effectively address their unique threats and security requirements. In this regard, it is necessary to identify new dimensions of information security and privacy within the context of government offices and to design models that align with the technical and administrative needs of these institutions. This raises the following question: What dimensions and characteristics should be included in a comprehensive information security and privacy model for government communication offices to effectively identify, assess, and manage cyber threats and protect sensitive data within these organizations?

2. Methodology

The present study employs a mixed-methods approach. The qualitative phase, due to the novelty of the subject, was conducted using the grounded theory method. The participants in the qualitative phase consisted of all experts related to the research topic who possessed relevant academic backgrounds and practical experience. In other words, the target population included specialists in the field of security and privacy protection. The sampling process was carried out using theoretical sampling.

The inclusion criteria for the study were having academic or practical experience, willingness to participate and share experiences, and possessing diverse and varied experiences related to the subject. The exclusion criterion was the participant's unwillingness to continue the interview. Sampling began with the first interview and continued until theoretical saturation was reached. Saturation refers to the point at which the responses of new participants to interview questions are similar to those provided by previous participants. Theoretical saturation was achieved after conducting interviews with 18 experts in related fields.

In the quantitative phase, during the Delphi phase, the same experts were involved, while the survey phase included users and audiences of Iraq's Ministry of Communications. In the quantitative phase, purposive sampling was employed for the Delphi phase, while 375 individuals were selected randomly for the survey phase.

In the qualitative phase, data were collected through semi-structured in-depth interviews (preferably conducted face-to-face, and in exceptional cases—such as when participants were abroad—via online platforms like email, Google Meet, and Skyroom). Sample interview questions included:

- Do you believe that information security and privacy receive adequate attention in government organizations? Why?
- What factors do you consider important for ensuring information security and privacy in your office?
- Does your organization have specific policies to protect personal information and privacy?
- What challenges do you face regarding information security and privacy?
- Have you encountered any incidents of privacy violations or data breaches in your office? How were they handled?
- What actions have you taken to raise awareness among employees and clients about information security risks?
- Do you use specific tools or technologies to manage information security in your office? Please explain.
- How do you assess whether the technologies used adequately ensure information security and privacy?

- In the event of a security breach, what is your organization's incident response and crisis management process?
- Are there inter-organizational collaborations to enhance information security and privacy? If yes, how?
- In your opinion, what changes should be made in the future regarding information security and privacy in government offices?
- How can necessary improvements be implemented in your organization's information security and privacy systems?

In the quantitative phase, data were collected from 375 respondents using a researcher-designed questionnaire based on the qualitative study findings.

The interview process began in early 2023 and continued until early 2024, simultaneously with the coding of data. In the first phase of theoretical sampling, interviews were conducted with 10 participants. As events, concepts, and categories gradually emerged, core categories were identified, leading to the second phase of sampling focused on these categories. The coding in the second phase was based on the influence of core codes on the process.

The data analysis process of the interview transcripts was conducted concurrently with data collection using ATLAS.ti software (version 8). The emerging approach included open coding, selective coding, and axial coding. Throughout the process, theoretical memos were documented. After saturation was reached, theoretical memo sorting was performed, providing an overarching theoretical framework for the grounded theory. Once the memos were sorted, the most suitable theoretical codes were selected. The sorting and coding processes occurred simultaneously.

To ensure the validity and reliability of the research data, four criteria proposed by Glaser (1998)—fit, workability, relevance, and modifiability—were applied. Fit refers to the emergence of categories from the data without being predetermined by theoretical frameworks. This criterion was ensured by deriving categories exclusively from collected data and maintaining a non-judgmental approach. Workability addressed whether the concepts addressed the core issues of participants. In this study, selective coding was derived directly and indirectly from participants, and field notes contributed to interpreting the decisions made by actors in the domain. Relevance was achieved when the theory was meaningful and logical to both participants and stakeholders. This was ensured through semi-structured interviews and the presentation of participants' perspectives. Modifiability indicated that the theory should remain flexible enough to be revised based on new data or changing contexts, implying that the grounded theory process is ongoing and evolving (Lomborg & Kirkehold, 2003).

To enhance the credibility of the research data, sufficient time was allocated for writing theoretical memos throughout the study, and the coding process was reviewed and validated by three participants (as observers) whose feedback was incorporated into axial coding. Moreover, efforts were made to ensure the collection of a wide range of opinions from various relevant fields and to achieve diversity among expert groups to enhance the validity of the interview process.

In the quantitative phase, data analysis was performed using SPSS and AMOS software. The analytical process included calculating statistical indices such as mean, standard deviation, Kendall's coefficient of concordance, and exploratory and confirmatory factor analysis. These analyses were conducted to evaluate the validity and reliability of the questionnaire and the research model.

3. Findings

Following the analysis of interviews conducted with 18 experts in relevant fields, a total of 252 initial conceptual codes, 7 main conceptual codes, and 26 sub-conceptual codes were identified to explain the key concepts, which are discussed in the following sections.

A) Open Coding:

In this stage, the process started with the first interview, and statements were coded as summarized concepts and expressions to facilitate further analysis.

B) Axial Coding:

In this stage, the researcher, after extensive reflection on the subject, logically arranged the concepts around the research questions. The researcher compared, combined, and integrated the categories and concepts obtained from the open coding stage, refining and summarizing them. Through creative and abstract thinking, the researcher connected the meanings derived from the study and categorized them into several key themes or theoretical axes, as shown in Table 1, which presents a sample of the axial coding process.

Quantitative Demographic Findings

The results indicated that the majority of participants belonged to the 31–40 age group, comprising 26.7% of the total sample. This was followed by the 41–50 age group at 21.3%, and individuals aged 30 and below at 20%. The age groups of 51–60 years and those above 60 years each accounted for 16% of the sample. This distribution suggests that the sample primarily consists of middle-aged individuals, with fewer participants in the younger and older age groups. The total sample size was 375 participants.

Additionally, gender distribution results showed that of the 375 participants, 52% were male and 48% were female, indicating a relatively balanced gender representation within the sample.

Educational background analysis revealed that the majority of participants held a bachelor's degree (40% of the total sample), followed by individuals with a master's degree (37.3%). Finally, 22.7% of the sample had a doctoral degree. This distribution highlights a concentration of participants with higher education, particularly at the bachelor's and master's levels, which could contribute to analyses related to educational levels and their impact on the findings.

Table 1. Sample of the Axial Coding Process

No.	Axial Code	Open Codes
1	Data Protection	Importance of data protection, user information security, restricted access to sensitive data
2	Access Management	Unauthorized access, restricted access control, multi-factor authentication, biometric authentication
3	User Training	Periodic training, educating users on new threats, social engineering awareness, phishing awareness
4	System Updates	Security system updates, software updates, access policy updates
5	Threat Detection	Cyber threat detection, suspicious behavior identification, real-time threat monitoring
6	Advanced Technologies Usage	Adoption of emerging technologies, blockchain implementation, smart technology utilization
7	Intrusion Protection	Prevention of unauthorized access, addressing internal and external attacks, system intrusion control
8	Monitoring and Surveillance	Use of monitoring systems, live monitoring, detection of suspicious activities
9	Alert Systems	Implementation of alert tools, intrusion detection systems, anti-malware solutions
10	Security Process Improvement	Enhancing protective processes, upgrading access control policies, improving internal security relations
11	Crisis Management Programs	Incident response, handling cyber incidents, backup and data recovery plans
12	Secure Data Storage	Secure data storage, regular backups, use of secure servers
13	Secure Communications	Secure communication protocols, internal and external secure communications, HTTPS protocol usage
14	Risk Assessment and Analysis	Analyzing past attack data, identifying potential threats, assessing system vulnerabilities

15	Preventive Tools Utilization	Multi-layer firewalls, behavioral analysis tools, anti-phishing systems
16	Password Management	Password management policies, regular password changes, use of complex passwords
17	Physical Data Security	Data center physical security, server protection, advanced physical security measures
18	Backup Programs	Automated data backups, regular backup schedules, backup system testing
19	Network Protection	Wireless network security, strengthening communication networks, preventing unauthorized access to public networks
20	Security Change Management	Managing system changes, resistance to change management, updating new security policies
21	Cryptographic Techniques	Use of encryption techniques, encryption of sensitive data, securing data in transit
22	External Threats Mitigation	Mitigating DDoS attacks, phishing protection, preventing malware and viruses
23	Private Networks Usage	VPN usage, internal private networks, secure network access management
24	Security Culture Development	Promoting security culture, continuous employee education on new policies, strengthening protective culture in government offices
25	Suspicious Behavior Analysis	Identifying suspicious behaviors, behavioral pattern analysis, detecting new threats based on data analysis
26	Advanced Security Systems	AI-based security systems, advanced intrusion detection tools, latest security technologies

These findings provide a comprehensive insight into the key themes related to information security and privacy, offering a basis for developing an effective security framework tailored for government communication offices.

C) Selective Coding:

Selective coding is the final stage of analysis, during which the integration of concepts around a core category takes place, and categories necessary for further refinement and expansion in the future are incorporated. At this stage, analytical notes and diagrams reflect the depth and complexity of the emerging theory. It should be noted that this coherence and integration are not achieved instantly; rather, it is a continuous process that begins with the initial data analysis and extends to the final reporting phase.

In this section, the central category of the research is identified, and the theory is derived, with the main subject being narrated as a story or report based on the collected data, marking the conclusion of the coding process. Table 2 presents the selective coding process.

D) Presentation of the Final Model:

The final information security and privacy model for the audience of government communication offices is illustrated in Figure 1.

Table 2. Selective Coding Process

| Selective Codes	Axial Codes
Data Protection	Data preservation, secure storage, network protection, backup programs
Access Control and Authentication	Access management, authentication and verification, password management, private networks
Training and Awareness	User training, security culture development, awareness of emerging threats
Threat Monitoring and Detection	Threat detection, advanced systems utilization, monitoring and surveillance, suspicious behavior analysis
Advanced Technologies and Tools	Adoption of advanced technologies, preventive tools, alert systems, secure communications
Crisis and Change Management	Crisis management, security change management, system updates, safety process improvement
Risk Analysis and Assessment	Risk assessment and analysis, external threat evaluation, past attack data analysis
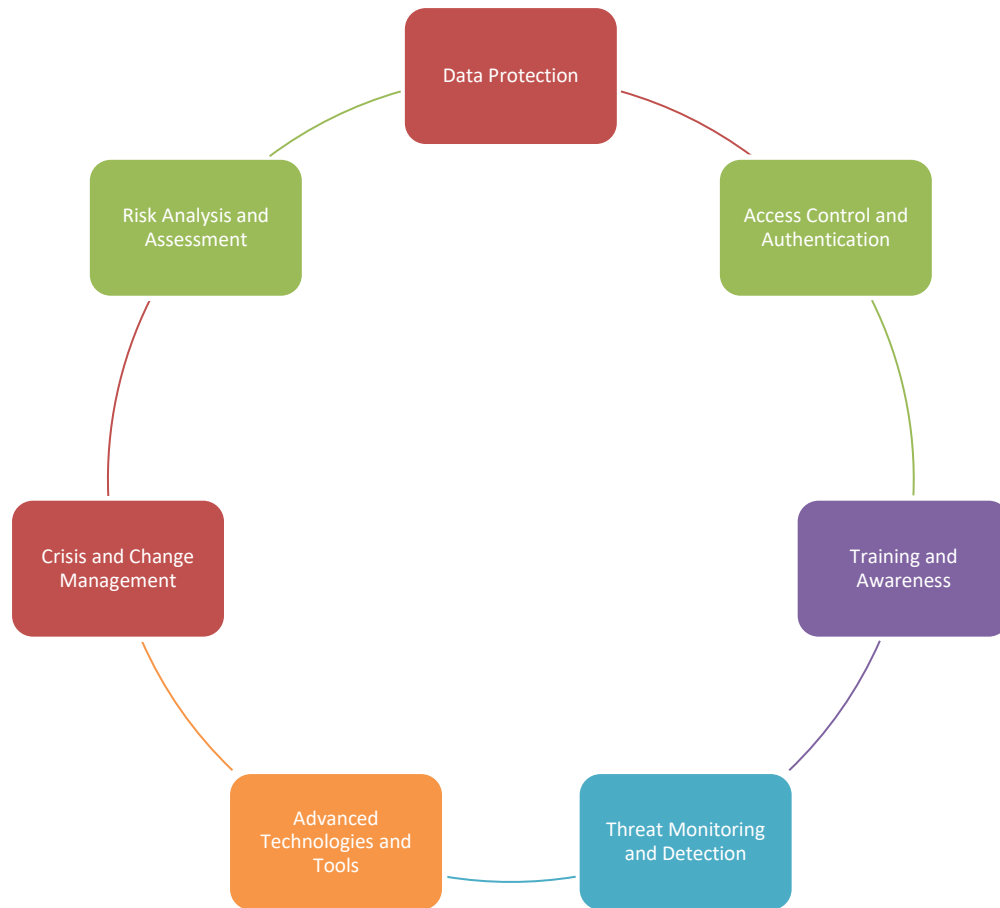
Figure 1. Final Information Security and Privacy Model for the Audience of Government Communication Offices

Table 3. Comparison of Mean Scores for Information Security and Privacy Dimensions with the Hypothetical Mean of 3

Component	Mean	Standard Deviation	Deviation from Mean	t-value	Degrees of Freedom	Significance Level
Data Protection	3.32	0.95	0.32	6.54	374	0.01
Access Control and Authentication	3.39	0.98	0.39	7.61	374	0.01
Training and Awareness	3.34	0.69	0.34	9.55	374	0.01
Threat Monitoring and Detection	3.32	0.90	0.32	6.87	374	0.04
Advanced Technologies and Tools	3.27	0.76	0.27	6.83	374	0.04
Crisis and Change Management	3.36	0.78	0.36	8.85	374	0.04
Risk Analysis and Assessment	3.28	0.96	0.28	5.53	374	0.05

The findings in Table 3 indicate that each component represents different aspects of information security and privacy that were assessed. The mean scores for all components were above 3, reflecting an overall positive evaluation. The standard deviation indicates the degree of dispersion or variability of the scores around the mean for each component. The deviation from the mean shows how far the average score deviates from the hypothetical mean of 3.

The t-value is used to test the hypothesis and determine whether there is a statistically significant difference between the sample mean and the hypothetical mean. The degrees of freedom, equal to 374, represent the sample size of 375 used in the t-value calculation. The significance level indicates the probability of observing the data if the null hypothesis is true, with values below 0.05 indicating statistical significance. Overall, the data show that the components were positively evaluated and statistically significant.

Based on the data and analyses provided in this study, the obtained model demonstrates statistical validity. Kendall's coefficient of concordance was 0.33 in the first round and improved to 0.38 in the second round, indicating an increased level of agreement among panel members.

The standard deviation of importance scores increased from 2.34 in the first round to 2.73 in the second round, reflecting greater diversity in expert opinions. However, the standard deviation of relevance remained stable at 0.15 in both rounds, indicating consistency in expert opinions regarding the relationship between indicators and components.

In terms of significance levels, the highest frequency in the first round corresponded to a significance level of 0.01, while in the second round, the most frequent significance level was 0.001, suggesting improved precision and importance of results in the second round.

Thus, the obtained model is considered to have acceptable validity, indicating an improvement in agreement and precision of expert opinions over successive study rounds.

4. Discussion and Conclusion

The present study aimed to provide dimensions for an information security and privacy model for the audience of government communication offices and to validate the obtained model. The findings indicate that each dimension of information security and privacy was positively evaluated by the audience of government communication offices. The mean scores of these components exceeded 3, suggesting that the audience perceives these dimensions as critical aspects of information security and privacy. This score above 3 indicates that participants in the study have serious concerns about the importance of these dimensions and believe that government communication offices should pay special attention to them.

The standard deviation, which represents the dispersion of scores around the mean, helps to understand the extent of variation among respondents. The results suggest that the variation in evaluations regarding information security and privacy is minor and does not pose significant concerns. Generally, a lower standard deviation indicates higher agreement among participants in the study.

The deviation from the mean helps to determine how far the mean scores deviate from the hypothetical mean of 3. A positive deviation indicates that actual scores exceed the hypothetical mean. In this study, the positive deviation suggests that information security and privacy components were evaluated above expectations and are considered highly important by participants.

The t-value was used as an indicator to test the hypothesis. The results showed that the observed differences between the sample mean and the hypothetical mean of 3 were statistically significant, highlighting the importance of information security and privacy dimensions for the audience.

The degrees of freedom, which equal 374, indicate that 375 individuals participated in the study. The degrees of freedom play an important role in calculating the t-value, as larger sample sizes result in more precise results. In this study, the high degrees of freedom suggest that the sample size was sufficiently large to yield statistically significant results.

The significance level, reported as less than 0.05, means that the probability of obtaining these results under the null hypothesis is very low. In other words, the study confirms that the difference between observed scores and the hypothetical mean is large enough to be statistically significant, emphasizing the reliability of the audience's positive evaluation of information security and privacy dimensions.

These positive evaluations suggest that the audience of government communication offices generally trusts these offices and considers their information security and privacy measures to be effective. This trust could result from effective actions taken by government offices, such as the use of advanced security techniques and ongoing employee training.

On the other hand, the standard deviation in some components indicates diversity in audience perspectives. This variation may stem from individual differences in information security awareness, personal experiences, or access to different technologies. However, these differences are not substantial enough to undermine the statistical significance of the results.

Overall, the findings of this study suggest that information security and privacy dimensions are considered highly important by the audience of government communication offices. These positive evaluations also indicate that the audience expects these offices to continue improving and upgrading their security systems. Given the increasing cyber threats, the importance of these dimensions is more pronounced than ever.

The findings can assist decision-makers in government communication offices in allocating more resources to the development and enhancement of information security infrastructure. Additionally, continuous training in cybersecurity for users can help raise awareness and reduce potential risks.

Finally, the study demonstrates that the current information security and privacy measures of government communication offices are perceived by the audience as effective and efficient.

The overall model fit indices suggest that the data align well with the proposed model. All factor analysis fit indices indicate the suitability of the information security and privacy model for the audience of government communication offices.

The table provided shows the impact coefficients of each information security and privacy dimension on other dimensions, with each row indicating the effect of one component on another. The impact coefficient reflects the degree to which one component influences another, with higher values indicating greater impact. The standard error represents the uncertainty in estimating the impact coefficient. The critical ratio, derived from dividing the impact coefficient by the standard error, is used for significance testing. The significance level indicates the probability of observing the data if the null hypothesis is true, with values below 0.05 indicating statistical significance.

Overall, the results demonstrate how each information security and privacy component can affect others and which impacts are statistically significant.

The validation results for the information security and privacy factor model for government communication offices indicate high quality and efficiency in explaining the relationships between various components of information security. Various indices were used for model evaluation, including degrees of freedom, relative chi-square, comparative fit index (CFI), parsimonious fit index (PNFI), and root mean square error of approximation (RMSEA).

The results suggest that the available data fit well with the proposed model and that the model effectively explains the relationships between information security and privacy components.

For the "Data Protection" component, the relative chi-square index was 2.25, indicating a good model fit. The comparative fit index was 0.95, close to 1, indicating a strong model-data fit. The parsimonious fit index of 0.82 suggests that the model effectively reduces complexity without compromising fit. The RMSEA of 0.05 is an acceptable value for this index.

Similarly, the "Access Control and Authentication" component demonstrated strong performance with a relative chi-square of 1.77 and a CFI of 0.94, indicating good alignment with the collected data. The RMSEA for this component was 0.05, further confirming the model's effectiveness in explaining this aspect of security.

The "Training and Awareness" component had a relative chi-square of 1.6 and a CFI of 0.98, making it one of the best-fitting components in the model. The RMSEA for this component was 0.06, which is within the acceptable range, underscoring the crucial role of training and awareness in the security model.

For the "Threat Monitoring and Detection" component, a relative chi-square of 1.11 and a CFI of 0.93 indicated good model fit. The RMSEA of 0.02 demonstrated high precision in explaining this component.

The "Advanced Technologies and Tools" component showed strong model performance, with a relative chi-square of 1.55 and a CFI of 0.96. The PNFI for this component was 0.88, indicating a good balance between model complexity and fit. The RMSEA was 0.04, which is an acceptable value.

The "Crisis and Change Management" component showed a relative chi-square of 1.96 and a CFI of 0.94, with an RMSEA of 0.02, indicating a strong fit.

Finally, the "Risk Analysis and Assessment" component had a relative chi-square of 2.62 and a CFI of 1.0, showing an excellent fit. The RMSEA for this component was 0.06, within an acceptable range.

The table of impact coefficients shows that "Data Protection" significantly influences other components, with an impact coefficient of 0.54 on "Access Control and Authentication," and a critical ratio of 13.85, demonstrating statistical significance.

The overall findings confirm that the information security and privacy factor model for government communication offices is both well-fitted and statistically significant, making it a reliable tool for analyzing and improving information security measures.

Like other studies, this research faced several limitations. One of the primary limitations was the lack of a predetermined sample size at the outset. Although sampling was conducted gradually until theoretical saturation was achieved, this approach might not have provided sufficient diversity and depth in the perspectives of the interviewees. Another limitation is that the study was conducted exclusively in Iraq and focused on interviews with experts in the field of information security and privacy within the country. This geographic concentration may limit the generalizability of the findings to other countries and cultural contexts. Additionally, the execution and analysis of interviews faced time constraints, which may have affected the depth and accuracy of the analyses. These time limitations could have impacted the quality of concept coding and categorization, potentially leading to missed insights or oversimplification of the data.

Given the high importance of information security and privacy dimensions identified in this study, it is recommended that more advanced and multi-layered authentication systems, such as two-factor authentication and biometric verification, be implemented in government communication offices to enhance the security and accuracy of access to sensitive information. The results also highlighted that training and awareness are critical factors influencing information security. Therefore, it is suggested that continuous and targeted training programs be conducted for government office staff to familiarize them with emerging cyber threats and appropriate countermeasures. Furthermore, to enhance the generalizability of the proposed model, it is recommended that

similar studies be conducted in other countries and cultural settings. Comparative studies across different nations could provide a better understanding of the impact of cultural and organizational factors on information security and privacy practices.

Authors' Contributions

Authors equally contributed to this article.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all participants who participate in this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

[1] y. lu, "Research on Data Privacy Protection and Information Security Algorithm Technology in the Standard Digitalization Background," p. 38, 2024, doi: 10.1117/12.3034787.

[2] O. Layode, "Data Privacy and Security Challenges in Environmental Research: Approaches to Safeguarding Sensitive Information," *International Journal of Applied Research in Social Sciences,* vol. 6, no. 6, pp. 1193-1214, 2024, doi: 10.51594/ijarss.v6i6.1210.

[3] P.-Y. Chen, "Information Security and Artificial Intelligence–Assisted Diagnosis in an Internet of Medical Thing System (IoMTS)," *Ieee Access,* vol. 12, pp. 9757-9775, 2024, doi: 10.1109/access.2024.3351373.

[4] D. Touriano, S. Sutrisno, A. D. Kuraesin, S. Santosa, and A. M. Almaududi Ausat, "The Role of Information Technology in Improving the Efficiency and Effectiveness of Talent Management Processes," *Jurnal Minfo Polgan,* vol. 12, no. 1, pp. 539-548, 05/24 2023, doi: 10.33395/jmp.v12i1.12454.

[5] P. K. Okoth, "Security Challenges in Civil Registration: Safeguarding Vital Information in an Evolving Landscape," *World Journal of Advanced Research and Reviews,* vol. 19, no. 1, pp. 1051-1071, 2023, doi: 10.30574/wjarr.2023.19.1.1203.

[6] A. Nazir *et al.*, "Advancing IoT security: A systematic review of machine learning approaches for the detection of IoT botnets," *Journal of King Saud University - Computer and Information Sciences,* vol. 35, no. 10, 2023, doi: 10.1016/j.jksuci.2023.101820.

[7] G. M. M. Catagua, "Information Security in the Metaverse: A Systematic and Prospective Review," *Código Científico Revista De Investigación,* vol. 4, no. 2, pp. 781-817, 2023, doi: 10.55813/gaea/ccri/v4/n2/257.

[8] S. Kumar and R. R. Mallipeddi, "Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions," *Production and Operations Management,* vol. 31, no. 12, pp. 4488-4500, 2022, doi: 10.1111/poms.13859.

[9] K. G. Chuma and M. Ngoepe, "Security of Electronic Personal Health Information in a Public Hospital in South Africa," *Information Security Journal a Global Perspective,* vol. 31, no. 2, pp. 179-195, 2021, doi: 10.1080/19393555.2021.1893410.

[10] L. Bahrami, N. Safaie, and H. Hamidi, "Effect of motivation, opportunity and ability on human resources information security management considering the roles of Attitudinal, behavioral and organizational factors," *International Journal of Engineering, Transactions C: Aspects,* vol. 34, no. 12, pp. 2624-2635, 2021, doi: 10.5829/ije.2021.34.12c.07.

[11] A. AlShabibi and M. Al-Suqri, "Cybersecurity awareness and its impact on protecting children in cyberspace," in *2021 22nd International Arab Conference on Information Technology (ACIT)*, 2021: IEEE, pp. 1-6.

[12] O. Ali, A. Shrestha, A. Chatfield, and P. Murray, "Assessing information security risks in the cloud: A case study of Australian local government authorities," *Government Information Quarterly*, vol. 37, no. 1, p. 101419, 2020, doi: 10.1016/j.giq.2019.101419.

[13] K. Rantos, A. Spyros, A. Παπανικολάου, A. Kritsas, C. Ilioudis, and V. Katos, "Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem," *Computers*, vol. 9, no. 1, p. 18, 2020, doi: 10.3390/computers9010018.

[14] R. Yousefi Zenouz, S. S. Najafi Esfahani, and I. Kolivand, "Advantages, Considerations, and Solutions to Ensure the Security of the Information Exchange Gateway of the Islamic Republic of Iran," *Intelligent Business Management Studies*, vol. 9, no. 34, pp. 215-246, 2019, doi: 10.22054/IMS.2020.52669.1735.

[15] S. Wang, W. Wang, S. Guan, and N. Guan, "Research on cyberspace security education for teenagers based on data analysis," in *Proceedings of the 2nd International Conference on Information Technologies and Electrical Engineering*, 2019, pp. 1-3, doi: 10.1145/3386415.3386971.