proceedings

MDPI

Proceeding Paper

The Moderating Role of Information Security Behaviour (ISB) on the Relationship between Digital Literacy (DL) and Information Security Culture (ISC): A Proposed Research Framework †

Mohd Sharulnizam Kamarulzaman [1], Shamila Mohamed Shuhidan [2,*] and Khalid Abdul Wahid [3]

[1] Cybersecurity Malaysia, Level 4, Tower 1, Menara Cyber Axis, Jalan Impact, Cyberjaya 63000, Malaysia
[2] Faculty of Information Management, Universiti Teknologi Mara Selangor Branch, Shah Alam 40150, Malaysia
[3] Faculty of Information Management, Universiti Teknologi Mara Kelantan Branch, Machang 18500, Malaysia
* Correspondence: shamila@uitm.edu.my; Tel.: +60-136-922-881

† Presented at the International Academic Symposium of Social Science 2022, Kota Bharu, Malaysia, 3 July 2022.

Abstract: Information Security Culture (ISC) has been suggested as a means of strengthening employees' information security in the workplace. However, the role of employees and their digital skills in the process has been largely overlooked. Establishing an information security culture that strives to secure information by having employees who are digitally literate, as well as exerting influence on the employees' behaviour regarding security, is one of the measures that may be utilised to mitigate risks provided by humans. Therefore, the purpose of this paper is to establish a research framework that moderates the effect of information security behaviour (ISB) on the relationship between digital literacy (DL) and information security culture (ISC). The study will improve DL and ISCB among employees who implement the country's development plans, such as enhancing administrative functions, social infrastructure, and economic growth performance in accordance with MyDigital initiatives, as well as the government's ISC.

Keywords: information security culture; information security behaviour; digital literacy

check for updates

Citation: Kamarulzaman, M.S.; Shuhidan, S.M.; Wahid, K.A. The Moderating Role of Information Security Behaviour (ISB) on the Relationship between Digital Literacy (DL) and Information Security Culture (ISC): A Proposed Research Framework. *Proceedings* **2022**, *82*, 35. https://doi.org/10.3390/proceedings2022082035

Academic Editor: Mohamad Rahimi Mohamad Rosman

Published: 13 September 2022

1. Introduction

Information security is vital nowadays. Our professional and personal lives depend on information. Many organizations could not exist without their information assets; thus, protecting them is a key responsibility, according to Alhogail [1], citing Van Niekerk and Von Solms [2]. Previous studies show that employee irresponsibility causes most data breaches [3,4]. 30% of security concerns were triggered by employees, 27% by former employees, and 23% by unknown hackers, according to PriceWaterhouseCoopers' 2018 study [5]. A security breach may compromise sensitive data from an organization, which thus this illustrates the necessity to build a culture of information security among Malaysian organizations. Information security culture is "the combination of views, beliefs, attitudes, assumptions, knowledge and skills that regulate human involvement with information assets within an organization" [6]. Masrek et al. [7] defined ISC as personnel having the essential awareness, abilities, and understanding of information security processes and procedures. Excellent ISCs offer employees the appropriate training, expertise, and awareness. For an effective ISC, examining each employee's DL skill and knowledge and understanding their security behaviour is key to a healthy information security culture. Humans' everyday contacts with technology impact everything they do, at work and at home. This is in line with the aspiration of the Malaysia Digital Economy Blueprint, MyDIGITAL, to improve the digital literacy of employees, as required for Thrust 1: to drive digital transformation in the public sector with the goal of educating all levels of government employees on digital literacy; and Thrust 6: to build trusted, secure, ethical digital environments with the goal of raising cyber security awareness [8].

2. Literature Review

An internet connection is vital for Malaysian organizations, services, and people involved in Industry 4.0 and My Digital. Businesses rely extensively on democratised technology, including social, mobile, IoT, Big Data, cloud computing, and AI, all reliant on connectivity [9]. Employees must be digitally competent as digital technology evolves, and everything connected to the Internet faces information security concerns. Information security is now becoming everyday routine. Every aspect of our lives uses information. Many businesses are unable to function without the use of information, and therefore must take great care to protect their information assets [2]. Every company needs an information security solution as a counter measure [10]. By fostering a security-conscious culture, information assets are safer [11]. Despite this risk, employees may help to reduce information asset risk by adherence to security rules and procedures that can improve information security [12]. The strongest link in an organization's architecture is a well-trained employee with adequate digital literacy abilities [13]. Employees should be digitally literate in order to comply with information security rules and legislation [12]. This facilitates the incorporation of information security into the organization's culture. Organizational culture should affect employees' security behaviours [13]. Information security academics and specialists increasingly emphasise these organizational human capital as a component of mitigating security risks and threats [14–16]. Despite modern technical security safeguards, employees (often unknowingly) contribute to security breaches by risky behaviour due to a poor information security culture [16,17]. An organization's information system security depends on their employees' online behaviour. The human factor is one of the most neglected components of information security in organizations [10]. Proper employee behaviour may greatly improve an organization's information security system and culture [11].

3. Problem Statement

A decade ago, the idea of enabling people to work remotely every day seemed inconceivable. Employers worried about productivity and security when employees worked remotely or from home, particularly with the current epidemic. When employees work remotely, organizations are more vulnerable to cyberattacks. Employees may potentially be a weakness in an organization's IT security systems, enabling cybercriminals to get access to business data, customer data, and intellectual property. In this instance, employees' digital literacy is vital, particularly security expertise, which impacts how they handle valuable data and information. Organizations must cultivate a culture of information security in order to guarantee that their employees engage in secure information handling practices. As the economy becomes more digital, most firms struggle to tackle the cyber threat. Employees' personal information, corporate data, consumer data, intellectual property, and critical infrastructure are all at risk. COVID-19's long-term impact on organization digitization is unknown, although it has boosted the process. Moreover, many employees now work remotely, which raises the risk of cyberattacks [18]. These research problems are listed below.

3.1. Vulnerability of Employee Behaviour

According to the results of the 2017/18 research by the Institute of Information Security Professionals (IISP), over 80% of security professionals cited "people" as the industry's greatest concern, as opposed to "technology and processes." Performgreen UK 2019 [19], an information security provider, argues that changing employee behaviour is the most effective way to enhance an organization's information security. Whether planned or inadvertent, insiders may be responsible for most data breaches, says a study by Verizon, 2009 [20]. Similar studies have shown that insiders represent a threat to information security [21–23] and that organizations must decrease the risk employees offer. While research emphasizes the necessity of managing employee behaviour to secure information assets [24–27] the most effective countermeasure is to include a mix of controls, not only technological ones.

3.2. Remote Working and Safety Issue

Remote working is not new, but security was not always a concern. A 2006 research study discovered significant user awareness and security gaps, leaving them unprepared for remote working [22]. Home in this research is a location where employees dwell permanently or temporarily outside of work hours. Remote employment is not the norm for a large portion of the workforce, even if it is secure. The sudden change to remote work likely took many employees by surprise. In many cases, employees are given the tools (e.g., computers and other devices) for remote work but not the training. Some of these people may have been requested to work remotely using just their IT talents [28]. Considering the attitude and psychology of remote working, it can be understood how this may be dangerous. In a more comfortable and familiar atmosphere, employees may be less obliged by workplace regulations. The question is whether organizations that have established excellent practices in an office environment can do so remotely with their employees. Digital natives and digital immigrants must be able to adopt information security best practices while working remotely in order to prevent security issues.

3.3. Insufficient Digital Literacy Skill

Information technology advancements have led to widespread Internet usage [29]. However, internet hackers may take advantage of people's ignorance or lack of knowledge. Increasing digital literacy and security knowledge among the public and employees is vital for minimizing "hacker" damage. Inclusion of digital literacy, particularly security, in today's educational institutions may have a significant influence [30,31]. Digital skills have become "important" and must be complemented with "soft skills" such as the ability to interact successfully online and offline. Large-scale digital innovations such as artificial intelligence, machine learning, and big data analytics requie the creation of new skill sets, and this in turn affects the capacity building and skill development of the digital economy. Information security and privacy measures are generally seen to be vulnerable to the actions of individuals, who are seen as the "weakest link" [12,32]. If employees do not defend their privacy, security, or copyright rights or those of others, the organization's information asset is at risk due to individual users that lack skills, knowledge, and proper behaviour, according to research [33]. To guarantee that employees are working in a safe online environment, this study examines the requirement for digital literacy and the cultivation of acceptable information security behaviour as a discipline within information security culture. In the case of pandemics, this is especially important when employees are working remotely or in circumstances where they are responsible for their own safety.

3.4. Digital Literacy Skill Knowledge Gap and Scarcity of DL Studies on Employees in the Government Sector, Security Aspects, Information Security Behaviour and Information Security Culture

To effectively identify the relationships under discussion here, there must first be enough research to address the issue. In the local context, many stakeholders, including academics, have already given much attention to digital literacy, especially in recent times, but much of the focus has been on the education sector. According to Ahsan 2021's [34] systematic literature review from 2010 to 2021, only 24.3% of the total research was oriented to people outside the education sector, such as urban and household respondents, adolescents, native people, pharmacists, and business owners and managers in Malaysia. Lack of focus on DL and cybersecurity in Malaysian organizations, especially among employees, causes a knowledge gap. Digital literacy is an essential part of everyday life, yet many overlook it. Engelbrecht found five key weaknesses in DL's coverage of cybersecurity in a 2017 paper. A preliminary literature search shows that no publication has addressed the study trends of digital literacy in relation to cybersecurity, in the context of information security behaviour and culture among Malaysians especially while they work remotely. A study by Nasir, 2020 [35] indicates a lack of research homogeneity in Malaysian ISC models, and there is no consistent set of criteria that can be used for all Malaysian organizations. These new results by Nasir [35] show that ISC is not properly addressed in Malaysian organizations and that there are no defined models or paradigms for an information security culture when employees work remotely. Not only should ISC be implemented in the workplace, but it should also be done while people are working remotely, especially given the current pandemic situation.

4. Proposed Framework

The research proposes evaluating the relationship between digital literacy, information security culture, and information security behaviour. The ISC was expected to be influenced by employees' DL. The assessment of DL and ISC is critical in order to identify the importance of DL for a successful ISC in the organizations. Adapted in Ng's 2012 [36] Digital Literacy Model, the Digital Competence Framework established by Calvani in 2008 [37] consists of three linked components: cognitive, technical, and social-emotional. This framework is optimal for evaluating DL. Cognitive, technical, and social-emotional aspects are the key indications of DL's influence on ISC. This research will investigate the overlap between the social-emotional and cognitive components as part of this research framework, with technology serving as the medium for initiating the DL advancement. This research will assess all of DL's primary components using sub-characteristics. Human nature is the weakest link in any security system, making ISB an essential moderating variable [38]. Performgreen UK 2019 [19], an information security provider, argues that changing employee behaviour is the most effective way to enhance an organization's information security. ISB helps researchers to examine if digitally literate personnel in an organization affect ISC. This framework is intended to offer a clear picture of whether ISB can assist in establishing the relationship between DL and ISC. In addition, the components of DL should be able to assess the acceptability of DL as a factor that will influence ISC for this research. In addition to bridging the DL, ISC, and ISB gaps, a full grasp of all factors is sought for.

This proposed research framework will be used to develop the research instrument by adopting a mixed-methods approach; both qualitative and quantitative data, based on the scope of the research topic. Because qualitative data is commonly available but does not have preset answers, while quantitative data is typically dependent on closed responses, such as those found on questionnaire instruments, a mix of qualitative and quantitative approaches is essential. Figure 1 shows the research framework and the derived hypotheses.

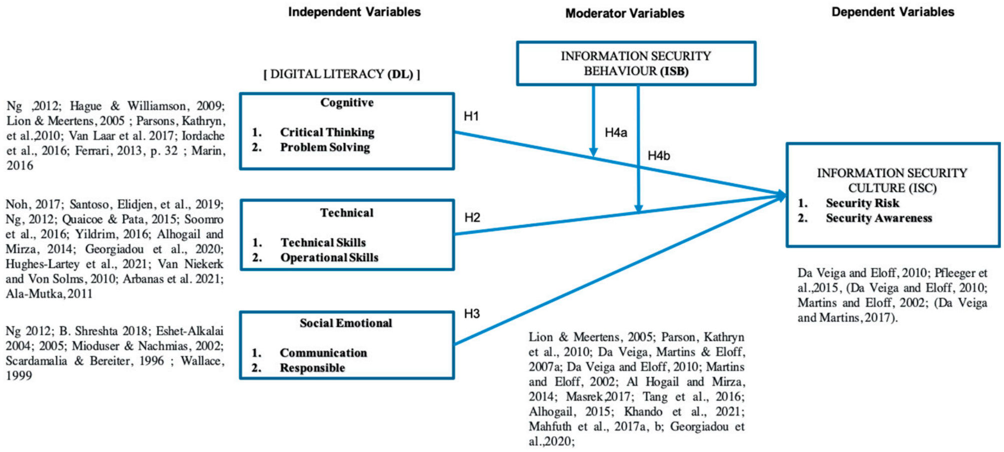
Independent Variables
Moderator Variables
Dependent Variables
[DIGITAL LITERACY (DL)]
INFORMATION SECURITY BEHAVIOUR (ISB)
Ng ,2012; Hague & Williamson, 2009; Lion & Meertens, 2005 ; Parsons, Kathryn, et al.,2010; Van Laar et al. 2017; Iordache et al., 2016; Ferrari, 2013, p. 32 ; Marin, 2016
Cognitive
1. Critical Thinking
2. Problem Solving
H1
H4a
H4b
Noh, 2017; Santoso, Elidjen, et al., 2019; Ng, 2012; Quaicoe & Pata, 2015; Soomro et al., 2016; Yildrim, 2016; Alhogail and Mirza, 2014; Georgiadou et al., 2020; Hughes-Lartey et al., 2021; Van Niekerk and Von Solms, 2010; Arbanas et al. 2021; Ala-Mutka, 2011
Technical
1. Technical Skills
2. Operational Skills
H2
INFORMATION SECURITY CULTURE (ISC)
1. Security Risk
2. Security Awareness
Da Veiga and Eloff, 2010; Pfleeger et al.,2015, (Da Veiga and Eloff, 2010; Martins and Eloff, 2002; (Da Veiga and Martins, 2017).
Ng 2012; B. Shreshta 2018; Eshet-Alkalai 2004; 2005; Mioduser & Nachmias, 2002; Scardamalia & Bereiter, 1996 ; Wallace, 1999
Social Emotional
1. Communication
2. Responsible
H3
Lion & Meertens, 2005; Parson, Kathryn et al., 2010; Da Veiga, Martins & Eloff, 2007a; Da Veiga and Eloff, 2010; Martins and Eloff, 2002; Al Hogail and Mirza, 2014; Masrek,2017; Tang et al., 2016; Alhogail, 2015; Khando et al., 2021; Mahfuth et al., 2017a, b; Georgiadou et al.,2020;

Figure 1. Proposed Research Framework.

H1: *The cognitive component has a significant relationship with information security culture.*

H2: *The technical component has a significant relationship with information security culture.*

H3: *The social-emotional component has a significant relationship with information security culture.*

H4a: *Information security behaviour will moderate the relationship between the cognitive component and information security culture.*

H4b: *Information security behaviour will moderate the relationship between the technical component and information security culture.*

4.1. Digital Literacy

Digital literacy (DL) means that information and digital technology are being utilised with self-assuredness and critical thinking to enhance personal, academic, and professional results for everyone involved. A person with DL skills can acquire and analyse data from many sources, use it in different settings, helping with problem solving and create new information in a digital environment [39]. The primary component of DL in this framework is shown by Ng's 2012 [36] Digital Literacy Model.

4.1.1. Cognitive Component

The cognitive component of Ng's [36] digital literacy paradigm is the ability to think critically throughout the search, appraisal, and creative stages of using digital information. Cognitive refers to an employee's ability to search, analyse, select, and use digital information to fulfil a work-related task while adhering to information security culture. Personality and cognitive differences may affect risk perception and tendency [40]. The study by Kathryn Parsons et al. [41] suggests that people may be categorised based on how they deal with risk, ranging from those who actively seek out danger to those who are very risk-averse. These disparities are anticipated to have an effect on how people understand the information around them, hence influencing the security behaviour that characterises the information security culture.

Table 1 shows the sub-components of the cognitive component. First, critical thinking is the ability to utilise ICT to make informed judgments and decisions about information and communication using reflective reasoning and appropriate evidence [42]. Problem solving is the second cognitive sub-component. Digital skills and competencies may be improved through problem-solving skills, which help users choose the correct digital tools to accomplish their goals and utilise digital technologies to handle conceptual and technical difficulties [43].

Table 1. Cognitive Sub-components.

No	Digital Literacy (DL)	
	Main Component	**Sub-Components**
1	Cognitive	• Critical Thinking • Problem Solving

4.1.2. Technical Component

The technical part of digital literacy is the possession of the technical and operational skills necessary to use ICT for everyday learning activities [44]. Digitally literate individuals are proficient with technology. "Technical" refers to employees' ability to upload, download, and install software for work and daily activities [36,45]. The sub-components of the technical component are shown in Table 2.

Table 2. Technical Sub-components.

No	**Digital Literacy (DL)**	
	Main Component	**Sub-Components**
2	Technical	• Technical Skills • Operational Skills

In the framework, technological components were classified as "technical," which contained three factors: antivirus protection, authentication and backup, and authorisation. These sub-components were chosen because they represent some of the most basic technical controls that organizations have built and address the three essential qualities of information security: confidentiality, integrity, and availability [46]. The second sub-component—operational abilities—pertains to computer and Internet software and hardware operation. In this context, it is crucial for individuals to understand how their data and information are shared, accessed, or used by governments and corporations; and, more importantly, they need the skills to protect themselves from disclosing information they may not need or want to disclose. Lack of the appropriate privacy settings and of critical skills can lead to loss of control and privacy [43,47].

4.1.3. Social Emotional

DL's third component is social emotional. The Internet and other digital communication platforms have introduced new dimensions and opportunities for collaborative learning through information-sharing and discussion groups, knowledge communities, and chat rooms, among other forms [48,49]. To take advantage of these new possibilities, users need sociological and emotional abilities that allow them to "understand the rules of the game" and overcome the obstacles in the information and communication of cyberspace. They need to understand the information security aspect of cyberspace and why organizations should adopt a proper information security culture [50].

Under the social-emotional component, there are two sub-components (Table 3). Communication involves using the Internet properly for conversing, interacting, and learning by following 'netiquette'. Internet etiquette governs the use of the Internet to communicate, socialise, and learn while adhering to the same rules of decorum as face-to-face encounters, such as using courteous language to prevent misunderstanding and misinterpretation [36]. The second dimension is responsible behaviour. Users are responsible for maintaining their own safety and privacy by preserving their privacy and keeping their personal information as secret as possible, not disclosing more personal information than required, and recognising when they are threatened and how to manage it.

Table 3. Social Emotional Sub-components.

No	**Digital Literacy (DL)**	
	Main Component	**Sub-Components**
3	Social Emotional	• Communications • Responsible Behaviour

4.2. Information Security Behaviour

Information security culture must include individual features, behaviours, and cognitive skills [51]. This research shows that ISB moderates cognitive and ISC implementation by organizations, supporting the idea that cognition and employee behaviour may impact risk perception (and desire to take risks) and reflect information security culture [40]. Gray and Ropeik [52] noted that an organization's culture and environment may impact how individuals think and behave. Even if employees are digitally literate and have cognitive and technical skills, understanding an organization's culture may explain why certain behaviours do or do not occur.

4.3. Information Security Culture

Information security culture is the attitudes, assumptions, beliefs, values, and knowledge which employees/stakeholders use to engage with the organization's systems and processes. Every organization wants an information security solution [10]. Despite improved technologies, companies struggle to manage information security [17]. An organization's information system security depends on employees' online behaviour. The human factor is one of the most neglected areas of IT security in organizations [10]. Focusing on staff behaviour and skills may improve an organization's information system security [11].

Information Security Culture (ISC) is recognised as an effective way to promote safe behaviour and manage security hazards in an organization. The researcher sought for framework evidence and information security culture indicators. When analysing an organization's information security culture, the security risk comes first (Table 4). To improve an organization's ISC, cutting-edge technology is given to employees (strategic component). A risk assessment (risk management component) identifies security hazards and determines how to minimise them. The second component of ISC is security awareness (Table 4), which is defined as an understanding of security threats, their negative ramifications, and the cost of security failures. "Security culture" refers to people's awareness and understanding of security issues and rules in the context of information security [53].

Table 4. Information Security Culture Components.

No	**Information Security Culture (ISC)**	
	Main Component	**Components**
4	Information Security Culture (ISC)	• Security Risk • Security Awareness

5. Discussion and Conclusions

It is crucial to understand employees' digital literacy and behaviour towards a successful information security culture, particularly in remote work environments. The research will give insight into employee digital literacy and how the remote work environment affects information security behaviour based on the organization's information security culture both when there are no additional security restrictions and when there are guidelines for working in a remote environment. Understanding the knowledge gap concerning the relationship between these factors, this research intends to contribute to this new research area and enhance present efforts and work in DL, ISC and ISB, applying the framework described above, and also developing guidelines. This research aims to improve the mapping of employees' digital literacy competency by combing it with an information security culture framework. It seeks to influence information security behaviours associated with working in a remote work environment, as well as assisting the government, policymakers, and organizations to remedy the knowledge gap concerning the said variables.

Author Contributions: Conceptualization, M.S.K. and S.M.S.; methodology, M.S.K. and S.M.S.; writing—original draft preparation, M.S.K.; writing—review and editing, M.S.K., S.M.S. and K.A.W.; supervision, S.M.S. and K.A.W.; project administration, M.S.K. and S.M.S.; resources, M.S.K. and S.M.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Special thanks to the Faculty of Information Management, Universiti Teknologi Mara Selangor Branch, Shah Alam, particularly the supervisors, for their assistance and guidance, as well as the event secretariats for the opportunities provided. Paper presented during a panel—organized by Universiti Teknologi MARA—in the context of the International Academic Symposium of Social Science 2022 (IASSC 2022).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. AlHogail, A. Design and validation of information security culture framework. *Comput. Hum. Behav.* **2015**, *49*, 567–575. [CrossRef]
2. Van Niekerk, J.F.; Von Solms, R. Information security culture: A management perspective. *Comput. Secur.* **2010**, *94*, 476–486. [CrossRef]
3. Cheng, L.; Liu, F.; Yao, D. Enterprise data breach: Causes, challenges, prevention, and future directions Wiley interdisciplinary reviews. *Data Min. Knowl. Discov.* **2017**, *7*, e1211. [CrossRef]
4. MyCert. 2017 Data Breaches Known So Far. Available online: www.mycert.org.my/data/content_files/27/831.pdf (accessed on 8 May 2020).
5. PriceWaterhouseCoopers. The Global State of Infor—Mation Security®Survey 2018. Available online: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/infor-mation-security-survey.html (accessed on 2 October 2019).
6. AlHogail, A.; Mirza, A. Information security culture: A definition and a literature review. In Proceedings of the 2014 World Congress on Computer Applications and Information Systems (WCCAIS), Hammamet, Tunisia, 17–19 January 2014; IEEE: Hammamet, Tunisia, 2014.
7. Masrek, M.N. Assessing information security culture: The case of Malaysia public organization'. In Proceedings of the 4th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, Indonesia, 18–19 October 2017; IEEE: Hammamet, Tunisia, 2017.
8. Malaysia Digital Economy Blueprint. Available online: https://www.epu.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf (accessed on 3 January 2022).
9. Aziz, K.A.; Norhashim, M.; Halim, E.M. Information security and information technology governance: A Malaysian case study. *Int. J. Manag. Pract.* **2011**, *4*, 331. [CrossRef]
10. Nel, F.; Drevin, L. Key elements of an information security culture in organisations. *Inf. Comput. Secur.* **2019**, *27*, 146–164. [CrossRef]
11. Da Veiga, A.; Eloff, J.H.P. A framework and assessment instrument for information security culture. *Comput. Secur.* **2010**, *29*, 196–207. [CrossRef]
12. Bulgurcu, B.; Cavusoglu, H.; Benbasat, I.I. Quarterly special issue information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Q.* **2010**, *34*, 523–548. [CrossRef]
13. Thomson, K.L.; Von Solms, R.; Louw, L. Cultivating an organizational information security culture. *Comput. Fraud Secur.* **2006**, *10*, 7–11. [CrossRef]
14. Gordon, L.A.; Loeb, M.P. *Managing Cybersecurity Resources: A Cost-Benefit Analysis*; McGraw-Hill: New York, NY, USA, 2005.
15. Orehek, Š.; Petrič, G. A Systematic Review of Scales for Measuring Information Security Culture. *Inf. Comput. Secur.* **2020**, *29*, 133–158. [CrossRef]
16. Tsohou, A.; Karyda, M.; Kokolakis, S. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Comput. Secur.* **2015**, *52*, 128–141. [CrossRef]
17. Singh, N.; Gupta, A.M.; Ojha, A. Identifying factors of organizational information security management. *J. Enterp. Inf. Manag.* **2014**, *27*, 644–667. [CrossRef]
18. Kontakte Klaus Julisch Managing Partner. Cybercrime—The Risks of Working from Home. Deloitte Switzerland. 2020. Available online: https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-cyber-crime-working-from-home.html (accessed on 16 March 2022).
19. *Information Security Behaviour Index. Perform Green*; Perform Green Limited: Cheltenham, UK, 2019.
20. Verizon. Data Breach Investigations Report. 2009. Available online: http://www.verizonbusiness.com/resources/security/reports/2009databreachrp.pdf (accessed on 7 June 2022).
21. Andric, M. Fighting the enemy within. *IT WEB Spec. Rep.* **2007**, *95*, 54.
22. Furnell, S.M.; Jusoh, A.; Katsabas, D. The challenges of understanding and using security: A survey of end-users. *Comput. Secur.* **2006**, *25*, 27–35. [CrossRef]
23. Walton, C.B.R.; Limited, W.-M. Balancing the insider and outsider threat. *Comput. Fraud. Secur.* **2006**, *11*, 8–11. [CrossRef]
24. Albrechtsen, E. A qualitative study of users' views on information security. *Comput. Secur.* **2007**, *26*, 276–289. [CrossRef]
25. Kraemer, S.; Carayon, P. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Appl. Ergon.* **2007**, *38*, 143–154. [CrossRef]
26. Stanton, J.M. Analysis of end user security behaviours. *Comput. Secur.* **2005**, *24*, 124–133. [CrossRef]
27. *COBIT Security Baseline—An Information Security Survival Kit*; IT Governance Institute: Schaumburg, IL, USA, 2004.

28. Furnell, S.; Navin Shah, J. Home working and cyber security—An outbreak of unpreparedness? *Comput. Fraud Secur.* **2020**, *2020*, 6–12. [CrossRef]
29. Mentsiev, A.U. The impact of digital technology on the study of languages and the development of digital education. *J. Physics. Conf. Ser.* **2019**, *1399*, 033085. [CrossRef]
30. Mentsiev, A.U.; Chebieva, H.S. Modern internet security threats and countermeasures (overview). *Eng. Her. Don.* **2019**, *3*, 15.
31. Pritam, S.N.; Vineeta, N.; Akhilesh, C.P. Impact of Information Technology on Learning, Teaching and Human Resource Management in Educational Sector. *Int. J. Comput. Sci. Telecommun.* **2011**, *2*, 66–72.
32. Boss, S.R. If someone is watching, I'll do what i'm asked: Mandatoriness, control, and information security. *Eur. J. Inf. Syst. Off. J. Oper. Res. Soc.* **2009**, *18*, 151–164. [CrossRef]
33. Burkell, J.A.; Fortier, A.; Di Valentino, L.; Roberts, S. Enhancing key digital literacy skills: Information privacy, information security, and copyright/Intellectual Property. *FIMS Publ.* **2015**, *35*, 67.
34. Ahsan, M.H.; Ayub, N.; Azman, N.S. Digital literacy in Malaysia: A systematic literature review on digital literacy in Malaysia: A systematic literature review on methodological approaches. *Malays. J. Qual. Res.* **2021**, *7*, 125.
35. Nasir, A. Information security culture model for Malaysian organizations: A review. *Int. J. Adv. Trends Comput. Sci. Eng.* **2020**, *9*, 117–121. [CrossRef]
36. Ng, W. Can we teach digital natives digital literacy? *Comput. Educ.* **2012**, *59*, 1065–1078. [CrossRef]
37. Calvani, A.; Cartelli, A.; Fini, A.; Ranieri, M. Models and Instruments for Assessing Digital Competence at School. *J. E-Learn. Knowl. Soc.* **2008**, *4*, 183–193.
38. Da Veiga, A.; Martins, N. Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Comput. Secur.* **2015**, *49*, 162–176. [CrossRef]
39. Martin, A.; Grudziecki, J. *DigEuLit*: Concepts and tools for digital literacy development. *Innov. Teach. Learn. Inf. Comput. Sci.* **2006**, *5*, 249–267. [CrossRef]
40. Lion, R.; Meertens, R.M. Security or opportunity: The influence of risk-taking tendency on risk information preference. *J. Risk Res.* **2005**, *8*, 283–294. [CrossRef]
41. Parsons, K.; Mccormac, A.; Butavicius, M.; Ferguson, L. Human Factors and Information Security: Individual, Culture and Security Environment. Science and Technology, (DSTO-TR-2484). 2010. Available online: http://www.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf (accessed on 7 June 2022).
42. van Laar, E. The relation between 21st-century skills and digital skills: A systematic literature review. *Comput. Hum. Behav.* **2017**, *72*, 577–588. [CrossRef]
43. Iordache, C.; Mariën, I.; Baelden, D. Developing digital skills and competences: A quick-scan analysis of 13 digital literacy models. *Ital. J. Sociol. Educ.* **2017**, *9*, 6–30.
44. Noh, Y. A study on the effect of digital literacy on information use behavior. *J. Librariansh. Inf. Sci.* **2017**, *49*, 26–56. [CrossRef]
45. Quaicoe, J.S.; Pata, K. The teachers' digital literacy: Determining digital divide in public basic schools in Ghana. *Commun. Comput. Inf. Sci* **2015**, *552*, 154–162. [CrossRef]
46. Arbanas, K.; Spremic, M.; Hrustek, N.Z. Holistic framework for evaluating and improving information security culture. *ASLIB J. Inf. Manag.* **2021**, *73*, 699–719. [CrossRef]
47. Ala-Mutka, K. *Mapping Digital Competence: Towards a Conceptual Understanding (Technical Note No." JRC67075-2011)*; European Commission Joint Research Centre: Seville, Spain, 2011.
48. Mioduser, D.; Nachmias, R. *WWW in Education'. Handbook on Information Technologies for Education and Training*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 23–43.
49. Scardamalia, M.; Bereiter, C. Engaging students in a knowledge society. *Educ. Leadersh.* **1996**, *54*, 6–10.
50. Wallace, P. *The Psychology of the Internet*; University Press: Cambridge, UK, 1999.
51. Da Veiga, A.; Martins, N.; Eloff, J.H.P. Information security culture—Validation of an assessment instrument. *Afr. J.* **2007**, *11*, 147–166.
52. Gray, G.M.; David, P.R. Dealing with the dangers of fear: The role of risk communication. *Health Aff. (Proj. Hope)* **2002**, *21*, 106–116. [CrossRef]
53. Lawrence, P.S.; Deanna, D.C. Leveraging Behavioral Science to Mitigate Cyber Security Risk. *Comput. Secur.* **2012**, *31*, 597–611. [CrossRef]