Journal of
Information Systems Engineering
and Business Intelligence

Vol.11, No.2, June 2025
Available online at: http://e-journal.unair.ac.id/index.php/JISEBI

Assessing Information Security Awareness Among Indonesian Government Employees: A Case Study of the Meteorology, Climatology, and Geophysics Agency

Aji Prasetyo [1)*], Rizal Fathoni Aji [2)], Wahyu Setiawan Wibowo [3)]

[1)] *Directorate of Data and Computational, Indonesian Agency for Meteorology, Climatology, and Geophysics (BMKG), Jakarta, Indonesia*
[1)] aji.prasetyo@bmkg.go.id

[2)] *Faculty of Computer Science, Universitas Indonesia, Depok, Indonesia*
[2)] rizal@cs.ui.ac.id

[3)] *Directorate of Statistical Dissemination, Statistics-Indonesia (BPS), Jakarta, Indonesia*
[3)] wahyu.setiawan@bps.go.id

Abstract

Background: Cybersecurity is important for government agencies and the usefulness shows the need for a thorough understanding of information security awareness (ISA) among employees in order to enhance protective measures and ensure compliance with regulations. The Meteorology, Climatology, and Geophysical Agency (BMKG) of Indonesia is very important in providing essential national data and this responsibility shows the need to assess and promote ISA among the employees. The efforts to ensure a robust ISA culture can allow BMKG to safeguard sensitive meteorological and geophysical data, strengthen operational resilience, maintain public trust, and mitigate potential cyber threats that are capable of compromising national security.
Objective: This study aimed to evaluate the level of organizational ISA among employees at BMKG and to improve measures considered important.
Methods: The Human Aspects of Information Security Questionnaire (HAIS-Q) was administered as the reference model to assess the knowledge, attitudes, and behaviors of employees regarding information security. A descriptive statistical analysis and Partial Least Squares Structural Equation Modelling (PLS-SEM) were further applied to analyze data from 459 BMKG employees across various security domains, including password management, email use, internet use, social media use, mobile device security, and incident reporting.
Results: The results showed that BMKG employees possessed a high overall level of ISA (88.06%) with the average knowledge, attitudes, and behaviors recorded to be 88.06%, 81.89%, and 80.74%, respectively. Meanwhile, specific areas such as email use (78.70%) and mobile device use (73.19%) had only moderate awareness. The structural model analysis also showed that behavior exerted the most significant influence on ISA ($\beta = 0.423$), followed by attitude ($\beta = 0.289$) and knowledge ($\beta = 0.214$).
Conclusion: The overall awareness level was positive but there was a need for targeted efforts in password management, email use, and mobile device security to improve ISA practices. Moreover, the implementation of comprehensive information security policies, regular training, and organizational support was suggested to be important for fostering a robust security culture within BMKG.

Keywords: Information Security Awareness, Cybersecurity, BMKG, PLS-SEM, Government Employees, Indonesia

Article history: Received 10 June 2024, first decision 3 January 2025, accepted 26 May 2025, available online 22 July 2025

I. INTRODUCTION

The information and communication technology (ICT) revolution is fundamentally reshaping government operations by enabling seamless communication, increasing transparency in decision-making, and facilitating e-government services and digital engagement [1], [2], [3], [4], [5]. The advancements have further assisted public service accessibility and even supported data-driven policymaking [6], [7]. However, the increased connectivity and reliance on digital systems are exposing governments to information security awareness (ISA) risks, such as phishing, ransomware, and data breaches [7], [8], [9], [10]. This is observed from several reports related to potential financial

* Corresponding author

ISSN 2443-2555 (online) 2598-6333 (print)
doi: http://dx.doi.org/10.20473/jisebi.11.2.126-142

losses at a global scale due to the threats [11], [12], [13]. The risks also extend beyond operational continuity and financial stability to national security [9], [14], [15], [16]. Previous studies showed that the inclusion of comprehensive audits, employee training, encryption protocols, and incident response could serve as the plans to protect sensitive data and critical security [8], [9].

Cybersecurity is another issue with significant impact on governments worldwide and its effect is observed at both the state and local levels [17], [18]. For example, phishing explains how human error remains a significant vulnerability specifically for government employees [17], [19], [20]. The other major issues include ransomware, Internet of Things vulnerabilities, and insider threats [19], [21], [22]. It was also observed that governments worldwide tended to encounter similar gaps in resources and readiness *"to wage war"* against the threats [8], [18], [23]. Moreover, funding, staffing, and governance are the triad of issues that further hinder ISA protection measures. The trend shows the need for regular vulnerability assessments, extensive user training, and improved authentication methods [17], [20], [21], [23], [24], [25]. This is necessary because the continuous adoption of emerging ICT in public sectors is increasing potential cyber-attacks, particularly when security measures are overlooked.

Cyber-attacks on governments can significantly reduce the public trust in the affected institutions [26]. The attacks exploit digital system vulnerabilities to cause substantial economic losses and pose serious risks to national security [9], [27], [28], [29]. For example, the cyber-attacks against e-government initiatives in Nigeria halted nationwide public services for the citizens [30]. India also experienced attacks in the form of ransomware and social engineering against governmental agencies [19]. Even local governments in the United States faced similar vulnerabilities due to inadequate cybersecurity management [17]. The impact extended widely to Ireland which endured cyber-attacks on critical infrastructures as observed in the Cancer Trials Ireland [31]. These incidents showed the pressing need for comprehensive ISA measures to protect national interests and government operations globally.

ISA is practically highly important for employees to address cybersecurity threats. The efforts to equip employees with the knowledge to identify and mitigate risks while ensuring adherence to security policies and best practices have become evident to proactively defend against cyber threats [32], [33]. Previous studies reported the effectiveness of ISA in preventing social engineering attacks [34] and in averting cyber-attacks in Myanmar [35]. Case studies from Saudi Arabia also showed the impact of the efforts of both public and private sectors to wage war against cybercrime [36], [37], [38]. Several factors such as attitude, normative beliefs, and self-efficacy proved influential in employee compliance with InfoSec policies [32], [39]. Moreover, the increasing use of mobile devices in the public sector to access sensitive data showed the need for specialized training and awareness campaigns [40], [41]. Customized education program was reported to further enhance ISA preparedness [40], [41]. The increase in the sophistication of cyber-attacks requires organizations to prioritize educating employees about cybersecurity threats to ensure robust defense mechanisms [42]. This is in line with the concept of *arming the soldiers against cybercrime.*

The mounting cyber threats motivated previous studies to further emphasize the importance of upholding principles such as confidentiality, integrity, availability, authenticity, and accountability in organizational assets and information [10], [43], [44], [45]. There was often a propensity to depend solely on technological solutions such as firewalls and antivirus software to address InfoSec challenges but previous studies suggested that employee awareness and vigilance were equally important in mitigating cyber risks [46], [47], [48]. For example, the Cybersecurity Monitoring Annual Report in Indonesia showed the escalating threat of cybercrime as well as the essence of robust measures to combat data misuse and cyberattacks [49].

An important observation is that ISA for government employees remains incomprehensively understudied [35], [36], [37], [38], [40]. Previous studies mostly did not include *top management* roles in assessing ISA, particularly within government-related institutions [50], [51], [52], [53], despite their increasingly important role in shaping the compliance behavior of employees to cybersecurity practices [38], [54], [55], [56]. Therefore, this study aimed to assess the ISA of government employees in Indonesia due to the dynamic nature of cybersecurity threats experienced. Several factors relating to individual characteristics such as age, gender, education, personality, risk perception, learning style, and internet habits were considered [57], [58], [59]. Organizational factors such as leadership style, trust, culture, management practices, and initiatives for ISA were also examined [60], [61], [62]. The recognition of the complexities can motivate organizations to prioritize improving ISA to effectively mitigate risks and protect critical infrastructure and data assets. The questions formulated to be answered in this study are presented as follows:

RQ1: *How aware are Indonesian Government employees about maintaining ISA?*

RQ2: *What factors contribute to the current ISA among Indonesian Government employees?*

II. LITERATURE REVIEW

A. Information Security Awareness

Information is the bedrock of organizational operations and serves as an important asset in daily functions [63]. This is observed in several forms ranging from the digital data stored on electronic or optical media to physical materials such as papers and intangible knowledge held by employees which are all required to be adequately protected [2], [41]. In private and public sectors, accurate information is vital for optimal operations and this shows the need to uphold its integrity and confidentiality [2], [15], [64], [65], [66]. ISA is focused on safeguarding data stored, transmitted, and processed within networked systems [2], [35], [43], [48] in adherence to standards such as ISO/IEC 27000 that stress the confidentiality, integrity, and availability (CIA) triad [52]. The confidentiality aspect prevents unauthorized access in addition to the protection of privacy and proprietary data. Integrity ensures data remains unaltered and valid while *availability* guarantees timely access [43]. The wide adoption of the CIA triad in diverse industries and governmental bodies [5], [45], [67] shows its high effectiveness for organizational continuity and reputation. However, the concept inherently requires top management commitment to implement robust policies and procedures [25], [40], [68].

ISA is currently and continuously very important in robust security management by *establishing policies*, *maintaining technology infrastructure*, *enhancing employee competence*, as well as *optimizing existing systems and business processes* [16], [32], [69], [70], [71], [72], [73]. Several countries have stressed the importance of cultivating a strong organizational culture and behavior to mitigate cyber threats [74]. Moreover, Parsons et al. [70], Zhen et al. [72], Grassegger & Nedbal [34], and Zulfia et al. [51] profoundly identified the adherence of employees to organizational rules and commitment to implementing best practices as critical elements of ISA. The National Institute of Standards and Technology (NIST) also claimed that ISA remained fundamental for ongoing education in IT security and all personnel were equipped to safeguard ICT assets [75]. NIST strongly supported ISA initiatives associated with inclusive training across all staff levels to ensure heightened awareness and specialized training complement other security measures [76].

TABLE 1
FOCUS AREA OF ISA

Focus Area	Indicator
Password Management	Secure password selection, changing passwords regularly, and not keeping track of passwords
Email Use	Not clicking on malicious email links and not opening malicious email attachments
Internet Usage	Not downloading files or software from unauthorized sources and not accessing questionable websites
Social Media Usage	Not sharing work-related information on social media and not opening social media during office hours
Mobile Device Usage	The danger of using Wi-Fi networks in public areas leads to the adoption of virtual private network (VPN) devices as well as the physical security of mobile devices
Computer Device Security	Locking computer devices when not in use, usage of licensed software, as well as antivirus installation and regular updates
Data & Information Handling	Destruction of sensitive or confidential work documents, regular data backup, as well as data and information exchange without USB devices
Incident Reporting	Report all InfoSec incidents and suspicious individuals
Information Security Policies	Implementation of InfoSec policies in all work units and the importance of InfoSec policies

The regular assessment of ISA is important due to the increasing threat landscape. This has motivated organizations to incorporate ISA measurement models into strategic security objectives. For example, Kruger & Kearney [77] advocated for a model that included knowledge, attitude, and behavior (KAB) to assess awareness levels among employees in various Indonesian organizations and government bodies. This was designed to be based on the criteria that less than or equal to 59% was "*Poor*" scale, 60–79% "*Medium*", and more than or equal to 80% "*Good*" scale [51], [52], [53], [78]. The Human Aspects InfoSec Questionnaire (HAIS-Q) was also used to assess the *knowledge*, *attitudes*, and *behaviors* of employees regarding InfoSec. The instrument covers several aspects such as *password management, email use, internet and social media usage, mobile device usage, computer device security, data and information handling, incident reporting*, and *information security policies* in Table 1 [51], [70], [79]. Each area employs a Likert scale to gauge responses in addressing security threats [51], [53], [80], [81].

B. Previous Studies

Previous studies have thoroughly investigated ISA of employees in diverse organizational settings. For example, Normandia et al. [80] assessed ISA among employees at the Indonesian Ministry of Foreign Affairs and reported an overall awareness level of 78.56%. The study also identified improvement needs in terms of *computer security* and *incident reporting*. Similarly, Zulfia et al. [51] evaluated ISA in a private sector (industrial company) using the HAIS-

Q framework and reported a satisfactory overall awareness but gaps were found in some practices such as *clicking links from known senders* and *accessing suspicious websites*. Another study by Mahardika et al. [53] explored ISA levels at the Centre of Analysis and Information Services, the Judicial Commission Republic of Indonesia and reported *moderate awareness* among employees but stressed the need for continuous training. Furthermore, Sari et al. [64] examined cultural differences in InfoSec across Indonesian healthcare personnel and identified *significant disparities* in security culture among employees of hospitals, clinics, and health centers. The results also emphasized the roles of management support, change management, and knowledge in shaping security behaviors within the healthcare sector.

Alkhazi et al. [73] analyzed the impact of ISA training methods on knowledge, attitudes, and behaviors of employees across various government sectors in Kuwait. The results showed the effectiveness of diverse training interventions with text-based and gamified sessions observed to have significant behavioral improvements compared to video or lecture-based methods. The study assessed awareness levels pre and post-training in addition to the provision of valuable insights into effective training methods. Moreover, complementary studies in Saudi Arabia and Malaysia emphasized the need for structured education campaigns and profoundly showed myriad factors in motivating positive security behaviors through *threat awareness*, *self-efficacy*, and *reward systems* [36], [38], [82]. Normandia et al. [80] and Mahardika et al. [53] studied Indonesian Government employees but the focus was only on the central government *without assessing the local level*. This gap shows the need for more comprehensive studies to conduct the assessment across all levels.

C. Theoretical Framework

The HAIS-Q model is considered very important for evaluating the knowledge, attitudes, and behaviors of employees concerning data and InfoSec practices within organizations [71], [72], [83] [51], [52], [81]. It is based on seven distinct focus areas that assess user behaviors, including password management, email usage, and incident reporting using Likert-scale responses. The model serves as a comprehensive method to assess InfoSec effectiveness [71], [72], [83]. Moreover, the recent trends in cyber incidents within the Indonesian Government which are largely attributed to human error show the urgent need to assess ISA among employees. This study used the knowledge, attitude, and behavior component model developed by Kruger & Kearney [77] and expanded by Parsons et al. [81] to examine knowledge, attitudes, and behaviors. The process was to determine the important role of senior management support in cultivating effective InfoSec cultures and identify the connection between understanding InfoSec practices, attitudes, and behaviors of employees in risk mitigation [81]. The models were used to develop the theoretical framework for this study in Figure 1 and to develop the following hypotheses:

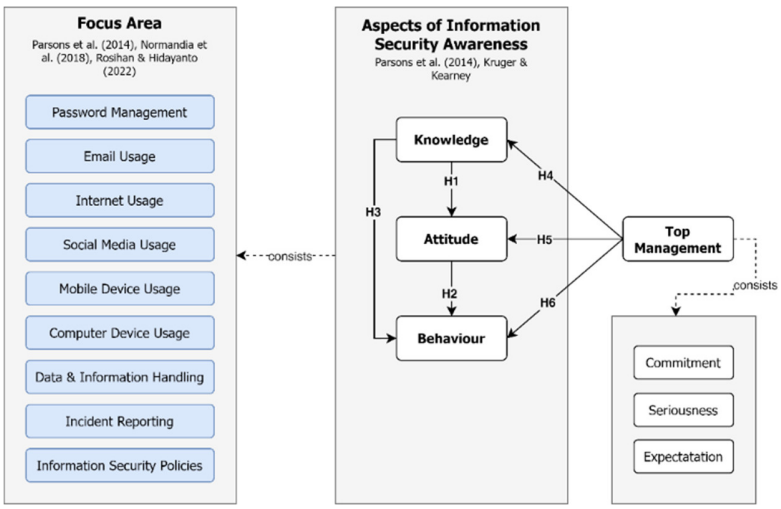

Fig. 1 Theoretical Framework

H1: Employee knowledge of ISA practices and procedures significantly influences the attitudes towards ISA practices and procedures.
H2: Employee attitudes towards ISA practices and procedures significantly influence the behavior in adhering to practices and procedures to maintain ISA.
H3: Employee knowledge of ISA practices and procedures significantly influences the behavior in adhering to practices and procedures to maintain ISA.

H4: Support from the top management level exhibited through commitment, seriousness, and expectations significantly influences employee knowledge of ISA practices and procedures.
H5: Support from the top management level exhibited through commitment, seriousness, and expectations significantly influences employee attitudes toward ISA practices and procedures.
H6: Support from the top management level exhibited through commitment, seriousness, and expectations significantly influences employee behavior in adhering to practices and procedures to maintain ISA.

III. METHODS

A. Study Design and Case Study Location

The maintenance of ISA in Meteorology, Climatology and Geophysics Agency (BMKG) of Indonesia is increasingly crucial due to the reliance on internet-connected services for disseminating vital weather, climate, and seismic data—*on a moment's notice*. The prioritization of SIA stands as a foundational element in safeguarding operational resilience and the integrity of sensitive information that can inherently affect the interests and security of the country [84]. The current proactive method implemented by BMKG includes strengthening its Information Security Management System (ISMS) as part of the strategic initiatives to aim and mitigate potential losses in the face of cyber threats [84]. However, cyber incidents such as hacking and ransomware attacks in early 2023 led to system disruptions, data loss, and encryption of critical geospatial data despite the efforts to adopt advanced security technologies in the form of Security Information and Event Management (SIEM), Endpoint Protection Platform (EPP), and Web Application Firewall (WAF) [85], [86], [87], [88], [89]. The incidents repeatedly show the challenges in ISA implementation and the imminent danger of cyber-attacks.

BMKG is currently a crucial government agency with a significant role in public safety, disaster mitigation, and national infrastructure resilience. The nationwide governance structure ensures that employees operate at central, regional, and local levels, reflecting the broader Indonesian government workforce [90]. The existence of professionals from diverse backgrounds, including IT specialists, meteorologists, and administrative staff shows that BMKG mirrors the composition of other government institutions. Moreover, heavy reliance on digital systems for data collection, analysis, and dissemination exposes the agency to cybersecurity threats that are capable of compromising operations and endangering the country. The adherence of BMKG to national security regulations and international standards like ISO 27001 shows that its cybersecurity practices and challenges are highly relevant to the wider public sector.

The real-time weather forecasts and disaster warnings provided by BMKG have become important for aviation, maritime transport, agriculture, and emergency response [91], [92], [93]. A cyber-attack on the systems of the agency is capable of jeopardizing public safety, disrupting critical services, and eroding trust in government institutions [26], [94]. Moreover, the exposure to cybersecurity risks and the significant role of BMKG in national security and economic stability makes the agency an ideal case for studying ISA among government employees [38], [95]. The assessment of the issue allows this study to provide in-depth valuable insights into cybersecurity preparedness across the Indonesian public sector by identifying key vulnerabilities and strategies for strengthening information security policies at a national level in order *to weather the cyber-storm*.

This study used a quantitative case study method to analyze awareness levels of employees about the InfoSec at BMKG to identify influential factors through surveys and interviews [51], [80], [96]. The selection of BMKG with vertical governance was based on access to both central and local government compared to the focus of previous studies [53], [80]. The trend showed that BMKG employees were a fine representation of the individuals working for the Indonesian Government.

B. Instrument Development

The development of a robust survey instrument is fundamental to any empirical investigation, particularly in relation to quantitative studies which require meticulous questionnaire for data collection and analysis [97]. To ensure the validity and reliability of the questionnaire before full distribution, a mini-pilot survey was conducted among a small group of academics particularly those with government and IT backgrounds. The process assisted in refining the clarity, relevance, and effectiveness of the questionnaire items. The feedback from the experts led to adjustments in wording, question structure, and response formats to ensure the instrument effectively measured the ISA of employees.

The questionnaire used in this study was formulated based on previous literature on factors influencing ISA of employees with a focus on top management as well as the knowledge, attitudes, and behaviors [64], [77], [98]. Demographic inquiries and statements were also included as presented in Table 2 to determine the influence through a Likert scale for nuanced responses [99].

TABLE 2
QUESTIONNAIRE ITEMS

	ID	Item
		Knowledge [50], [51], [52], [53], [70], [100], [101]
Password Management	K_MKS-1	Good passwords are a combination of uppercase & lowercase letters, numbers, and symbols with a minimum length of 8 characters.
	K_MKS-2	Regularly changing passwords will make them more secure than passwords that are never changed.
	K_MKS-3	Keeping passwords visibly accessible to coworkers in office areas poses no risk to InfoSec.
Email Use	K_PEE-1	Emails can contain links that, when clicked, may redirect users to dangerous sites.
	K_PEE-2	Attachments in emails can contain dangerous files that contain viruses/malware.
Internet Usage	K_PEI-1	Downloading applications, images, and videos from unofficial sources can increase the risk of virus or malware attacks.
	K_PEI-2	Checking the destination URL address before accessing an unfamiliar website aims to avoid threats.
Social Media Usage	K_PMS-1	Sharing sensitive/secret work information on any social media platform is strictly prohibited.
	K_PMS-2	Accessing social media during office hours may lead employees to share confidential work-related information.
Mobile Device Usage	K_PPM-1	Information transmitted using public wi-fi networks may be intercepted by third parties.
	K_PPM-2	When working outside the office using a laptop, ensure the laptop is securely maintained
Computer Device Security	K_KPK-1	Computer devices must be protected with passwords and always logged out and locked when not in use.
	K_KPK-2	Using licensed software reduces the risk of virus or malware spreading.
	K_KPK-3	To protect computers from virus/malware threats, antivirus programs must be installed and regularly updated.
Data & Information Handling	K_PDI-1	Sensitive/secret work documents that are no longer needed can be disposed of like regular documents without the need for shredding.
	K_PDI-2	Regularly backing up data in different storage locations can prevent data loss during InfoSec incidents.
	K_PDI-3	Unknown flash drives in the office or elsewhere pose a risk to InfoSec if used as temporary storage and data exchange.
Incident Reporting	K_PIN-1	All InfoSec incidents that occur in the workplace must be reported.
	K_PIN-2	Any strangers or coworkers deemed to pose a threat to InfoSec in the workplace must be reported.
Information Security Policies	K_KKI-1	InfoSec policies need to be established and implemented across all organizational units.
	K_KKI-2	InfoSec policies are crucial to protecting information systems, IT infrastructure, data, and information within organizations.
		Attitude [50], [51], [52], [53], [70], [100], [101]
Password Management	A_MKS-1	I feel unconcerned using passwords with < 8 characters on my accounts and computer devices because it is sufficiently secure.
	A_MKS-2	I feel secure by not regularly changing passwords on my accounts and computer devices, except when I forget my password.
	A_MKS-3	I feel safe writing passwords and sticking them in my workspace because there is no individual in the office except my colleagues.
Email Use	A_PEE-1	I feel curious, if I refrain from clicking on enticing links in emails, even if the sender is unknown.
	A_PEE-2	I feel indifferent and unworried about opening or downloading attachments from emails, even if it is from an unfamiliar sender.
Internet Usage	A_PEI-1	I feel there is no issue in downloading files from unofficial websites if it aids in completing the task at hand.
	A_PEI-2	I feel unconcerned about accessing any website without prior inspection of the URL to be visited.
Social Media Usage	A_PMS-1	I feel no qualms about sharing any work-related information on social media.
	A_PMS-2	I feel no issue in accessing social media during office hours.
Mobile Device Usage	A_PPM-1	I feel secure sending confidential work-related data/information via public Wi-Fi networks using Virtual Private Network (VPN).
	A_PPM-2	I feel there's no problem leaving my laptop unattended for a few minutes while working outside the office.
Computer Device Security	A_KPK-1	I feel secure and unconcerned leaving the computer powered on but not logged out, if it's only for a short period.
	A_KPK-2	I feel secure using unlicensed/pirated software on the computer devices I use for work.
	A_KPK-3	I feel sufficiently secure by only installing antivirus software on my computer, without the need for regular updates.
Data & Information Handling	A_PDI-1	I feel sufficiently secure disposing of unused confidential documents in the trash without shredding them first.
	A_PDI-2	I feel sufficiently secure without the need for regular data backups, as InfoSec incidents rarely occur.
	A_PDI-3	I feel safe if there's an unknown flash drive in the office or elsewhere for temporary storage and data exchange for work purposes.
Incident Reporting	A_PIN-1	I feel there's no need to report InfoSec incidents if I can handle them myself.
	A_PIN-2	I feel there's no need to report strangers or colleagues acting in ways that jeopardize InfoSec if I'm focused on completing my tasks.
Information Security Policies	A_KKI-1	I feel there's no need for InfoSec policies in the office.
	A_KKI-2	I feel InfoSec policies can mitigate InfoSec risks.

TABLE 3 (CONTINUED)
QUESTIONNAIRE ITEMS

	ID	Item
		Behavior [50], [51], [52], [53], [70], [100], [101]
Password Management	B_MKS-1	I do not use recommended passwords (uppercase and others) on all accounts and work on a computer device that I use.
	B_MKS-2	I regularly change passwords on all information system accounts and work on a computer device that I use.
	B_MKS-3	I write down passwords on paper for all accounts and work on a computer device that I use and stick them in the office area.
Email Use	B_PEE-1	I open or click on links that appear interesting in emails, even if they are from unknown senders.
	B_PEE-2	I open or download attachments in emails that appear interesting, even if they are from unknown senders.
Internet Usage	B_PEI-1	I download applications, images, and videos for work purposes from official websites.
	B_PEI-2	I access any website I want by checking the destination URL.
Social Media Usage	B_PMS-1	I send and share anything I want about my work on social media.
	B_PMS-2	I always open social media while working during office hours.
Mobile Device Usage	B_PPM-1	When outside the office, I always use public Wi-Fi networks to open emails or send sensitive/secret work files by activating a VPN.
	B_PPM-2	Sometimes I leave my laptop unattended to go to the bathroom when working outside the office.
Computer Device Security	B_KPK-1	I leave the office computer locked when not in use.
	B_KPK-2	I use/install software on my work computer that does not have an official license.
	B_KPK-3	I use antivirus software and regularly update antivirus programs on the work computer I use.
Data & Information Handling	B_PDI-1	I leave and do not destroy sensitive or secret work documents after they are no longer needed.
	B_PDI-2	I make backups of important work data.
	B_PDI-3	I use any office flash drive as a temporary storage and data exchange place for work data.
Incident Reporting	B_PIN-1	I report InfoSec incidents that occur in the workplace.
	B_PIN-2	I report strangers or coworkers who act to jeopardize InfoSec in my workplace.
Information Security Policies	B_KKI-1	I understand and comprehend InfoSec policies if established as regulations.
	B_KKI-2	I always adhere to InfoSec policies if established as regulations.
		Top Management [64], [98]
	TM-1	Top managements consistently show commitment to InfoSec.
	TM-2	Top managements regard InfoSec as a matter of utmost seriousness and importance.
	TM-3	Top managements elucidate what is expected of employees regarding InfoSec.

C. Data Collection

The targeted population were individuals who shared common characteristics which reached 5,310 employees. The minimum required sample size was determined based on factors such as the number of formative indicators per construct (21 indicators) and the structural paths (3 paths) [102]. The calculation recommended a sample size of 30 to 210 individuals. However, to ensure statistical reliability with a 95% confidence level and a 5% error, this study applied the Slovin formula which led to a sample size of 359 employees [103].

The digital or online survey method was based on a targeted method to explore the *knowledge, attitudes*, and *behaviors* of employees regarding ISA. The questionnaire distributed via Google Forms facilitated data collection through the internal communication channels of BMKG, including *email* and *WhatsApp groups*. Representation was ensured across different departments through a quota sampling method to achieve inclusivity and comprehensive data collection.

The process of collecting the data was initiated through an extensive outreach across the operational units of the organization via internal communication channels and the questionnaire was accessible from 3rd October to 17th October 2023. A dataset of 459 valid responses was obtained after initial validation procedures were conducted to ensure data integrity by requiring complete responses as well as identifying and excluding hastily completed surveys associated with a lack of engagement. The study's objectives, procedures, and participants' rights were fully disclosed, and consent was documented in line with standard research protocols

D. Analysis

Data were processed through descriptive statistical analysis as the primary method for interpretation. This method facilitated the presentation of ISA scores across dimensions and focus areas to ensure a comprehensive understanding of awareness levels associated with employees within the BMKG context [51], [80]. Kruger & Kearney [77] proposed a model for measuring ISA through the categorization of awareness levels as Poor (≤ 59%), Medium (60–79%), and Good (80–100%). This scale provides a structured framework for assessing the understanding, mindset, and practices of individuals in relation to information security [51], [52], [53].

The analytical phase applied the multivariate analysis in the form of Structural Equation Modelling (SEM) using Partial Least Square (PLS) – SEM as a powerful tool for unraveling the complex interplay among multiple variables [104], [105], [106]. The evaluation of the *reflective measurement model* included examining reflective indicator

loadings, ensuring internal consistency using measures such as Cronbach's Alpha and Composite Reliability (CR), assessing convergent validity through Average Variance Extracted (AVE), and confirming discriminant validity using stringent criteria [104], [105], [106], [107]. In the subsequent phase of *structural model assessment*, path coefficients were analyzed to understand causal relationships between predictor constructs and evaluate the coefficient of determination (R^2) to gauge explanatory power [104], [105], [106], [107]. This thorough method ensured the reliability and robustness of the analysis by validating hypotheses and identifying significant factors influencing model outcomes [99], [104], [105], [106], [107].

IV. Results

A. Respondents Demography

The data presented in Table 4 showed that most respondents were male employees comprising 276 individuals (60.13%) while female were 183 (39.87%). There was significant diversity in educational attainment with the largest proportion, 301 employees (65.58%), holding a bachelor's degree followed by 119 (25.93%) with a master's degree while only 5 (1.09%) had a doctoral degree. In terms of age groups, the majority was 30–39 years old with 187 employees (40.74%) followed by 113 (24.62%) aged between 20–29 years and 116 (25.27%) in the 40–49 years group while the smallest was aged 50 years and above with only 43 employees (9.37%). It was also observed that the majority had educational backgrounds outside the field of Information Systems or Information Technology (IS/IT) with 396 employees (86.27%) found to be in accounting while those with IS/IT educational backgrounds were 63 (13.73%).

TABLE 4
Respondents Demography

Demographic Variable/ Item	n	%	Demographic Variable/ Item	n	%
Gender			Education		
Male	276	60.13	High School Graduate	6	1.31
Female	183	39.87	College Diploma	28	6.10
Age			Bachelor/Four-year college	301	65.58
20–29	113	24.62	Master's degree	119	25.93
30–39	187	40.74	Doctor	5	1.09
40–49	116	25.27	Background		
> 50	43	9.37	IS/IT	63	13.73
			Non-IS/IT	396	86.27

B. Descriptive Analysis

Descriptive statistical analysis was used to assess awareness levels across various aspects with the results presented in Table 5. The evaluation showed generally strong knowledge with an average of 88.06% but email usage was slightly lower at 78.70%. Attitudes towards InfoSec were also positive with an average of 81.89% but areas such as password management, social media usage, and mobile device security showed moderate awareness levels. Moreover, behavioral scores averaged 80.74% with areas such as mobile and internet usage, and computer security showing moderate awareness. Mobile device usage was specifically 73.19% and this showed the need for targeted interventions to enhance InfoSec practices among BMKG employees.

TABLE 5
ISA Score

Focus Area	Knowledge	Attitude	Behavior a)	Average
Password Management	90.90*	78.98**	82.59*	84.16*
Email Use	78.70**	90.03*	91.39*	86.71*
Internet Usage	87.31*	84.10*	74.35**	81.92*
Social Media Usage	82.72*	78.21**	81.70*	80.88*
Mobile Device Usage	90.36*	67.73**	61.49**	73.19**
Computer Device Security	90.58*	82.28*	77.87**	83.58*
Data & Information Handling	87.78*	88.02*	85.97*	87.26*
Incident Reporting	88.64*	84.18*	83.74*	85.52*
Information Security Policies	95.59*	83.44*	87.58*	88.87*
Average	88.06*	81.89*	80.74*	83.56*

Note: *) Good, **) Medium, ***) Poor

C. Multivariate Analysis

Multivariate analysis with PLS-SEM was administered to explore the factors influencing ISA. Moreover, the guidelines presented by Hair et al. [102] were followed to assess the quality of reflective measurement models with a

focus on reflective indicator loading, AVE examination, heterotrait-monotrait (HTMT) tests for discriminant validity, and internal consistency reliability tests for CR. Outer loading values below 0.400 were removed and those between 0.400 and 0.700 were scrutinized for the impact on AVE as presented in Table 6. The results of AVE after refinement showed strong convergent validity across all constructs. Furthermore, the HTMT ratios confirmed effective discriminant validity because all values were below 0.90 and this ensured clear differentiation among the measured constructs.

TABLE 6
FIRST ORDER INDICATOR LOADING

Item	Outer Loading	Item	Outer Loading	Item	Outer Loading
K_KKI-1	0.929	A_KKI-1	0.983	B_KKI-1	0.911
K_KKI-2	0.928	A_KKI-2	-0.184	B_KKI-2	0.934
K_KPK-1	0.791	A_KPK-1	0.762	**B_KPK-1**	**0.358**
K_KPK-2	**0.536**	A_KPK-2	0.842	B_KPK-2	0.817
K_KPK-3	0.781	A_KPK-3	0.853	B_KPK-3	0.713
K_MKS-1	0.836	A_MKS-1	0.798	B_MKS-1	0.745
K_MKS-2	0.812	A_MKS-2	0.799	B_MKS-2	0.569
K_MKS-3	**0.371**	A_MKS-3	0.727	B_MKS-3	0.764
K_PDI-1	**0.286**	A_PDI-1	0.818	B_PDI-1	0.768
K_PDI-2	0.799	A_PDI-2	0.88	**B_PDI-2**	**0.539**
K_PDI-3	0.782	A_PDI-3	0.847	B_PDI-3	0.785
K_PEE-1	0.916	A_PEE-1	0.884	B_PEE-1	0.953
K_PEE-2	0.919	A_PEE-2	0.909	B_PEE-2	0.953
K_PEI-1	**0.324**	A_PEI-1	0.879	B_PEI-1	1
K_PEI-2	0.975	A_PEI-2	0.896	**B_PEI-2**	**-0.166**
K_PIN-1	0.886	A_PIN-1	0.886	B_PIN-1	0.93
K_PIN-2	0.854	A_PIN-2	0.907	B_PIN-2	0.923
K_PMS-1	0.829	A_PMS-1	0.867	B_PMS-1	0.848
K_PMS-2	**0.667**	A_PMS-2	0.81	B_PMS-2	0.821
K_PPM-1	0.776	A_PPM-1	-0.769	**B_PPM1**	**-0.862**
K_PPM-2	0.788	A_PPM-2	0.872	B_PPM2	0.842

Henseler et al. [108] stated that HTMT values above 0.9 showed strong correlations between reflective constructs and this led to difficulty in the differentiation process. The factors contributing to the high values include similarities between constructs, excessive indicators, or measurement flaws. Therefore, it was important to carefully examine correlations among variables and provide averages to identify similarities. The process led to the removal of indicators such as *A_PMS-2, A_KPK-3, B_KPK-2, A_PEI-2, K_KPK-3, K_PPM-2,* and *K_PMS-1*. The elimination of these variables and recalculation using SmartPLS provided HTMT ratio values <0.90. The next step after assessing first-order constructs was to save the scores for latent variables in the process of preparing for the evaluation of second-order reflective models [109].

TABLE 7
SECOND ORDER INDICATOR LOADING

Indicator	Attitude	Indicator	Behavior	Indicator	Knowledge	Indicator	Top Management
A_KKI	0.762	B_KKI	0.497	K_KKI	0.758	TM1	0.954
A_KPK	0.793	B_KPK	0.377	K_KPK	0.696	TM2	0.945
A_MKS	0.743	B_MKS	0.701	K_MKS	0.641	TM3	0.927
A_PDI	0.861	B_PDI	0.721	K_PDI	0.717		
A_PEE	0.742	B_PEE	0.732	K_PEE	0.453		
A_PEI	0.698	B_PEI	0.645	K_PEI	0.648		
A_PIN	0.800	B_PIN	0.582	K_PIN	0.721		
A_PMS	0.666	B_PMS	0.715	K_PMS	0.357		
A_PPM	0.722	B_PPM	0.645	K_PPM	0.558		

The assessment of second-order reflective measurement models in PLS-SEM mirrored the first-order models and the focus shifted to reliability and validity assessments [102], [104], [105], [106] These included tests for *convergent validity*, *discriminant validity*, and *internal consistency* using Cronbach's alpha and composite reliability. Reflective indicator loadings were assessed with AVE and HTMT tests to ensure the robustness and validity of the models. The results presented in Table 7 showed the importance of maintaining outer loading values >0.400 to ensure construct validity. Variables such as K_PMS and B_KPK were flagged for potential removal due to inadequate loading values of 0.357 and 0.377, respectively. Table 8 further shows that AVE values exceed 0.50 for all constructs as an indication of a strong convergent validity. The CR values were also within acceptable ranges which confirmed the internal consistency and reliability of second-order constructs with the figures between 0.7 and 0.9 representing satisfactory

to excellent reliability. This evaluation showed the theoretical constructs and ensured the reliability of measurement tools in PLS-SEM analysis.

TABLE 8
CONSTRUCT VALIDITY AND RELIABILITY

Variable	AVE	Result	CR	Result
Knowledge	0.598	Valid	0.856	Reliable
Behavior	0.613	Valid	0.863	Reliable
Attitude	0.616	Valid	0.918	Reliable
Top Management	0.887	Valid	0.959	Reliable

A discriminant validity test was used to evaluate the effectiveness of measurement instruments. The method applied in this study deviated from the Fornell-Larcker criteria and opted for the HTMT due to the perceived superiority as suggested by Henseler et al. [108]. Therefore, values higher than the threshold necessitated a thorough examination of correlation coefficients and the potential elimination of variables exhibiting consistently high correlation ratios as presented in Table 9.

TABLE 9
HTMT RATIO FOR MAIN CONSTRUCTS AND COEFFICIENTS OF DETERMINATION

Variable	Coefficient of Determination		HTMT			
	R^2	R^2 Adjusted	Knowledge	Behavior	Attitude	Top Management
Knowledge	0.077	0.074				
Behavior	0.219	0.216	0.613			
Attitude	0.583	0.580	0.557	0.891		
Top Management			0.328	0.216	0.204	

The coefficient of determination (R^2) determined the coordination level of the predictions with the sample construct internally. The application was based on the criterion that higher R^2 values showed better model performance while lower values showed potential constraints or overlooked factors. The model used in this study was able to explain approximately 7.4% of the variability in knowledge (modest) and accounted for 21.6% in attitudes. It also had significant predictive success by explaining 58% of the variation in behavior. The evaluation of reflective measurement and structural models was followed by hypothesis testing. This was achieved by using t-statistics and p-values to decide the acceptance or rejection of the proposed hypotheses in order to identify influential factors within the study model. The evaluation process included checking when t-statistic values exceeded critical thresholds for one-tailed testing which was 1.28 at a 10% significance level, 1.65 at a 5%, and 2.33 at 1%. Furthermore, p-values were used to assess the significance levels with values below 0.05 considered significant at the 5% level. The results presented in Table 10 showed that hypotheses regarding the relationships between *knowledge and attitude* (H1), *attitude and behavior* (H2), and *knowledge and behavior* (H3) had significant **positive** correlations. This was because the t-statistic values exceeded critical thresholds and p-values were below 5%. Similarly, the hypothesis on the *influence of top management on knowledge* (H4) showed significant **positive** correlations. The hypotheses related to the *influence of top management on attitude* (H5) and *behavior* (H6) also showed positive correlations but **did not reach significance** at the 5% level.

TABLE 10
SUMMARY OF HYPOTHESES TESTING

	Relation	β	T Statistics	P Values	Result
H_1	Knowledge → Attitude	0.447	8.015	0.000	Approved
H_2	Attitude → Behavior	0.669	8.529	0.000	Approved
H_3	Knowledge → Behavior	0.165	2.488	0.007	Approved
H_4	Top Management → Knowledge	0.278	6.502	0.000	Approved
H_5	Top Management → Attitude	0.063	1.537	0.063	*Rejected*
H_6	Top Management → Behavior	0.014	0.424	0.332	*Rejected*

V. DISCUSSION

A. Employee Awareness (Addressing RQ1)

The enhancement of ISA at BMKG requires immediate and strategic attention in several critical areas. This can be initiated by implementing *effective password management protocols*, including the use of *complex passwords regex* and *regular updates* to reduce the risk of unauthorized access [110], [111]. Despite the baseline knowledge in this aspect, discernible gaps were observed in terms of employee attitudes and behaviors that potentially increased susceptibility to breaches. The mandatory adoption of the bmkg.go.id domain was supported by the integration of Google Mail services to serve as a preventive measure against phishing attempts. The process showed the need to reinforce secure email handling practices, particularly during office hours. Internet use also had some significant issues

because employees exhibited an adequate understanding but there was a need for behavioral improvement and organizational guidelines to address activities such as downloading from unreliable sources. Similarly, the use of social media was frequent but there were no policies and regulations regarding its usage during working hours. The prevalent use of mobile devices outside official premises required security measures, particularly the utilization of VPN.

The results further showed that BMKG employees generally possessed a *high level of awareness* across the three primary components, including *knowledge, attitude*, and *behavior* as presented in Table 5. There was a significant conceptual understanding of security policies, data handling procedures, and incident reporting mechanisms as observed in the knowledge scores exceeding 88%. However, this positive trend did not uniformly extend to practical application. This was observed from the fact that several areas, including attitude towards password management, social media and mobile usage, knowledge regarding email usage, behavior towards internet usage, mobile device usage, and computer device security had **moderate or medium** levels of awareness. A particular issue of concern was identified because the disparity in the use of internet and mobile technologies was high and proper knowledge was not matched by secure practices. For example, VPN usage was significantly low, and unsafe browsing behaviors such as access to suspicious websites persisted among a high proportion of employees.

The disparity between knowledge and implementation shows the critical need for more targeted and context-specific interventions. Bridging this gap requires a multi-pronged method that includes *regular awareness campaigns*, *practical training modules*, and *scenario-based learning* to reinforce secure practices in day-to-day activities, as shown effective in various case studies [36], [38], [82]. Moreover, the establishment of clearer organizational policies regarding the use of personal devices, online activity during work hours, and protocols for handling sensitive information can further promote consistent, *security-conscious* behavior. There is also the need to cultivate a robust and sustainable culture to ensure awareness is *not only theoretical* but integrated into the operational routines of all personnel.

B. Influential Factors (Addressing RQ2)

The results showed that BMKG employees generally had a strong knowledge of InfoSec by achieving an average awareness score of 88.06% based on the HAIS-Q model. This positive trend was associated with effective training and socialization programs conducted by the BMKG Database and Communication Network Centre. However, a significant gap was identified specifically in password security practices, device protection protocols, and adherence to InfoSec policies across BMKG units. These gaps showed the necessity for comprehensive InfoSec guidelines and consistent enforcement to reinforce the adoption of best practices and reduce security risks by employees [50], [51], [52], [53], [112].

Previous studies conducted using the HAIS-Q model in government and private sector organizations reported similar results. However, there was a significant difference in the rejection of hypotheses **H5 (Top Management → Attitude)** and **H6 (Top Management → Behavior)**. This study showed that top management commitment enhanced employee knowledge (H4: $\beta = 0.278$, $p < 0.05$) but did not have a statistically significant impact on attitude (H5: $\beta = 0.063$, $p = 0.063$) or behavior (H6: $\beta = 0.014$, $p = 0.332$).

The deviations compared to previous studies can be explained through several factors. First, the organizational culture of BMKG is probably different from those used in previous studies, particularly in relation to the communication and enforcement of cybersecurity policies by the top management. The lack of consistent engagement, monitoring, and enforcement mechanisms can also limit the direct influence of ISA endorsed by the top management on the day-to-day attitudes and actions of employees. Second, BMKG employees can rely more on peer influence and self-directed learning rather than managerial directives. The constant digital interactions and access to real-time meteorological and disaster-related data in the agency are capable of contributing to a heightened sense of individual responsibility in security practices. Employees working in such high-stakes environments can prioritize security measures independently which further reduces the reliance on management-driven initiatives. This contrasts with other sectors where employees handle less critical information and possibly require managerial reinforcement in adhering to security policies.

Top management is continuously important in achieving ISA within government agencies such as BMKG because authorization is necessary for the dissemination and approval of related knowledge. The role at BMKG includes being the primary gatekeeper or *the sentinel in a war* to facilitate or restrict the access of employees to specific ISA-related information. This shows the need for strategic initiatives to sustain InfoSec integrity through *robust policy documentation, oversight of implementation, and regular compliance monitoring*. The priorities are required to connect organizational objectives to InfoSec practices and maintain *vigilance* against possible security threats within the BMKG environment. The efforts to strengthen the measures can enhance InfoSec awareness and foster proactive engagement among employees in safeguarding organizational assets.

C. Implications

This study offers both practical and theoretical insights into improving ISA among government employees. Practical recommendations stress the importance of *enhanced training*, *better socialization*, and *rigorous InfoSec policy implementation*. These actions are critical for gaining leadership backing to shape employee attitudes and behaviors toward security regulations [81]. Moreover, the theoretical implications include the need to *refine assessment methods* particularly within the HAIS-Q framework to ensure a better connection to organizational needs. This can be achieved by focusing on relevant areas and statements within the domains identified [81]. Previous theories on the significant impact of InfoSec knowledge on individual behaviors are also supported. Furthermore, the results show how leadership support influences employee knowledge, attitudes, and behaviors which is slightly different from the trends identified in some earlier studies [64], [98].

The results showed the need for BMKG to *expand the role of top management* beyond merely disseminating policies to ensure that leaders actively exemplify and promote secure behaviors. Interactive training, unique communication strategies, and accountability measures could also be effectively used to bridge the gap between top-level support and employee conduct in addition to reinforcing peer-led security awareness initiatives. This was expected to be more effective in fostering consistent cybersecurity practices across the organization than conventional top-down methods.

D. Limitations

This study only focuses on assessing ISA among BMKG employees because the agency serves as a reasonable *proxy* for Indonesian government ministries or agencies due to the nationwide presence, vertical governance structure, and heavy reliance on ICT infrastructure. However, the organizational culture, security policies, and operational requirements are probably not entirely in line with those of *all* Indonesian government institutions.

The relevance and accuracy of the recommendations are ensured by primarily focusing on enhancing ISA within BMKG. The proposed measures are designed to strengthen cybersecurity policies, increase leadership engagement, and cultivate security-oriented organizational culture. Certain insights can be applicable to other government agencies with similar challenges, specifically those managing critical data and digital infrastructure. However, the application to a broader context across the Indonesian public sector requires further validation through multi-agency studies.

Future studies need to extend the scope by conducting comparative analyses across multiple government institutions. The method can facilitate a more comprehensive evaluation of ISA trends and the key factors influencing cybersecurity practices within the public sector of Indonesia.

VI. CONCLUSION

In conclusion, this study examined ISA among BMKG employees with a specific focus on knowledge, attitudes, and behaviors concerning cybersecurity. The results showed that BMKG employees had a high level of overall security awareness (88.06%) with substantial knowledge (88.06%) and positive attitudes (81.89%). However, behavioral adherence was comparatively lower (80.74%) particularly in email security (78.70%) and mobile device usage (73.19%) which showed a disparity between awareness and practical security compliance.

Knowledge ($\beta = 0.214$) and attitudes ($\beta = 0.289$) significantly influenced behavior ($\beta = 0.423$) and this showed that only awareness was insufficient without a corresponding commitment to secure practices. Top management support was observed not to have a significant influence on attitudes (H5) or behaviors (H6). This was different from the results reported in previous studies conducted on similar topics. Furthermore, peer influence, direct exposure to cyber threats, and practical training were found to be more instrumental in shaping security practices of employees. The nature of operations at BMKG required personnel to manage real-time weather, climate, and disaster-related data. This activity could motivate employee to develop a heightened sense of personal accountability and reduce the dependence on the direction provided by the leadership.

The enhancement of ISA measures for government employees required strategic initiatives centered on comprehensive InfoSec policies supported by strong top management commitment. These efforts were important for shaping employee attitudes and behaviors towards ISA in order to strengthen security measures across all government bodies. Future studies should explore the technical aspects by evaluating technology infrastructure, assessing the sophistication of security systems, and incorporating ISO 27001:2022 standards to comprehensively broaden awareness efforts. The efforts to address these gaps and draw insights from ongoing studies could assist the Indonesian government in progressing towards a more resilient InfoSec framework needed to safeguard digital assets and bolster organizational security in governmental contexts.

Author Contributions: *Aji Prasetyo*: Conceptualisation, Methodology, Data Curation, Writing -Original Draft. *Wahyu Setiawan Wibowo*: Conceptualisation, Writing -Review & Editing, Supervision. *Rizal Fathoni Aji*: Writing - Review & Editing, Supervision.

All authors have read and agreed to the published version of the manuscript.

Funding: This research did not receive any dedicated funding from external agencies or grant sources.

Acknowledgments: The authors deeply thank BMKG for their invaluable guidance, support, and collaboration. The BMKG team's dedication, time, and expertise significantly enhanced this study. Their cooperation in granting permits and providing crucial data was vital to achieving the research objectives. BMKG's generosity and commitment fostered a meaningful partnership between academia and the public sector, enhancing the academic rigour of this research and exemplifying their dedication to advancing knowledge and promoting collaborative research.

Conflicts of Interest: The authors hereby declare that there are no conflicts of interest regarding the publication of this research paper.

Data Availability: The authors have meticulously ensured the clarity and accessibility of the data supporting this paper's findings. However, to address confidentiality concerns and safeguard participant privacy, certain data sections remain restricted. The authors commit to providing access to the non-confidential data upon reasonable request, adhering to ethical and legal considerations.

Informed Consent: Informed Consent was obtained.

Institutional Review Board Statement: Not applicable.

Animal Subjects: There were no animal subjects.

ORCID:
Aji Prasetyo: https://orcid.org/0000-0002-3190-9458
Rizal Fathoni Aji: -
Wahyu Setiawan Wibowo: https://orcid.org/0000-0002-1327-0072

REFERENCES

[1] M. Mansoor, "An interaction effect of perceived government response on COVID-19 and government agency's use of ICT in building trust among citizens of Pakistan," *Transforming Government: People, Process and Policy*, vol. 15, no. 4, pp. 693–707, Nov. 2021, doi: 10.1108/TG-01-2021-0002.

[2] Y.-P. Yuan *et al.*, "Government Digital Transformation: Understanding the Role of Government Social Media," *Gov Inf Q*, vol. 40, no. 1, p. 101775, Jan. 2023, doi: 10.1016/j.giq.2022.101775.

[3] A. Mishra, Y. I. Alzoubi, A. Q. Gill, and M. J. Anwar, "Cybersecurity Enterprises Policies: A Comparative Study," *Sensors*, vol. 22, no. 2, pp. 1–36, 2022, doi: 10.3390/s22020538.

[4] T. M. Washington, "Stakeholder Perceptions of the Organization's Information Security Policy: A Q Methodology Study to Support Evidence-Based Policymaking in the Federal Government," University of Fairfax PP - United States -- Virginia, US, United States -- Virginia, US, 2023.

[5] A. Mishra, Y. I. Alzoubi, M. J. Anwar, and A. Q. Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations," *Comput Secur*, vol. 120, p. 102820, Sep. 2022, doi: 10.1016/j.cose.2022.102820.

[6] A. Uyar, K. Nimer, C. Kuzey, M. Shahbaz, and F. Schneider, "Can e-government initiatives alleviate tax evasion? The moderation effect of ICT," *Technol Forecast Soc Change*, vol. 166, p. 120597, May 2021, doi: 10.1016/j.techfore.2021.120597.

[7] A. M. Samsor, "Challenges and Prospects of e-Government implementation in Afghanistan," *International Trade, Politics and Development*, vol. 5, no. 1, pp. 51–70, May 2021, doi: 10.1108/ITPD-01-2020-0001.

[8] A. Visvizi and M. D. Lytras, "Government at risk: between distributed risks and threats and effective policy-responses," *Transforming Government: People, Process and Policy*, vol. 14, no. 3, pp. 333–336, Jul. 2020, doi: 10.1108/TG-06-2020-0137.

[9] R. M. Alguliyev, Y. N. Imamverdiyev, R. Sh. Mahmudov, and R. M. Aliguliyev, "Information security as a national security component," *Information Security Journal: A Global Perspective*, vol. 30, no. 1, pp. 1–18, Jan. 2021, doi: 10.1080/19393555.2020.1795323.

[10] S. Mishra, M. A. Alowaidi, and S. K. Sharma, "Impact of security standards and policies on the credibility of e-government," *J Ambient Intell Humaniz Comput*, 2021, doi: 10.1007/s12652-020-02767-5.

[11] Statista Market Forecast, "Cybersecurity - Worldwide." Accessed: Feb. 05, 2024. [Online]. Available: https://www.statista.com/outlook/tmo/cybersecurity/worldwide#revenue

[12] Statista Market Forecast, "Estimated cost of cybercrime worldwide 2017-2028." Accessed: Mar. 05, 2024. [Online]. Available: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide
[13] International Monetary Fund, "Cyber threats to the financial system are growing, and the global community must cooperate to protect it." Accessed: Mar. 05, 2024. [Online]. Available: https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm
[14] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: Systematic review," *Comput Secur*, vol. 99, p. 102030, Dec. 2020, doi: 10.1016/j.cose.2020.102030.
[15] R. Yuliana and Z. Arifin Hasibuan, "Best practice framework for information technology security governance in Indonesian government," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 6, p. 6522, Dec. 2022, doi: 10.11591/ijece.v12i6.pp6522-6534.
[16] A. Kő, G. Tarján, and A. Mitev, "Information security awareness maturity: conceptual and practical aspects in Hungarian organizations," *Information Technology & People*, vol. 36, no. 8, pp. 174–195, Dec. 2023, doi: 10.1108/ITP-11-2021-0849.
[17] D. F. Norris, L. Mateczun, A. Joshi, and T. Finin, "Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity," *J Urban Aff*, vol. 43, no. 8, pp. 1173–1195, Sep. 2021, doi: 10.1080/07352166.2020.1727295.
[18] S. T. Hossain, T. Yigitcanlar, K. Nguyen, and Y. Xu, "Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework," *Applied Sciences*, vol. 14, no. 13, p. 5501, Jun. 2024, doi: 10.3390/app14135501.
[19] S. T. R. and S. K. T., "A Review on Major Cyber Threats and Recommended Counter Measures," *Int J Res Appl Sci Eng Technol*, vol. 11, no. 3, pp. 1758–1761, Mar. 2023, doi: 10.22214/ijraset.2023.49764.
[20] W. Hatcher, W. L. Meares, and J. Heslen, "The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices," *Journal of Cyber Policy*, vol. 5, no. 2, pp. 302–325, May 2020, doi: 10.1080/23738871.2020.1792956.
[21] T. Baker and A. Shortland, "The government behind insurance governance: Lessons for ransomware," *Regul Gov*, vol. 17, no. 4, pp. 1000–1020, Oct. 2023, doi: 10.1111/rego.12505.
[22] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K.-K. R. Choo, and P. Burnap, "Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses," *Electronics (Basel)*, vol. 9, no. 9, p. 1460, Sep. 2020, doi: 10.3390/electronics9091460.
[23] A. Frandell and M. Feeney, "Cybersecurity Threats in Local Government: A Sociotechnical Perspective," *The American Review of Public Administration*, vol. 52, no. 8, pp. 558–572, Nov. 2022, doi: 10.1177/02750740221125432.
[24] A. Hussain, A. Mohamed, and S. Razali, "A Review on Cybersecurity," in *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*, New York, NY, USA: ACM, Mar. 2020, pp. 1–7. doi: 10.1145/3386723.3387847.
[25] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: Systematic review," *Comput Secur*, vol. 99, p. 102030, Dec. 2020, doi: 10.1016/j.cose.2020.102030.
[26] R. Shandler and M. A. Gomez, "The hidden threat of cyber-attacks – undermining public confidence in government," *Journal of Information Technology & Politics*, vol. 20, no. 4, pp. 359–374, Oct. 2023, doi: 10.1080/19331681.2022.2112796.
[27] S. Iftikhar, "Cyberterrorism as a global threat: a review on repercussions and countermeasures," *PeerJ Comput Sci*, vol. 10, p. e1772, Jan. 2024, doi: 10.7717/peerj-cs.1772.
[28] S. Kaur, S. Sharma, and A. Singh, "Cyber Security: Attacks, Implications and Legitimations across the Globe," *Int J Comput Appl*, vol. 114, no. 6, pp. 21–23, Mar. 2015, doi: 10.5120/19983-1932.
[29] H. Jahankhani, L. N. K. Meda, and M. Samadi, "Cybersecurity Challenges in Small and Medium Enterprise (SMEs)," 2022, pp. 1–19. doi: 10.1007/978-3-030-98225-6_1.
[30] S. Oni, K. Araife Berepubo, A. A. Oni, and S. Joshua, "E-Government and the Challenge of Cybercrime in Nigeria," in *2019 Sixth International Conference on eDemocracy & eGovernment (ICEDEG)*, IEEE, Apr. 2019, pp. 137–142. doi: 10.1109/ICEDEG.2019.8734329.
[31] H. Harvey *et al.*, "The Impact of a National Cyberattack Affecting Clinical Trials: The Cancer Trials Ireland Experience," *JCO Clin Cancer Inform*, no. 7, Apr. 2023, doi: 10.1200/CCI.22.00149.
[32] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Comput Secur*, vol. 106, p. 102267, Jul. 2021, doi: 10.1016/j.cose.2021.102267.
[33] A. R. Ahlan, M. Lubis, and A. R. Lubis, "Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures," *Procedia Comput Sci*, vol. 72, pp. 361–373, 2015, doi: 10.1016/j.procs.2015.12.151.
[34] T. Grassegger and D. Nedbal, "The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering," *Procedia Comput Sci*, vol. 181, pp. 59–66, 2021, doi: 10.1016/j.procs.2021.01.103.
[35] L. Y. C. Chang and N. Coppel, "Building cyber security awareness in a developing country: Lessons from Myanmar," *Comput Secur*, vol. 97, p. 101959, Oct. 2020, doi: 10.1016/j.cose.2020.101959.
[36] A. Alzubaidi, "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia," *Heliyon*, vol. 7, no. 1, p. e06016, Jan. 2021, doi: 10.1016/j.heliyon.2021.e06016.
[37] M. Hassan, K. Saeedi, H. Almagwashi, and S. Alarifi, "Information Security Risk Awareness Survey of Non-governmental Organization in Saudi Arabia," 2023, pp. 39–71. doi: 10.1007/978-3-031-19560-0_4.
[38] R. AlMindeel and J. T. Martins, "Information security awareness in a developing country context: insights from the government sector in Saudi Arabia," *Information Technology & People*, vol. 34, no. 2, pp. 770–788, May 2020, doi: 10.1108/ITP-06-2019-0269.
[39] Bulgurcu, Cavusoglu, and Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly*, vol. 34, no. 3, p. 523, 2010, doi: 10.2307/25750690.
[40] H. A. R. Amjad, U. Naeem, M. A. Zaffar, M. F. Zaffar, and K.-K. R. Choo, "Improving Security Awareness in the Government Sector," in *Proceedings of the 17th International Digital Government Research Conference on Digital Government Research*, New York, NY, USA: ACM, Jun. 2016, pp. 1–7. doi: 10.1145/2912160.2912186.
[41] J. Kävrestad, F. Burvall, and M. Nohlberg, "A taxonomy of factors that contribute to organizational Cybersecurity Awareness (CSA)," *Information & Computer Security*, Jun. 2024, doi: 10.1108/ICS-11-2023-0209.
[42] N. A. Hassan, "Security Awareness Training: Best Practices for Implementing a Security Awareness Training Program," in *Ransomware Revealed*, Berkeley, CA: Apress, 2019, pp. 155–173. doi: 10.1007/978-1-4842-4255-1_6.
[43] W. Stallings, *Cryptography and Network Security: Principles and Practice, Global Edition*, 8th ed. Harlow: Pearson Education, 2023.
[44] M. Alsharif, S. Mishra, and M. AlShehri, "Impact of Human Vulnerabilities on Cybersecurity," *Computer Systems Science and Engineering*, vol. 40, no. 3, pp. 1153–1166, 2021, doi: 10.32604/CSSE.2022.019938.

[45] A. Mishra, Y. I. Alzoubi, A. Q. Gill, and M. J. Anwar, "Cybersecurity Enterprises Policies: A Comparative Study," *Sensors*, vol. 22, no. 2, pp. 1–36, 2022, doi: 10.3390/s22020538.
[46] E. Yildirim, "The Importance of Information Security Awareness for the Success of Business Enterprises," 2016, pp. 211–222. doi: 10.1007/978-3-319-41932-9_17.
[47] S. R. Muller and M. L. Lind, "Factors in Information Assurance Professionals' Intentions to Adhere to Information Security Policies," *International Journal of Systems and Software Security and Protection*, vol. 11, no. 1, pp. 17–32, Jan. 2020, doi: 10.4018/IJSSSP.2020010102.
[48] K. Arbanas, M. Spremic, and N. Zajdela Hrustek, "Holistic framework for evaluating and improving information security culture," *Aslib Journal of Information Management*, vol. 73, no. 5, pp. 699–719, Sep. 2021, doi: 10.1108/AJIM-02-2021-0037.
[49] Direktorat Operasi Keamanan Siber BSSN, "Laporan Tahunan Monitoring Keamanan Siber Tahun 2021," Jakarta, 2022.
[50] G. Papp and P. Lovaas, "Assessing Small Institutions' Cyber Security Awareness Using Human Aspects of Information Security Questionnaire (HAIS-Q)," 2021, pp. 933–948. doi: 10.1007/978-3-030-80129-8_62.
[51] A. Zulfia, R. Adawiyah, A. N. Hidayanto, and N. F. A. Budi, "Measurement of Employee Information Security Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q): Case Study at PT. PQS," in *2019 5th International Conference on Computing Engineering and Design (ICCED)*, 2019, pp. 1–5. doi: 10.1109/ICCED46541.2019.9161120.
[52] D. S. Hermawan, F. Setiadi, and D. Oktaria, "Measurement Level of Information Security Awareness for Employees Using KAB Model with Study Case at XYZ Agency," in *2022 1st International Conference on Software Engineering and Information Technology (ICoSEIT)*, 2022, pp. 174–179. doi: 10.1109/ICoSEIT55604.2022.10029989.
[53] M. S. Mahardika, A. N. Hidayanto, P. A. Paramartha, L. D. Ompusunggu, R. Mahdalina, and F. Affan, "Measurement of employee awareness levels for information security at the center of analysis and information services judicial commission Republic of Indonesia," *Advances in Science, Technology and Engineering Systems*, vol. 5, no. 3, pp. 501–509, 2020, doi: 10.25046/aj050362.
[54] E. A. Puspitaningrum, F. T. Devani, V. Q. Putri, A. N. Hidayanto, Solikin, and I. C. Hapsari, "Measurement of Employee Information Security Awareness: Case Study at A Government Institution," in *2018 Third International Conference on Informatics and Computing (ICIC)*, IEEE, Oct. 2018, pp. 1–6. doi: 10.1109/IAC.2018.8780571.
[55] S. TALIB, R. ABDUL MUNIR, N. N. ABDUL MOLOK, and M. R. AHMAD, "INFORMATION SECURITY GOVERNANCE ISSUES IN MALAYSIAN GOVERNMENT SECTOR," *Journal of Information Systems and Digital Technologies*, vol. 5, no. 2, pp. 1–18, Nov. 2023, doi: 10.31436/jisdt.v5i2.404.
[56] S. Tenzin, T. McGill, and M. Dixon, "An Investigation of the Factors That Influence Information Security Culture in Government Organizations in Bhutan," *Journal of Global Information Technology Management*, vol. 27, no. 1, pp. 37–62, Jan. 2024, doi: 10.1080/1097198X.2023.2297634.
[57] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and Information Security Awareness," *Comput Human Behav*, vol. 69, pp. 151–156, Apr. 2017, doi: 10.1016/j.chb.2016.11.065.
[58] M. Pattinson *et al.*, "Matching training to individual learning styles improves information security awareness," *Information & Computer Security*, vol. 28, no. 1, pp. 1–14, Nov. 2019, doi: 10.1108/ICS-01-2019-0022.
[59] J. Zhen, K. Dong, Z. Xie, and L. Chen, "Factors Influencing Employees' Information Security Awareness in the Telework Environment," *Electronics (Switzerland)*, vol. 11, no. 21, 2022, doi: 10.3390/electronics11213458.
[60] S. Bauer, E. W. N. Bernroider, and K. Chudzikowski, "Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks," *Comput Secur*, vol. 68, pp. 145–159, Jul. 2017, doi: 10.1016/j.cose.2017.04.009.
[61] A. Koohang, J. Anderson, J. H. Nord, and J. Paliszkiewicz, "Building an awareness-centered information security policy compliance model," *Industrial Management & Data Systems*, vol. 120, no. 1, pp. 231–247, Dec. 2019, doi: 10.1108/IMDS-07-2019-0412.
[62] W. Rocha Flores and M. Ekstedt, "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness," *Comput Secur*, vol. 59, pp. 26–44, Jun. 2016, doi: 10.1016/j.cose.2016.01.004.
[63] ISACA, *ISSE 2009 Securing Electronic Business Processes*. Wiesbaden: Vieweg+Teubner, 2010. doi: 10.1007/978-3-8348-9363-5.
[64] P. K. Sari *et al.*, "Information security cultural differences among health care facilities in Indonesia," *Heliyon*, vol. 7, no. 6, 2021, doi: 10.1016/j.heliyon.2021.e07248.
[65] E. Yildirim, "The Importance of Information Security Awareness for the Success of Business Enterprises," 2016, pp. 211–222. doi: 10.1007/978-3-319-41932-9_17.
[66] P. A. W. Putro, D. I. Sensuse, and W. S. S. Wibowo, "Framework for critical information infrastructure protection in smart government: a case study in Indonesia," *Information & Computer Security*, vol. 32, no. 1, pp. 112–129, Jan. 2024, doi: 10.1108/ICS-03-2023-0031.
[67] R. Von Solms, K.-L. Thomson, and P. M. Maninjwa, "Information Security Governance control through comprehensive policy architectures," in *2011 Information Security for South Africa*, IEEE, Aug. 2011, pp. 1–6. doi: 10.1109/ISSA.2011.6027522.
[68] S. Schinagl and A. Shahim, "What do we know about information security governance?," *Information & Computer Security*, vol. 28, no. 2, pp. 261–292, Jan. 2020, doi: 10.1108/ICS-02-2019-0033.
[69] A. McIlwraith, *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training, and Awareness*, 2nd ed. New York, NY, USA: Routledge, 2022.
[70] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Comput Secur*, vol. 66, pp. 40–51, May 2017, doi: 10.1016/j.cose.2017.01.004.
[71] M. Pattinson *et al.*, "Matching training to individual learning styles improves information security awareness," *Information & Computer Security*, vol. 28, no. 1, pp. 1–14, Nov. 2019, doi: 10.1108/ICS-01-2019-0022.
[72] J. Zhen, K. Dong, Z. Xie, and L. Chen, "Factors Influencing Employees' Information Security Awareness in the Telework Environment," *Electronics (Switzerland)*, vol. 11, no. 21, 2022, doi: 10.3390/electronics11213458.
[73] B. Alkhazi, M. Alshaikh, S. Alkhezi, and H. Labbaci, "Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior," *IEEE Access*, vol. 10, pp. 132132–132143, 2022, doi: 10.1109/ACCESS.2022.3230286.
[74] M. Tvaronavičienė, T. Plėta, S. Della Casa, and J. Latvys, "Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania," *Insights into Regional Development*, vol. 2, no. 4, pp. 802–813, Dec. 2020, doi: 10.9770/IRD.2020.2.4(6).
[75] E. Lee, Y.-D. Seo, S.-R. Oh, and Y.-G. Kim, "A Survey on Standards for Interoperability and Security in the Internet of Things," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1020–1047, 2021, doi: 10.1109/COMST.2021.3067354.
[76] W. Stallings, *Cryptography and Network Security: Principles and Practice, Global Edition*, 8th ed. Harlow: Pearson Education, 2023.

[77] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput Secur*, vol. 25, no. 4, pp. 289–296, 2006, doi: 10.1016/j.cose.2006.02.008.
[78] Rosihan and A. N. Hidayanto, "Measurement of Employee Information Security Awareness: A Case Study at an Indonesian Correctional Institution," in *2022 1st International Conference on Information System & Information Technology (ICISIT)*, IEEE, Jul. 2022, pp. 318–323. doi: 10.1109/ICISIT54091.2022.9872988.
[79] H. Chen and Y. Hai, "Exploring the critical success factors of information security management: a mixed-method approach," *Information & Computer Security*, Jan. 2024, doi: 10.1108/ICS-03-2023-0034.
[80] Y. Normandia, L. Kumaralalita, A. N. Hidayanto, W. S. Nugroho, and M. R. Shihab, "Measurement of Employee Information Security Awareness Using Analytic Hierarchy Process (AHP): A Case Study of Foreign Affairs Ministry," in *2018 International Conference on Computing, Engineering, and Design (ICCED)*, IEEE, Sep. 2018, pp. 52–56. doi: 10.1109/ICCED.2018.00020.
[81] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput Secur*, vol. 42, pp. 165–176, May 2014, doi: 10.1016/j.cose.2013.12.003.
[82] N. S. Sulaiman, M. A. Fauzi, S. Hussain, and W. Wider, "Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks," *Information*, vol. 13, no. 9, p. 413, Aug. 2022, doi: 10.3390/info13090413.
[83] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and Information Security Awareness," *Comput Human Behav*, vol. 69, pp. 151–156, Apr. 2017, doi: 10.1016/j.chb.2016.11.065.
[84] A. Lopes, L. Reis, H. São Mamede, and A. Santos, "Information Security Threat Assessment Using Social Engineering in the Organizational Context – Literature Review," *Lecture Notes in Networks and Systems*, vol. 469 LNNS, pp. 233–242, 2022, doi: 10.1007/978-3-031-04819-7_24.
[85] L. B. Bhagwat and B. M. Patil, "Detection of Ransomware Attack: A Review," 2020, pp. 15–22. doi: 10.1007/978-981-15-0790-8_2.
[86] H. A. Acosta-Maestre, "The Empirical Study of the Factors that Influence Threat Avoidance Behavior in Ransomware Security Incidents," Nova Southeastern University PP - United States -- Florida, United States -- Florida, 2021.
[87] C. Lamers, E. Spoerl, G. Levey, N. Choudhury, and M. Ahmed, "Ransomware: A Threat to Cyber Smart Cities," 2023, pp. 185–204. doi: 10.1007/978-3-031-24946-4_13.
[88] Direktorat Operasi Keamanan Siber BSSN, "Laporan Tahunan Monitoring Keamanan Siber Tahun 2021," Jakarta, 2022.
[89] J. W. Han, O. J. Hoe, J. S. Wing, and S. N. Brohi, "A Conceptual Security Approach with Awareness Strategy and Implementation Policy to Eliminate Ransomware," in *Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence*, in CSAI 2017. New York, NY, USA: Association for Computing Machinery, 2017, pp. 222–226. doi: 10.1145/3168390.3168398.
[90] M. Muslih, "Towards a Better Organizational Structure," *Journal of Business and Economics*, vol. 12, no. 4, pp. 446–454, Apr. 2021, doi: 10.15341/jbe(2155-7950)/04.12.2021/010.
[91] G. K. Singh, P. S. Ughara, M. M. Ishaq, A. P. Singh, and K. Chauhan, "Meteorological Progress: A Comprehensive Review of Weather Prediction," in *2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, IEEE, Dec. 2023, pp. 485–490. doi: 10.1109/ICIMIA60377.2023.10425965.
[92] I. Gultepe, "A Review on Weather Impact on Aviation Operations: Visibility, Wind, Precipitation, Icing," *Journal of Airline Operations and Aviation Management*, vol. 2, no. 1, pp. 1–44, Aug. 2023, doi: 10.56801/jaoam.v2i1.1.
[93] A.-M. LUCHIAN, "THE IMPACT OF WEATHER ON FLIGHT PERFORMANCE AND AVIATION COMMUNICATION," *SCIENTIFIC RESEARCH AND EDUCATION IN THE AIR FORCE*, vol. 25, pp. 179–184, Jul. 2024, doi: 10.19062/2247-3173.2024.25.20.
[94] S. Matzkin, R. Shandler, and D. Canetti, "The limits of cyberattacks in eroding political trust: A tripartite survey experiment," *The British Journal of Politics and International Relations*, vol. 26, no. 4, pp. 1033–1054, Nov. 2024, doi: 10.1177/13691481231210383.
[95] M. G. Ikhsan and K. Ramli, "Measuring the Information Security Awareness Level of Government Employees Through Phishing Assessment," in *2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC)*, IEEE, Jun. 2019, pp. 1–4. doi: 10.1109/ITC-CSCC.2019.8793292.
[96] J. Recker, *Scientific Research in Information Systems*. in Progress in IS. Cham: Springer International Publishing, 2021. doi: 10.1007/978-3-030-85436-2.
[97] J. W. Cresswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, Fourth. Sage Publications, Inc, 2014.
[98] M. A. Alnatheer, "Information Security Culture Critical Success Factors," in *2015 12th International Conference on Information Technology - New Generations*, IEEE, Apr. 2015, pp. 731–735. doi: 10.1109/ITNG.2015.124.
[99] A. Prasetyo, D. Irawan, D. I. Sensuse, S. Lusa, P. A. Wibowo, and A. Yulfitri, "Evaluation of e-Service Quality Impacts Customer Satisfaction: One-Gate Integrated Service Application in Indonesian Weather Agency," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 1, pp. 145–152, 2023, doi: 10.14569/IJACSA.2023.0140116.
[100] A. McCormac, D. Calic, M. Butavicius, K. Parsons, T. Zwaans, and M. Pattinson, "A Reliable Measure of Information Security Awareness and the Identification of Bias in Responses," *Australasian Journal of Information Systems*, vol. 21, Nov. 2017, doi: 10.3127/ajis.v21i0.1697.
[101] M. Pattinson, M. Butavicius, K. Parsons, A. McCormac, and D. Calic, "Managing information security awareness at an Australian bank: a comparative study," *Information & Computer Security*, vol. 25, no. 2, pp. 181–189, Jun. 2017, doi: 10.1108/ICS-03-2017-0017.
[102] J. F. Hair Jr, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. SAGE Publications, 2021.
[103] J. J. Tejada, J. Raymond, and B. Punzalan, "On the Misuse of Slovin's Formula," *The Philippine Statistician*, vol. 61, no. 1, p. 8, 2012.
[104] J. F. Hair, G. T. Hult, C. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. 2017.
[105] J. F. Hair, J. J. Risher, M. Sarstedt, and C. M. Ringle, "When to use and how to report the results of PLS-SEM," *European Business Review*, vol. 31, no. 1, pp. 2–24, Jan. 2019, doi: 10.1108/EBR-11-2018-0203.
[106] J. F. Hair, G. T. M. Hult, C. M. Ringle, M. Sarstedt, N. P. Danks, and S. Ray, *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R*. in Classroom Companion: Business. Cham: Springer International Publishing, 2021. doi: 10.1007/978-3-030-80519-7.
[107] W. S. Wibowo, A. Fadhil, D. I. Sensuse, S. Lusa, P. A. W. Putro, and A. Yulfitri, "Pinpointing Factors in the Success of Integrated Information System Toward Open Government Data Initiative: A Perspective from Employees," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 1, pp. 94–109, 2023, doi: 10.14569/IJACSA.2023.0140111.
[108] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *J Acad Mark Sci*, vol. 43, no. 1, pp. 115–135, 2015, doi: 10.1007/s11747-014-0403-8.

[109] M. Sarstedt, J. F. Hair, J.-H. Cheah, J.-M. Becker, and C. M. Ringle, "How to Specify, Estimate, and Validate Higher-Order Constructs in PLS-SEM," *Australasian Marketing Journal*, vol. 27, no. 3, pp. 197–211, Aug. 2019, doi: 10.1016/j.ausmj.2019.05.003.
[110] A. Rechavi, T. Berenblum, and D. Maimon, "The secondary global market for hacked data," *International Journal of Cyber Criminology*, vol. 12, no. 2, pp. 408–426, 2018, doi: 10.5281/zenodo.3366118.
[111] D. Shoemaker, A. Kohnke, and K. Sigler, "The Cybersecurity Body of Knowledge," *The Cybersecurity Body of Knowledge*, pp. 39–85, 2020, doi: 10.1201/9781003022596-2.
[112] K. J. Knapp, R. Franklin Morris, T. E. Marshall, and T. A. Byrd, "Information security policy: An organizational-level process model," *Comput Secur*, vol. 28, no. 7, pp. 493–508, Oct. 2009, doi: 10.1016/j.cose.2009.07.001.