2022

Information Systems Security Countermeasures: An Assessment of Older Workers in Indonesian Small and Medium-Sized Businesses

Hari Samudra Roosman

Information Systems Security Countermeasures: An Assessment of Older Workers in Indonesian Small and Medium-Sized Businesses

by

Hari Samudra Roosman

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Assurance

College of Computing and Engineering
Nova Southeastern University

2022

We hereby certify that this dissertation, submitted by Hari Samudra Roosman Conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Marti Snyder

Martha M. Snyder, Ph.D.
Chairperson of Dissertation Committee

5/16/22
Date

Yair Levy, Ph.D.
Dissertation Committee Member

5/16/22
Date

Ling Wang, Ph.D.
Dissertation Committee Member

5/16/21
Date

Approved:

Meline Kevorkian

Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

5/16/21
Date

College of Computing and Engineering
Nova Southeastern University

2022

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Information Systems Security Countermeasures: An Assessment of Older Workers in Indonesian Small and Medium-Sized Businesses

by
Hari Samudra Roosman
May 2022

Information Systems (IS) misuse can result in cyberattacks such as denial-of-service, phishing, malware, and business email compromise. The study of factors that contribute to the misuse of IS resources is well-documented and empirical research has supported the value of approaches that can be used to deter IS misuse among employees; however, age and cultural nuances exist. Research focusing on older workers and how they can help to deter IS misuse among employees and support cybersecurity countermeasures within developing countries is in its nascent stages. The goal of this study was two-fold. The first goal was to assess what older workers within Indonesian Small to Medium-sized Businesses (SMBs) do to acquire, apply, and share information security countermeasures aimed at mitigating cyberattacks. The second goal was to assess if and how younger workers share information security countermeasures with their older colleagues.

Using a qualitative case study approach, semi-structured interviews were conducted with five dyads of older (50-55 years) and younger (25-45 years) workers from five SMBs in Jakarta, Indonesia. A thematic analysis approach was used to analyze the interview data, where each dyad represented a unit of analysis. The data were organized into three main themes including 1) Indonesian government IS policy and oversight, which included one topic (stronger government IS oversight needed); 2) SMB IS practices, which included three topics (SMB management issues, SMB budget constraints, SMB diligent IS practices, and IS insider threat); and 3) SMB worker IS practices, which included three topics (younger worker job performance, IS worker compliance issues, older worker IS practices) and five sub-topics under older worker IS practices (older worker diligent in IS, older worker IS challenged, older worker riskier IS practices, older worker more IS dependent, and older worker more forgetful on IS practices).

Results indicated that older and younger workers at Indonesian SMBs acquire, apply, and share information security countermeasures in a similar manner: through IS information dissemination from the SMB and through communication from co-workers. Also, while younger workers share IS countermeasures freely with their older co-workers, some have negative perceptions that older co-workers are slower and less proficient in IS. Overall, participants reported positive and cohesive teamwork between older and younger workers at SMBs through strong IS collaboration and transparent information sharing.

The contribution of this research is that it provides valuable empirical data on older worker behavior and social dynamics in Indonesian organizations. This was a context-specific study aimed at better understanding the situationalities of older workers within organizations in the developing country of Indonesia and how knowledge is shared within the organization. This assessment of cybersecurity knowledge acquisition, skill implementation, and knowledge sharing contributes to the development of organization-wide cybersecurity practices that can be used to strengthen Indonesian SMBs and other organizations in developing countries. This study also provides a blueprint for researchers to replicate and extend this line of inquiry. Finally, the results could shed light on how older workers can be a productive part of the solution to information security issues in the workplace.

Acknowledgements

First and foremost, I am extremely grateful to my doctoral advisor, Dr. Martha (Marti) Snyder, for her invaluable wisdom, mentorship, encouragement, and enduring patience during the course of my Ph.D. study, which spanned several years. My completion of this dissertation would have been impossible without her guiding presence and support throughout. Her expertise and experience have shown me what is possible beyond one's perceived limits of fortitude and abilities.

I also want to thank Dr. Yair Levy and Dr. Ling Wang for their wisdom, guidance, insight, optimism, and encouragement throughout my study.

Finally, I want to thank the interview participants in Jakarta for their generous time in between their busy work and family schedules. This study could also never have been completed without their critical contributions.

Table of Contents

Chapters

Appendices

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

Information security can be defined as “the protection of information and IS from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability” (National Institute of Standards and Technology [NIST], 2011, p. 93). Information security is an important focal point for organizations large and small, and there is no shortage of advice on effective organizational approaches. Oftentimes however, the term cybersecurity is used interchangeably with information security. Conflating the two terms can make important differences unclear. Weiss et al. (2013) distinguished between information security and cybersecurity by explicitly stating that cybersecurity includes using Information Technology (IT) offensively to attack adversaries. There are various definitions and interpretations of cybersecurity (e.g., Bay, 2016; Craigen et al., 2014; Schatz et al., 2017; Von Solms & Von Solms, 2018). Rout (2015) provided definitions of cybersecurity according to different contexts such as technology media, industry sectors, the U.S. government, and research firms. Given the context of this research is industry, the definition from the International Telecommunication Union (n.d.) and also cited by Rout (2015) as a definition for industry sectors is most relevant as follows: “Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cybersecurity environment and organization and user's assets" (para. 1).

There are many ways that IT can be used to attack adversaries. These are called cyberattacks. The more common cyberattacks include the following:

1. Denial-of-Service (DOS) and Distributed Denial of Service (DDOS) attacks. DDOS attacks force a high volume of individual systems connected to the Internet to send bulk traffic to the same destination simultaneously (Kavisankar & Chellappan, 2011). Kavisankar and Chellappan (2011) stated that the bulk traffic the systems produce can cripple the network and system traffic the systems produce can cripple the network and system resources of the targeted recipient. DDOS attacks are easy to implement and difficult to be effectively stopped and have become one of the most serious ongoing threats in computer network security. One common DDOS variant are Transmission Control Protocol (TCP) synchronize flood (SYN Flood) attacks, where attackers overwhelm the TCP protocol connection queue of the host, thereby denying legitimate connection requests. Adding to this, a significant vulnerability in current network architectures is authentication of the source address, which is concerned with only the destination targeted by the packet, and attackers can exploit this vulnerability and attempt to impersonate the source address as a trusted source of the server (Kavisankar & Chellappan, 2011). Numerous incidents of major DDOS attacks have been reported and are used by malicious parties to blackmail organizations and companies that rely heavily on network access and availability (Stefanidis & Serpanos, 2005).
2. Man-in-the-Middle (MITM) attacks. MITM attacks exploit the logic behind Hypertext Transfer Protocol Secure (HTTPS) servers which transmits certificates with public keys

to web browsers (Callegati et al., 2009). Callegati et al. (2009) stated that attackers replace the original certificate authenticating the HTTPS server with modified certificates and can succeed in the attacks if the recipients neglect to reverify the certificate when the browser sends a warning notification to them, and that MITM attacks occur more frequently among users who use self-signed digital certificates when accessing intranet sites.

3. Phishing and spear phishing attacks. Phishing is a form of online identity theft using social engineering and technical subterfuge to steal user credentials, such as usernames and passwords (Badra et al., 2007). In phishing attacks, attackers pose as trustworthy sources to deceive targets into sharing their user credentials and personal information (Sumner & Xuan, 2019). Sumner and Xuan (2019) stated that spear phishing is a type of phishing attack where attackers attempt to steal information on selected targets rather than a mass of indiscriminate targets, and targeted data sources for phishing attacks include web pages, emails, and domain names.
4. Malware attacks. Malware attacks are caused by malicious software including worms, viruses, bots, rootkits, and spyware (Chen & Ji, 2009). Any software that does something that causes harm to a user, computer, or network can be considered malware (Zhioua, 2013). Chen and Ji (2009) stated that a key characteristic of malware is self-propagation where the malware can infect vulnerable hosts and exploit infected hosts to self-disseminate, and key components of malware propagation are malware-scanning methods, namely, how effectively the malware can detect and attack vulnerable targets.
5. Business Email Compromise (BEC). BEC attacks are sophisticated email scams that specifically target businesses which specialize in or routinely conduct wire transfers as

part of their normal operations, and exploit legitimate business email accounts through hacking, phishing, and social engineering to deceive victims into unwittingly committing fraudulent wire transactions (Aviv et al., 2019). Aviv et al. (2019) stated that social engineering is a key component in BEC attacks, and cybercriminals have been successful in defrauding businesses and employees worldwide through BEC and other attacks; further, BEC attacks have been blamed for over $26 billion in global financial losses, with losses continually escalating.

There have been several high-profile cyberattacks. One notable case was the 2010 Stuxnet malware attack, which specifically targeted Iran's nuclear system infrastructure. The Stuxnet attack and its subsequent damage on Iran's Natanz uranium enrichment facility is believed to have been the underlying cause of the three-year delay in the country's nuclear program (Zhioua, 2013). The massive data breach of Equifax in 2017 was another large scale international cyberattack which resulted in the theft of personal records of 148 million Americans, 15 million Britons, and 19,000 Canadians (Viswanatha et al., 2020). Viswanatha et al. (2020) reported that the malicious attack originated from state actors affiliated with China's People's Liberation Army. Organizational data breach has become as typical as news of car accidents on the highways (Levy & Gafni, 2021).

Kayworth and Whitten (2010) suggested that a modern-day view of IS security measures should include both technical and socio-organizational factors. Kayworth and Whitten stated that from a socio-organizational perspective, human behavior continues to be an important area of research in IS security in the United States, and the study of human behaviors that contribute to the misuse of information system resources within organizations is well documented; however, more research is needed across contexts and cultures. For instance, in a meta-analysis to identify key antecedents to employees' behavior relating to security policy compliance, Cram et al. (2019) identified one of its noteworthy findings as "the importance of selected antecedents for particular national cultures" (p. 549).

Developing countries rely on IS security advancements from the western world because they often lack the resources, experience, and expertise within their countries (Zareen et al., 2013). Zareen et al. (2013) stated that it is important for developing countries to better understand how they can inform, educate, and motivate their workforce on policies and practices related to IS security, so that they can implement strategies to deter user misuse of IS, and contribute to a more globally secure workplace. D'Arcy et al. (2009) tested an extended deterrence theory model on 269 computer users from eight different companies and found that the key practices that can discourage misuse of information system resources are awareness of security policies; Security, Education, Training, and Awareness (SETA) programs; and computer monitoring.

D'Arcy et al. (2009) indicated that SETA could be an effective deterrent to IS misuse and recommended greater focus on SETA programs and dedicating resources to support them. Additionally, D'Arcy et al. (2009) recommended that given cultural and legal differences in other countries, future research outside of the United States is needed. Hovav and D'Arcy (2012) examined whether national culture influenced the deterrent capabilities of information security policies, SETA programs and computer monitoring. Using U.S. and South-Korean sample data, Hovav and D'Arcy (2012) found that the deterrent effect of certain security countermeasures differed between the two countries, as did the influence of age and gender.

The value of the older workers in organizations is well-documented. Older workers can provide valuable talent and knowledge to organizations and often possess greater experience, knowledge, skills, maturity, professionalism, work ethic, quality awareness, and lower rates of turnover than younger workers (Ciutiene & Railaite, 2014; Hughes et al., 2019). Older workers can also have a greater capacity for teamwork, leadership, and high social competence in soft skills (Hughes et al., 2019). Additionally, Small to Medium-sized Businesses (SMBs) tend to be owned and operated by older members, who are the key decision makers of the businesses who can dictate policies, including cybersecurity policies of the SMBs that they run (Lichtenstein, 2014). Thus, older members of SMBs can, in their capacity as owners and key decision-makers, also serve as valuable resources to support cybersecurity policies and countermeasures within the organization.

Organizations regard knowledge as one of its most strategic resources, and management of its knowledge critical to its organizational success (Ipe, 2003). This paradigm has led to the conceptualization of knowledge management, which can be defined as an organizational systemic effort to capitalize on the cumulative knowledge possessed by the organization (Serban & Luan, 2002). Organizations have been increasingly standing up Knowledge Management Systems (KMS) and practices to optimize their knowledge resources and capabilities (Ipe, 2003). As the exchange of information between employees in organizations is a critical part of the knowledge management process, knowledge-sharing has become a major focus area in knowledge management (Cabrera & Cabrera, 2002; Hendriks, 1999).

Organizations, however, face challenges in knowledge-sharing and KMS buy-in among employees due to difficulties in encouraging employees to share their ideas (Cabrera & Cabrera, 2002). Connelly et al. (2020) indicated that employees can be unwilling to share their knowledge, even when organizational practices are designed and encouraged to facilitate knowledge sharing and transfer. This deliberate obfuscation or withholding of organizational knowledge by an employee is known as knowledge-hiding. Knowledge-hiding can be defined as an intentional attempt by an individual to withhold or conceal knowledge requested by another individual (Chawla & Gupta, 2020). Knowledge hiding can be influenced by a multitude of factors, such as personal and interpersonal organizational dynamics, as well as external pressures (Chawla & Gupta, 2020; Connelly et al., 2012; Gagne et al., 2019). Yang and Ribiere (2020) theorized that employees engage in knowledge-hiding in organizations due to their perception of competitive advantage through their sustained proprietary knowledge. Knowledge-hiding is a barrier to knowledge sharing and can disrupt organization performance and effectiveness (Silva De Garcia et al., 2020).

Problem Statement

The United Nations Information Economy Report (2017) emphasized how the new digital era would impact the world, noting “This has major implications for the implementation of the 2030 Agenda for Sustainable Development, presenting significant opportunities but also challenges for developing countries” (p. xiii). Coupled with the growth of digitization in developing countries is the growth in the number of older adults in the workplace (Soja & Soja, 2020). While some research has pointed to the deficits of older workers, there is growing evidence of the value that older workers bring to their organizations. Older workers provide valuable talent and knowledge to organizations and often possess greater experience, knowledge, skills, maturity, professionalism, work ethic, quality awareness, and lower rates of turnover than younger workers (Ciutiene & Railaite, 2014; Hughes et al., 2019;).

The research problem focuses on cybercrime as an ongoing threat which can cause significant financial losses to SMBs (Amrin, 2014; Anderson et al., 2019; Berry & Berry 2018; Paoli et al., 2018; Smith et al., 2010). Attackers are using increasingly sophisticated methods and continuously adapt and evolve their attack techniques and tactics (Aviv et al., 2019; FBI IC3, 2020). It is well-documented in the literature that older workers serve as valuable leaders in SMBs due to their professionalism, maturity, and experience (Ciutiene & Railaite, 2014; Hughes et al., 2019). However, research remains limited on how much older workers know about cyber-attacks, how they acquire cybersecurity Knowledge, Skills, and Abilities (KSAs), what they do to mitigate cyber-attacks, and how they share their knowledge and skills with colleagues.

Dissertation Goal

The goal of this research was two-fold. The first goal was to assess what older workers within Indonesian SMBs do to acquire, apply, and share information security countermeasures aimed at mitigating cyberattacks. The second goal was to assess if and how younger workers share information security countermeasures with their older colleagues.

This was a context-specific study aimed at better understanding the situationalities of older workers within organizations in the developing country of Indonesia and how knowledge is shared within the organization. It is hoped that an assessment of cybersecurity knowledge acquisition, skill implementation, and knowledge sharing will contribute to the development of organization-wide cybersecurity practices that can be used to strengthen Indonesian SMBs as well as other organizations in developing countries. Furthermore, the results could shed light on how older workers can be a productive part of the solution to information security issues in the workplace.

Research Questions

The following research questions guided this research:

1. What countermeasures are currently in place in Indonesian SMBs to mitigate cyberattacks?

2. How do older workers acquire information on countermeasures?
3. How do older workers apply countermeasures to protect their organizations?
4. How do older workers share their knowledge and skills related to cybersecurity countermeasures with other employees in their organization?
5. What knowledge related to cybersecurity countermeasures do older workers hide from younger employees in their organization?
6. How do younger workers share cybersecurity countermeasures with older workers?
7. What knowledge related to cybersecurity countermeasures do younger workers hide from older employees in their organization?

Relevance and Significance

Despite obstacles faced by older workers, such as perceived weakness in their technology skills and awareness in the workplace, literature indicates that compliance of older workers in IS security practices is comparable to younger workers. The underlying reasons to this remain unclear, but literature has offered possible explanations, such as age and gender being a predictor for IS security awareness and compliance, and age being an indicator of maturity and stronger sense of responsibility.

Conflicting studies indicate, on one hand, that age can be a more accurate predictor to IS security awareness, resulting in older workers being more compliant and risk-averse in information security than younger workers. But on the other hand, studies also indicate information security training trumping other factors, such as age and gender, in information security awareness enhancement among workers. Findings from this study can contribute to the information security body of knowledge by providing practitioners with better understanding of IS security compliance practices specific to older workers. Organizations can also adopt findings into their IS security compliance best practices, or to address IS security compliance deficiencies, such as in training or strategic planning programs focusing on needs of their older employees.

Barriers and Issues

Challenges were encountered in gathering the source data for this research. The original plan was to conduct a field study with organization workers in Jakarta, Indonesia, and collect data from interviews with them. During this period however, the COVID-19 global pandemic abruptly emerged, resulting in international travel restrictions which included Indonesia. Indonesia was significantly impacted by this pandemic, and the Indonesia Government drastically restricted foreign visitors. This was the main challenge to the study. The workaround to this was to conduct the interviews remotely from the United States with the subjects in Indonesia via Zoom and WhatsApp remote video teleconferencing. The second challenge was to recruit participants sufficient for this study. Thirty-two prospective participants were contacted and 24 agreed to be interviewed; however, 16 participants actually committed to and completed the interview process.

The time zone difference between the United States and Indonesia proved another challenge. Participants dictated their availability for the interviews which were mostly during their afternoon work week hours. This meant that most interviews were conducted during workdays in the early morning hours between 0300 to 0700 in the U.S. Eastern time zone.

Assumptions, Limitations and Delimitations

Several assumptions were made in this study. Regarding cybersecurity, SMBs are generally assumed to be in a more disadvantaged position and status compared to larger businesses. This is certainly not always the case, as there are many SMBs that are well-resourced and well-managed in their cybersecurity implementation. Indeed, many SMBs are themselves leading IT and cybersecurity firms that provide authoritative and lucrative consulting expertise to large organizations with high demand. At the same time, there are many large business and government organizations, which in their cybersecurity implementation, face serious budget and resource constraints, poor governance and oversight from management, and bureaucratic inefficiencies, all which aggregately compromise their state of cybersecurity. Sectors of the U.S. Federal Government often face budget shortfalls and delays in their cybersecurity implementation. Therefore, it was acknowledged that the size of an organization and magnitude of its resources are not necessarily a reliable indicator of success in cybersecurity.

The second assumption was that older workers can be an asset to organizations and that they can be as productive and technologically proficient as their younger counterparts, through longer job experience and relevant technology training and education. While this assumption can be validated through case studies and examples, this assumption was also acknowledged in that there are also some older workers who fall within the negatively perceived category of not being as productive and technologically proficient as their younger colleagues due to multiple reasons, such as outdated technology, job roles and responsibilities, and absence of training in current technologies. At the same time, younger workers may appear to have an inherent advantage of added IT literacy and proficiency by virtue of being part of a generation that grew parallel to the IT revolution. Yet, these advantages do not necessarily guarantee IT competency and effectiveness in the workplace, as there are criteria beyond this to measure worker value to the organization. Therefore, the relativity in relationship between worker age and job competency and effectiveness was also acknowledged.

There were also limitations. This study was an ambitious effort involving research and synthesis of multiple disciplines and topics—each complex and with large bodies of research and knowledge. These disciplines and topics included cybersecurity, cybercrime, information assurance, IT, SMB management, knowledge hiding, aging workforce, and organizational change. Added to this synthesis were cultural dimensions such as cybersecurity, aging workers, and SMB cybersecurity management in Indonesia culture, society, and business environment. Therefore, from a research scoping perspective, it was expected that this study would conclude with significant gaps remaining and in need of future research.

Extensive advanced coordination for interviews with study participants in Indonesia was conducted. Thirty-two prospective participants were contacted and invited for this research. Twenty-four participants initially indicated their agreement to be interviewed. Eight of the 24 prospective participants, however, became non-committal and then completely unresponsive to the researcher's follow-on communication to reconfirm their interview schedules. Ultimately, 16 of the 24 participants actually participated and completed the interviews.

The ideal research interview is where the participant is open and responsive to all questions asked, and the data collected from the interview can be analyzed and interpreted into meaningful research findings. This was not the case for some participants as their interviews unfolded. Some participants were curt and hurried in their responses and appeared aloof and intent on finishing the interview. Some other participants responded that they did not know the answer to several questions because they were not qualified due to their limited IS knowledge, or because that they did not work in the IS or IT department. These non-responses are noted by the blank fields or "Don't Know" responses in the Participant Interview Response Data in Appendix

C. At the same time, other participants were talkative, responsive, and thoughtful and intelligent in the responses to all interview questions.

It was difficult to identify whether participants withheld information in their responses. Participant responses were mostly formal and diplomatic with exception of three participants who were more candid about deficiencies in their SMBs and characterizations of some co-workers. Some participants alluded to past insider threat incidents without going into further detail. Other participants described shortcomings in IS performance of their co-workers in a polite and sometimes joking manner. It could not be determined whether more descriptions of co-worker shortcomings were withheld.

As cited, the scope of the study encompassed a range of disciplines and topics which the study cannot fully cover. Therefore, delimitations were established and distilled to key points of the disciplines and topics that correlate directly to the study to make completion manageable and finite. Another delimitation was the context. Participants were limited to those who work in SMBs in Indonesia.

Definitions of Terms

Following is a list of terms and how they are defined within the context of this study.

Anomaly Intrusion Detection: An intrusion detection which attempts to estimate the normal or standard behavior of the system to be protected and generate an anomaly alarm whenever activity deviating from the normal behavior occurs (Kabanda et al., 2018).

Business Email Compromise (BEC): A sophisticated email scam that targets businesses specializes in or routinely conduct wire transfers as part of its normal operations, and exploits legitimate business email accounts through hacking, phishing, and social engineering to deceive victims into unwittingly committing fraudulent wire transactions (Aviv et al., 2019).

Cybercrime: An omnipresent threat targeting organizations of all types, with attackers utilizing sophisticated methods and continuously evolving their attack methods (Aviv et al., 2019).

Cybersecurity: Tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cybersecurity environment and organization and user's assets (International Telecommunication Union, 2008).

Cybersecurity Capacity Building: An approach for dealing with increasing cyber threats and mitigating the impacts of cyberattacks. Cybersecurity Capacity Building includes domains of policy and strategy; cultural and societal norms and behavior; cybersecurity education training and skills; legal and regulatory frameworks; standards, organizational arrangements, and technologies (Dutton et al., 2019).

Denial-of-Service (DOS) Attack: An attack characterized by an explicit attempt by the attacker to prevent legitimate users of a service from using the desired network resources (Lau et al., 2000). An example of a DOS attack is an attempt by an attacker to overwhelm the target network and cripple its bandwidth and network traffic (Lau et al., 2000).

Deterrence Theory: the application of security countermeasures to deter information systems misuse in organizations (D’Arcy & Hovav, 2005).

Distributed Denial of Service (DDOS) Attack: The distributed format of DOS which adds multiple dimensions that makes these attacks more difficult to prevent (Lau et al., 2000). A DDOS attack is composed of four elements: It involves a victim, i.e., the target host; it involves the presence of the attack daemon agents; there is a control master program, which coordinates the attack; and there is the mastermind behind the attack (Lau et al., 2000).

Heuristic Research: A research process that begins with a question or problem which the researcher seeks to illuminate or answer (Moustakas, 1998).

Honeypot: A computer connected to the Internet that offers services and data that appear to be of value to an attacker but are in fact deception traps used to monitor and log activities of attackers (Kabanda et al., 2018).

Hybrid Approach in Anomaly and Signature Intrusion Detection Methods: Deployment of a principal signature-based detection module which is combined with a complementary anomaly-based scheme (Kabanda et al., 2018).

Information Security (IS): The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction to provide confidentiality, integrity, and availability (National Institute of Standards and Technology, 2011, p. 93).

Information Technology (IT): Computer software and hardware solutions that provide support to management, operations, and strategies in organizations (Thong & Yap, 1995).

Intrusion Detection Systems (IDS): A passive security systems that detects and flags irregular network activities that fall outside acceptable behavior (Choi & Allison, 2017).

Intrusion Prevention Systems (IPS): A system that performs control functions that take active roles in securing networks and restricting potential and actual network threats (Choi & Allison, 2017).

Knowledge Hiding: An intentional attempt by an individual to withhold or conceal knowledge requested by another individual, which can be influenced by individual, interpersonal dynamics, and organizational factors (Chawla & Gupta, 2020; Connelly et al., 2012).

Knowledge Sharing: A process where individuals mutually exchange their tacit and explicit knowledge to create new knowledge (Van den Hooff et al., 2004).

Malicious Software (Malware): Any software that does something that causes harm to a user, computer, or network can be considered malware (Zhioua, 2013). Attacks caused by malicious software including worms, viruses, bots, rootkits, and spyware (Chen & Ji, 2009).

Man-in-the-Middle (MITM) Attack: Attack which exploits HTTPS server logic and transmits certificates with public keys to web browsers (Callegati et al., 2009).

Phishing: Online identity theft using social engineering and technical subterfuge to steal user credentials, such as usernames and passwords (Badra et al., 2007).

Rationalized Hiding: The act of the knowledge hider blaming other parties for failing to provide required knowledge or present a justification of being unable to submit the requested knowledge (Butt & Ahmad, 2019).

Security Education, Training, and Awareness (SETA): An educational program that is designed to reduce the number of security breaches that occur through a lack of employee security awareness (Hight, 2015).

Signature Pattern: A type of intrusion detection which seek defined patterns, or signatures, within the analyzed data (Kabanda et al., 2018).

Small to Medium-sized Business (SMB): A business that due to its size has different IT requirements and can face different IT challenges than larger businesses (Gartner, n.d.). An SMB can be categorized as an organization with less than 100 employees (Gartner, n.d.).

Spear Phishing: A phishing attack where attackers attempt to steal information on specific targets and their data sources which include web pages, emails, and domain names — rather than broad indiscriminate targets (Sumner & Xuan, 2019).

Stuxnet: A computer program designed to penetrate and establish control over remote systems in semi-autonomous fashion (Farwell & Rohozinski, 2011). Stuxnet represents a new generation of fire-and-forget malware that can be aimed in cyberspace against selected targets (Farwell & Rohozinski, 2011).

Web Server Logging: Activity to gain knowledge of the state of a web server with suitable web server log information (Kabanda et al., 2018).

List of Acronyms

Following is a list of acronyms that are used within this document.

BEC	Business E-mail Compromise
BI	Bank Indonesia (Indonesia’s Central Bank)
BLS	Bureau of Labor Statistics
BSSN	Badan Siber dan Sandi Negara (Indonesian Cybersecurity Agency)
CCB	Cybersecurity Capacity Building
CERT-ID	Computer Emergency Response Team – Indonesia
COVID-19	Coronavirus Disease 2019
CSI	Crime Scene Investigation
CSIRT	Critical Security Incident Response Teams
DDOS	Distributed Denial of Service
DOS	Denial-of-Service
EAC	E-mail Account Compromise
FBI	Federal Bureau of Investigation
HR	Human Resource
HTTPS	Hypertext Transfer Protocol Secure

IC3	Internet Crime Complaint Center
ICT	Information and Communication Technologies
IDS	Intrusion Detection Systems
IDSIRTII	Indonesia Incident Security Response Team on Internet Infrastructure
IEC	International Electrotechnical Commission
IP	Information Protocol
IPS	Intrusion Prevention Systems
IS	Information Systems
ISKS	Information Systems Knowledge Sharing
ISO	International Organization for Standardization
ISP	Information Security Policy
IT	Information Technology
ITIL	Information Technology Infrastructure Library
KMS	Knowledge Management Systems
KSA	Knowledge, Skills, and Abilities
MITM	Man-in-the-Middle
MSMB	Micro to Small and Medium Sized Business
NIST	National Institute of Standards and Technology
OSSIEM	Open-Source Security Information and Event Management
SETA	Security Education, Training, and Awareness
SIEM	Security Information and Event Management
SMB	Small to Medium-sized Business
TCP	Transmission Control Protocol

Summary

This chapter provided a description of the current situation including the essence of the research problem, goal, and research questions. The critical role of information security in organizational IT implementation, and the most known cyberattacks and methods employed by the attackers were identified. Case examples of notable cyberattacks on organizations and governments were discussed to underscore the seriousness of external and internal cyberthreats. The vulnerability of developing countries in cybersecurity, mainly due to resource constraints, was addressed, as well as the role and benefit of SETA for organizations to raise cybersecurity awareness.

The important role and value that older workers play in organizations was discussed, which include perception challenges, mostly in productivity and technical competence, from organizations, in contrast with a younger more favored workforce. The research problem identified was that cybercrime is an ongoing threat which can cause SMBs major financial losses. At the same time, cybersecurity attackers are becoming increasingly sophisticated and continuously adapting and evolving their penetration methods. What is still unclear and less understood, however, is how much older workers are knowledgeable on cybersecurity, and how they acquire their cybersecurity KSAs and share it with colleagues.

The dissertation goal was presented, which was to assess cybersecurity behavior of older workers at Indonesian SMBs, as well as the behavior of young workers, specifically in sharing cybersecurity knowledge with their older colleagues. The research questions provided direction and scope for the research problem and dissertation goal. The relevance and significance of this research, the anticipated barriers and issues and assumptions, limitations, and delimitations were described. The chapter concludes with definitions of terms and a list of acronyms.

Chapter 2

Review of Literature

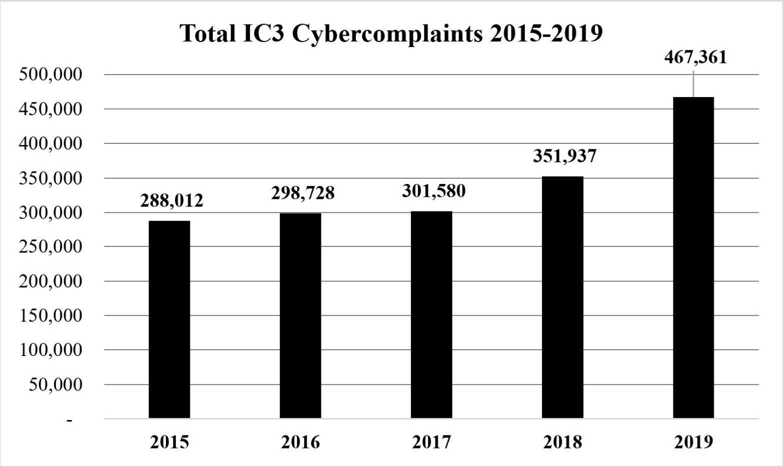
The following review of the literature includes a discussion of the topics relevant to the research problem, goal, and research questions. This review is organized in the following order: Current and Emerging Threats in Cybersecurity; SMBs and Cybersecurity; Cybersecurity Landscape in Developing Countries; Older Workers; Deterrence Theory in IS; Summary of What is Known and Unknown; and Chapter Summary.

Current and Emerging Threats in Cybersecurity

Cybercrime is an omnipresent threat targeting organizations of all types, with attackers utilizing sophisticated methods and continuously evolving their attack methods (Aviv et al., 2019). E-mail is the most common route used by attackers to compromise organizations for financial gain (Aviv et al., 2019). Information security is a serious concern for both businesses and society. Estimates of the financial impact of compromises to information security range from tens, if not hundreds of billions of dollars (United Nations, 2005) to over one trillion dollars each year worldwide (Mercuri, 2003). As shown in Figure 1, cybersecurity related complaints rose from 288,012 in 2015 to 467,361 in 2019 (Federal Bureau of Investigation Internet Crime Complaint Center, 2019).

Figure 1

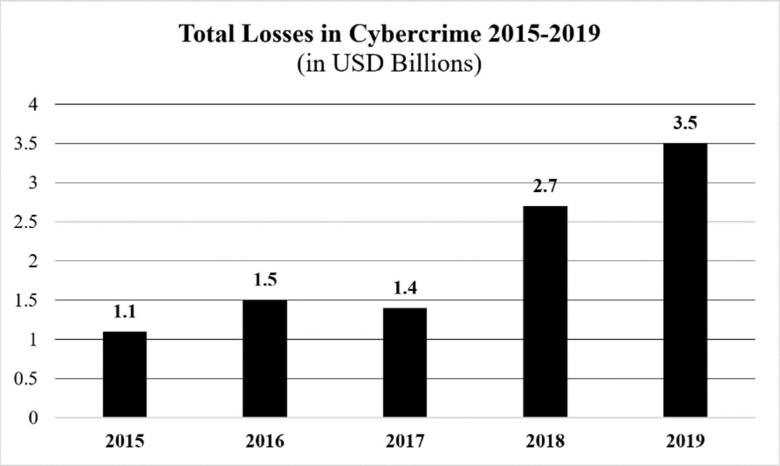
FBI IC3 Cybersecurity Complaints 2015-2019



Losses to victims exceeded US $3.5 billion in 2019 (Figure 2). The U.S. Federal Bureau of Investigation Internet Crime Complaint Center (FBI IC3, 2019) divides cybercrime complaints into Business E-mail Compromise (BEC); ransomware; elder fraud; and tech support fraud (FBI IC3, 2019). The most prevalent crime types reported were phishing/vishing/smishing/pharming; non-payment/non-delivery; extortion; and personal data breach (FBI IC3, 2019). The top three crime types with the highest reported losses were BEC; confidence/romance fraud; and spoofing (FBI IC3, 2019).

Figure 2

FBI IC3 Losses in Cybercrime 2015-2019



Insider IS Misuse

Security risks often originates from inside the organization, and these risks are often due to insider IS misuse and are well-reported (Dojkovski et al., 2007). Insider IS misuse can be defined as the intentional misuse of computer systems by users authorized to access those information and networks systems, which represents a real and costly threat to organizations (Schultz, 2002).

Intentional employee misuse of IS represents a global problem, and worker IT misuse is a significant risk for organizations and a real security and financial threat (D'Arcy & Devaraj, 2012; D'Arcy & Hovav, 2004; Schultz, 2002). Worker misuse of network access or e-mail is one of the most frequent and expensive types of security breach, with research showing that IS and data loss incidents are mostly attributable to the actions of workers (D'Arcy & Devaraj, 2012). Additionally, Chelly (2016) indicated that workers often do not comply with cybersecurity guidelines and policies and may not even know that they exist.

Udofot and Topchyan (2020) stated that lack of safe practices in the organization create risks for security protection; for example, disgruntled employees can create security vulnerabilities by sabotage or due to carelessness, and security vulnerabilities can become target for exploitation by attackers. Insider threats can create substantial problems and may predict cyberattacks, since more employees may create higher vulnerability for a business (Udofot & Topchyan, 2020)

A broader example of insider threat due to neglect was the 2013 data breach of Target Corporation which resulted in the theft of 70 million customer data records and $252 million in losses (Chen, 2016). That breach was traced to unintentional insider threat (Chen, 2016). A Target vendor, Fazio Mechanical Services, utilized outdated anti-malware software and were compromised when an employee fell victim to a phishing attack, after which attackers gained access to the Target system through Fazio Mechanical Services internal link, and then proceeded to exfiltrate Target’s cache of customer data (Chen, 2016).

The 2004 CSI/FBI Computer Crime and Security Survey reported 53% of 480 industry and government respondents faced IS security incidents due to the actions of its workers, with estimated losses estimated as high as $100,000 per incident and reported $10.6 million in losses due to insider network misuse within their organizations (Gordon et al., 2005). Further, the percentage of respondents in this survey reporting IS security incidents originating from within the organization has risen steadily through the years from 37% (of 512 respondents) in 1999, to 52% (of 481 respondents) in 2004 (Gordon et al., 2005). The frequency of IS misuse and the number of losses associated with it are expected to continue in the future due to increasing sophistication of computer users and proliferation of advanced software tools (D’Arcy & Hovav, 2005; Kim et al., 2002).

Research indicated that security countermeasures can deter misuse by increasing the perceived certainty and severity of punishment for such behavior (Hovav & D'Arcy, 2012). But despite organization enforcement of IS security policies, most organizations have been focusing on external and not internal threats (Arage & Tesema, 2016). Hadlington (2017) stated that the research in the fight against cybercrime and the prevention of cyberattacks in businesses moves emphasis away from technology towards human factors, which indicates how aspects of personality, problematic Internet use and employee attitudes can impact effective Information Security behaviors. The more organizations learn about threat prevention, detection, and response, the more effective they can become at preventing and mitigating cyberattacks (Saleem et al., 2017).

Knowledge Hiding

Knowledge hiding can be defined as an intentional attempt by an individual to withhold or conceal knowledge that has been requested by another individual, and can be influenced by individual, interpersonal dynamics, and organizational factors (Chawla & Gupta, 2020; Connelly et al., 2012). Gagne et al. (2019) stated that while knowledge sharing is generally motivated through meaning and enjoyment, knowledge hiding is influenced by external pressures.

Knowledge hiding typically manifests in three forms: knowledge hiding, playing dumb and rationalized hiding (Connelly et al., 2012). In knowledge hiding, the perpetrator intentionally provides inaccurate information, or makes false promises to share information (Butt, 2020). Playing dumb occurs when the knowledge hider feigns to show lack of familiarity with the requested knowledge. Connelly et al. (2012) indicated, however, that the way in which an employee hides knowledge can depend on the characteristics of the knowledge in question; when the question was complicated, the employee was more likely to be evasive in knowledge sharing. Connelly et al.'s finding suggests that employees can adjust their knowledge hiding actions according to circumstantial requirements; for example, it may be ineffective for a knowledge-hiding employee to play dumb or rationalize when the requested knowledge is relatively straightforward.

Finally, in rationalized hiding, the knowledge hider blames other parties for failing to provide the required knowledge or presents a justification of being unable to provide the knowledge needed (Butt & Ahmad, 2019). Connelly et al. (2012) found that employees who distrust a co-worker were more likely to hide knowledge from that individual. Undesired behaviors in knowledge flow among employees can undermine knowledge sharing efforts and harm interpersonal and organizational performance (Silva De Garcia et al., 2020). Knowledge

Hiding and Knowledge Hoarding both hinder the flow of knowledge in social interactions (Silva De Garcia et al., 2020).

Employees can be unwilling to share their knowledge, even when organizational practices are designed to facilitate knowledge transfer (Connelly et al., 2012). Yang and Ribiere (2020) stated that employees of organizations hide knowledge from other employees for reasons which include sustainment of personal knowledge advantage to be more competitive, or because they are not confident with what they know. Han et al. (2020) indicated that the antecedents of knowledge hiding are competitive psychological climate which can encourage employees to withhold their knowledge to hold competitive advantage among colleagues. Han et al. (2020) indicated that employees who perceived a competitive climate at the workplace reported increased risk of knowledge hiding and suggested that competitive psychological climates encourage employees to keep their knowledge to themselves, without sharing with colleagues to hold competitive advantage over them. Serenko and Bontis (2016) found that job insecurity espoused intra-organizational knowledge hiding; when organizations encounter budget shortfalls, it reduced employees and their compensation; employees, in return, started to conceal knowledge from their colleagues to increase their expert power and demonstrate their value to the employer. This relationship may manifest itself even more in organizational contexts that are entirely performance-based.

Connelly and Zweig (2015) showed how knowledge-hiders who rationalized their behaviors and anticipated harmed relationships and retaliation from their targets. The knowledge-hider engaging in playing dumb perceived that their targets would later retaliate by withholding knowledge from them as well (Connelly & Zweig, 2015). Jiang et al. (2019)

indicated that knowledge hiding had a detrimental effect on knowledge hiders themselves by preventing them from thriving at work due to the harm it did to their psychological safety.

Floder (2020) studied the association between knowledge hiding and self-monitoring, and whether a commitment-based Human Resource (HR) system influenced this relationship. This study found that self-monitoring increased knowledge sharing motivation, specifically job autonomy and cognitive job demands enhanced knowledge-sharing while also discouraging knowledge hiding (Floder, 2020). Gagne et al. (2019) stated that work design influenced employee motivation in knowledge-sharing; for instance, younger employees in cybersecurity may hide knowledge from older colleagues due to perception of competitive advantage and lack of self-confidence against their more experienced colleagues.

Butt (2020) found that managers who relied on counterparts within the organization to complete tasks stimulated knowledge sharing while also discouraging knowledge hiding. Butt (2020) also suggested that open workspaces stimulated more open and friendly interaction among managers and reinforced the notion that organizations with strong bureaucratic systems and cultures are more prone to knowledge-hiding. Connelly et al. (2012) also indicated that employees in organizations with stronger knowledge sharing cultures were less prone to engage in evasive knowledge hiding.

Liu et al. (2020) found that employees with status in organizations may promote a range of less social behaviors, which include knowledge-hiding. Liu et al. (2020) also found that the decision on whether an employee hides or shares knowledge is complex; for example, an employee’s desirable workplace status can generate ambivalent feelings, such as feeling obliged to share knowledge and feeling envied, which in turn can trigger knowledge-protecting behavior.

Knowledge hiding can lower task performance and augments counterproductive work behaviors, and its outcomes can threaten the well-being of an organization and its members, consequently requiring timely action from organization managers (Singh, 2019). Organizations need to mitigate knowledge hiding by dismantling psychological ownership of the knowledge hider through sustained cultivation of team culture and supporting human resource practices (Singh, 2019).

Knowledge hiding can also negatively affect employee performance and lead to a culture of distrust and negativity among employees, increasing employee turnover and ultimately being detrimental for employees and the organization itself (Anand & Hassan, 2019). Lanke (2018) also stated that interpersonal relations between employees lacking dignity and respect can result in knowledge hiding behavior, particularly when the other employee has higher expertise. This can lead to lack of organizational innovativeness, and organizations need to find ways to prevent this (Lanke, 2018). Connelly et al. (2019) stated that despite continuous innovations in Information and Communication Technologies (ICT) that can improve knowledge sharing in organizations, knowledge hiding among employees remain pervasive. Organizations are becoming more knowledge-intensive, so there is a need for resilient systems to eliminate ulterior agendas and issues rooted in personal values and cultural differences (Anand & Hassan, 2019).

Business Email Compromise

Business Email Compromise (BEC) can be described as a sophisticated scam targeting business organizations and individuals which involve transfer of funds and is conducted when a user compromises legitimate business e-mail accounts through social engineering or computer intrusion methods, such as spearphishing, malware, and unauthorized fund transfer (Aviv et al., 2019). Aviv et al. (2019) reported that conventional security countermeasures, such as spam filters, have been largely unsuccessful in thwarting BEC attacks. BEC methods constantly evolve, with attackers becoming increasingly sophisticated and adept in their methods (FBI IC3, 2019).

BEC causes significant financial losses for organizations (Cross & Gillette, 2020). In 2019, the FBI IC3 received 23,773 BEC and E-mail Account Compromise (EAC) complaints with an estimated loss of $1.7 billion and $26 billion since 2016 (Cross & Gillett, 2020; FBI IC3, 2019). In another study, BEC attacks have been blamed for over $26 billion in financial losses globally, with losses continuing to escalate (Aviv et al., 2019). The economic implications of BEC are also far reaching, with proliferation in cybercrimes having adverse impact on businesses and the economies of countries (Boateng et al., 2012; Cross & Gillett, 2020). BEC and EAC constantly evolves as scammers become more sophisticated (FBI IC3, 2019).

This chapter provided an overview of the current and emergent threats in cybersecurity. Cybercrime is an omnipresent threat targeting all organizations, and cybercriminals use sophisticated methods which constantly evolve. Cybercriminals attack targets most often through e-mails, and variations of phishing, non-payment, non-delivery, extortion, and personal data breach are common forms of cybercrime. The cost of cybercrimes is estimated to range anywhere from several billions of dollars to individual victims annually, to hundreds of billions to trillion of dollars annually to organizations. BEC, romance and confidence fraud, and spoofing are the cybercrimes that cause the most losses to victims. Security risks frequently originate from organization insiders and are mostly due to insider misuse with consequences that can be both damaging and costly to the organization. Security countermeasures enacted by the organization can deter misuse through severity in punishment perceived by insiders. BEC is a form of insider information security threat where sophisticated scams target organizations with a focus on fund transfer via compromise of internal users and systems. BEC can also cause significant financial losses for organizations. Knowledge hiding, playing dumb, and rationalized hiding are variations of deliberate attempts by individuals to conceal knowledge from other individuals. These forms of knowledge hiding can negatively impact employee performance and morale, and lead to a culture of distrust and negativity among employees, thereby reducing organizational productivity and effectiveness. The studies discussed in this section are summarized in Table 1.

Table 1

Summary of Current and Emerging Threats in Cybersecurity Literature

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
Anand and Hassan (2019)	Literature review and analysis.	None (review of literature only)	Literature review	Organizations have changed a lot over the past decade. To be successful in a knowledge-based economy and to develop competitive advantage, the appropriate management of knowledge becomes a crucial task for organizations.
Arage and Tesema (2016)	Literature review and analysis.	None (review of literature only)	Positivist Paradigm. GDT and National culture constructs to study employee ISS behavior.	Almost all investments in information systems security have been focused only on technological solutions. This view on the information systems security problem is insufficient and researchers need to include social factors into the solution space, such as culture.
Aviv et al. (2019)	Literature review and analysis. Data and statistical analysis.	n=30	BECD measure leveraging a cybersecurity expert panel review and analysis process utilizing Delphi method.	The contributing attributes to BEC detection are email authenticity detection skills; malicious mobile application detection skills; ability to detect mobile malware indicators; and the ability to detect phishing emails.

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
Boateng et al. (2012)	Literature review and analysis. Data and statistical analysis.	n=40	Interviews. Exploratory case study.	Although awareness of cybercrimes have increased, cybercrimes mostly go unreported. The study recommended a multi-stakeholder effort and appropriate technical training for law enforcement and legislators.
Butt and Ahmad (2019)	Literature review and analysis. Multiple case study methodology	n=20	Qualitative interviews with managers of buying and supplying firms having a local and foreign nationality.	Based on the qualitative interviews, managers were found to be intentionally hiding knowledge from their managers based on five individual, three interpersonal and two firm-level reasons.
Butt (2020)	Literature review and analysis. Case study methodology.	n = 26	Interviews.	Strategies that organizations can employ to mitigate knowledge hiding behavior among managers include reducing chain of command; developing informal interaction among managers; and introducing and implementing incentive policy.
Chawla and Gupta (2020)	Literature review and analysis. Data and statistical analysis.	n=150	Survey-Questionnaire Likert scale Knowledge-based psychological ownership from Van Dyne and Pierce scales	Knowledge psychological ownership mediates open climate and knowledge hiding, organizational commitment moderates trust climate; and knowledge hiding and Machiavellianism moderate knowledge psychological ownership and knowledge hiding.
Chelly (2016)	Literature review and analysis. Data and statistical analysis.	n=11	Survey-Questionnaire	Need for the cybersecurity field to adopt a proactive approach towards human behavior.
Chen (2016)	Literature review and analysis.	None (review of literature only).	Review of literature	Cybersecurity criminals use small businesses, serving as vendors for larger businesses, as a bridge to gain access and steal data.

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
Connelly et al. (2019)	Literature review and analysis.	None (review of literature only).	Review of literature	Knowledge hiding remains pervasive in organizations, notwithstanding continual innovations in communication technologies that can have the potential to increase knowledge sharing among coworkers.
Connelly et al. (2012)	Literature review and analysis. Data and statistical analysis.	n=35	Survey-Questionnaire Multi-level modeling technique	Knowledge hiding is comprised of three related factors: evasive hiding, rationalized hiding, and playing dumb. These behaviors are predicted by distrust, but each also have different sets of interpersonal and organizational predictors.
Connelly and Zweig (2015)	Literature review and analysis. Data and statistical analysis.	n=194	Survey-Questionnaire Research Model AMOS 19.0. Anderson and Gerbing two-step procedure for SEM analysis. Confirmatory Factor Analysis (CFA) model	Knowledge hiding is comprised of evasive hiding, rationalized hiding, and playing dumb. Each behavior is predicted by distrust, yet each also has a different set of interpersonal and organizational predictors. Not all knowledge hiding is harmful. Some knowledge hiding may enhance relationships between colleagues and break the cycle of knowledge hiding in organizations.
Cross and Gillette (2020)	Literature review and analysis	None (review of literature only).	Gap analysis	BEC fraud can have significant impacts at a personal and collective level. Increased knowledge of these non-financial impacts will improve how organizations respond to BEC fraud and how employees can be supported before and after an incident occurs.
D’Arcy and Hovav (2004)	Literature review and analysis	None (review of literature only)	Analysis of literature.	Organizations have changed significantly in the past decade. To be successful in a knowledge-based economy and to develop competitive advantage, the appropriate management of knowledge is a crucial task for organizations.
D’Arcy and Devaraj (2012)	Literature review and analysis. Data and statistical analysis.	N = 228	Survey-Questionnaire PLS Structural Model	There is predisposition toward a need for social approval and moral beliefs regarding behavior that are key determinants of technology misuse.

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
De Garcia et al. (2020)	Literature review and analysis	None (review of literature only)	Analysis of literature using knowledge hiding, hoarding, collection, and donation framework	Social aspects and workplace characteristics could influence someone's decision to share or withhold their knowledge from co-workers.
Dojkovski et al. (2007)	Literature review and analysis	n=12	Analysis of literature using Glaser-adapted inductive grounded approach.	Eisenhardt theoretical sampling strategy SME owners may benefit from adopting a risk-based approach to IS and should be educated about the strategic role of IT/IS.
Federal Bureau of Investigation (2019)	Literature review and analysis. Data and statistical analysis.	Government Data.	Review on literature. Statistical analysis on data.	In 2019, IC3 received a total of 467,361 complaints with reported losses exceeding $3.5 billion. The most prevalent crime types reported were Phishing/Vishing/Smishing/Pharming, Non-Payment/Non-Delivery, Extortion, and Personal Data Breach. The top three crime types with the highest reported losses were BEC, Confidence/Romance Fraud, and Spoofing.
Floder (2020)	Literature review and analysis. Data and statistical analysis.	n=139	Survey – questionnaire	There is a significant direct positive relationship between self-monitoring and knowledge hiding. There is a negative non-significant moderating association of the commitment-based Human Resource system on the relationship between self-monitoring and knowledge hiding. A commitment-based Human Resource system has insufficient impact to influence self-monitoring which provides high self-monitors with opportunities to hide their knowledge.

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
Gagne et al. (2019)	Literature review and analysis. Data and statistical analysis.	n=1,394	Survey-Questionnaire Empirical method.	Cognitive job demands and job autonomy were positively related to future reports of knowledge-sharing frequency and usefulness via autonomous motivation to share knowledge. Task interdependence was positively related to forms of knowledge hiding (evasive hiding, and rationalized hiding, and playing dumb) via external regulation to share knowledge.
Gordon et al. (2004)	Literature review and analysis. Data and statistical analysis.	n=491	Survey-questionnaire	- Unauthorized use of computer systems and reported dollar amount of annual financial losses resulting from security breaches are both in the rise. - Virus attacks and denial of service has outpaced theft of proprietary information. - Organizations reporting computer intrusions to law enforcement over the last year is on the decline due to concern for negative publicity. - Most organizations conduct economic evaluation of their security expenditures, with 55% using Return on Investment (ROI), 28% using Internal Rate of Return (IRR), and 25% using Net Present Value (NPV). - Over 80% of the organizations conduct security audits. - The majority of organizations do not outsource computer security activities. Among organizations that outsource computer security activities, the percentage of security activities outsourced is low. - The Sarbanes-Oxley (SOX) Act is beginning to have an impact on information security in some industries.

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
Hadlington (2017)	Literature review and analysis. Data and statistical analysis.	n=538	Survey-Questionnaire Qualtrics Research Panel Abbreviated impulsiveness scale (ABIS) Online cognition scale (OCS) Risky cybersecurity behaviors scale (RScB) Attitudes towards cybersecurity and cybercrime in business (ATC-IB)	Aspects of personality, problematic Internet use and employee attitudes can impact on the potential to engage in effective IS behaviors in the organization.
Han et al. (2020)	Literature review and analysis. Data and statistical analysis. Hierarchical regression analyses - conceptual mode	n=296	Survey-Questionnaire	Competitive psychological climate is positively related to knowledge hiding. This relationship becomes weaker when there is high organizational justice and high optimism.
Hovav and D'Arcy (2012)	Literature review and analysis. Data and statistical analysis.	n = 366	Survey-questionnaire Research model and hypotheses derived from D'Arcy et al.'s deterrence model, Hofstede's findings, and research on Confucianism and face-saving within East Asian society. Adaptations were made to the D'Arcy et al. model based on advances in the deterrence literature and due to the contextual nature of our cross-cultural investigation.	Using U.S. and Korean samples, the study found evidence that the deterrent effect of security countermeasures varied between the two countries, as did the influence of age and gender. The results have implications for IS management practices in global businesses

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
Jiang et al. (2019)	Literature review and analysis. Data and statistical analysis.	n=214	Field survey Mediation model	Provided insight on how knowledge hiding negatively affects employees and how managers can mitigate this effect through alleviating employee cynicism. Study finds that when organizational cynicism decreases, knowledge hiding is less harmful to the hider's psychological safety and consequently less negative impact on thriving.
Lanke (2018)	Literature review and analysis.	None (review of literature only)	Review of literature.	Interpersonal interaction involving lack of dignity and respect shown toward others can result in knowledge hiding behavior, especially when the other person holds higher expertise, which can lead to lack of innovativeness in the organization. Organizations and its managers need to invest their efforts to identify ways to prevent this unfavorable behavior by their employees.
Lee and Chung (2002)	Literature review and analysis.	None (review of literature only)	Review of literature.	Approaches to detecting intrusions can be classified into two categories: Anomaly Detection and Misuse Detection. Misuse detection is best suited for reliably detecting known use patterns. Misuse detection systems can detect many or all known attack patterns, but they are of little use for as yet unknown attack methods Mobile agents to provide computational security by constantly moving around the Internet and propagating rules is presented as a solution to misuse detection.

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
				This study presents a method of use of mobile agent mechanisms to add mobility features to the process of rule propagation. This approach presents significant advantages in terms of spreading rules rapidly, increasing scalability and providing fault tolerance.
Liu et al. (2020)	Literature review and analysis. Data and statistical analysis.	n=227	Survey-questionnaire Confirmatory factor analyses (CFA)	Workplace status is associated with knowledge hiding via two opposing mechanisms: felt obligation to share knowledge and feeling envied.
Mercuri (2003)	Literature review and analysis.	None (review of literature only)	Review and analysis of literature.	Costs related to computer security are difficult to assess because accurate metrics have been unrealistic. The largest financial value involves theft of proprietary information or financial fraud. Others have resulted in significant loss of use or productivity include viruses and malware, web server denial-of-service attacks, abuse of access privileges, and equipment vandalism and theft.
Saleem et al., (2017)	Literature review and analysis.	None (review of literature only)	Review of literature.	The more organizations learn about threat prevention, detection and response, the faster they will become at preventing and mitigating cyberattacks.
Schultz (2002)	Literature review and analysis	None (review of literature only)	Review of literature. Multiple regression analysis	Novel approach for predicting and detecting insider attacks. No single indicator is sufficient to predict and detect insider attacks. Multiple indicators and a mathematical representation of each indicator contribution may be possible to predict and detect insider attacks.

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
Serenko and Bontis (2016)	Literature review and analysis. Data and statistical analysis.	n=691	Survey-Questionnaire PLS Structural model	Knowledge hiding and knowledge sharing belong to unique and overlapping constructs. Individual employees believe that they engage in lesser knowledge hiding than their co-workers. The availability of knowledge management systems and knowledge policies has no impact on intra-organizational knowledge hiding. The existence of a positive organizational knowledge culture has a negative effect on intra -organizational knowledge hiding. In contrast, job insecurity motivates knowledge hiding. Employees may reciprocate negative knowledge behavior, and knowledge hiding promotes voluntary turnover.
Singh (2019)	Literature review and analysis. Data and statistical analysis	n=198	Survey-questionnaire Confirmatory factor analysis (CFA) and structural equation modeling (SEM)	Territoriality and knowledge hiding has negative effect on task performance, but a positive influence on interpersonal and organizational workplace deviance. Knowledge hiding negatively mediates the influence of territoriality on task performance and workplace deviance.
Udofot and Topchyan (2020)	Literature review and analysis. Data and statistical analysis	n=362	Survey-Questionnaire Open Rational Systems theory and Network theory	Length of Company Ownership and Cyberattack Protection (H1). The study failed to confirm the hypothesis on the predictive relationship between length of owner experience and cyberattack protection because no linear relationship between the two variables was identified.

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
				Number of Employees and Cyberattack Protection (H2). The study failed to confirm the hypothesis of the predictive relationship between number of employees and cyberattack protection because no linear relationship between the two variables was identified. Cyberattack Knowledge and Cyberattack Protection (H3). The study confirmed the hypothesis that cyberattack knowledge predicts cyber-attack protection. Cyberattack Success Coefficient and Cyberattack Protection (H4). The study partially confirmed the hypothesis that cyberattack success coefficient predicts cyberattack protection. Cyberattack Protection in Companies with and without Cyberattack (H5). The study confirmed the hypothesis that cyberattack protection in companies with no cyberattack were higher than those with cyberattacks.
United Nations (2005)	Literature review and analysis. Metadata and statistical analysis	United Nations metadata	Statistical analysis on metadata	The vigorous efforts being undertaken by many developing countries to catch up with their more developed partners in the dissemination and use of ICT. However, it also shows that the gaps are still far too wide and the catching-up far too uneven for the promise of a truly global information society, with its attendant benefits for sustainable social and economic development, to materialize without the sustained engagement of national Governments, the business sector and civil society, and the tangible solidarity of the international community.

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
Yang and Ribiere (2020)	Literature review and analysis. Qualitative analysis	n = 5	Exploratory sequential mixed-method research design	Personal traits and sustaining personal knowledge advantage constructs significantly influenced knowledge hiding behavior, but the construct of interpersonal relationships had no significant influence on our sample's knowledge hiding behavior.

Small to Medium-sized Businesses and Cybersecurity

SMBs constitute over 95% of all businesses in the U.S. and produce about 50% of the U.S. income and 99% of all U.S. employers and are a vital segment of the U.S. economy (Kisell, 2009; Kissel et al., 2014). SMBs in the U.S. total more than 28.2 million, create over 60% of all new U.S. private sector jobs, and produce over 47% of the country's Gross National Product (Kisell et al., 2014). Therefore, it is critical for SMBs to protect sensitive data of their customers, intellectual property, and other valuable information to protect their reputation (Alshboul & Streff, 2015).

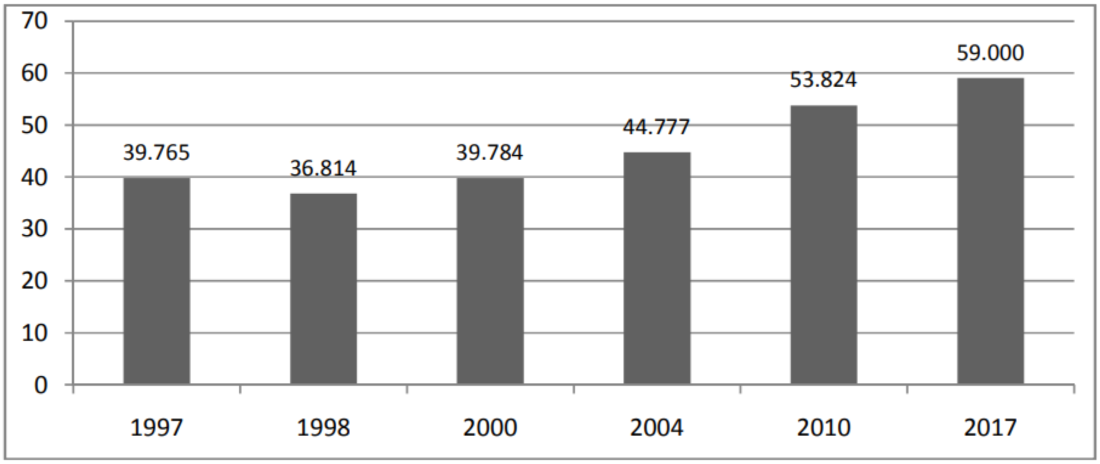
The U.S. Small Business Committee reported that 71% of cyberattacks occur at business with fewer than 100 employees (i.e., SMBs) and are generally targeted for multiple reasons, but mainly because they are easier to attack than larger organizations (Chen, 2016). SMBs are more often vulnerable to cyberattacks due to their adoption of low-cost approaches with compromised cybersecurity standards (Alahmari & Duncan, 2020). SMBs suffer from cybersecurity risk management due to their lower priorities and strategies (Alahmari & Duncan, 2020). SMBs are being increasingly targeted by online threats because attackers perceive them as being more vulnerable and are scoping new opportunities which include SMBs as targets (Hayes & Bodhani, 2013). Levy and Gafni (2020) indicated that cyberattacks focus on the individuals or small organizations in the supply chain of larger organizations that cause the domino effect.

Similarly, Indonesia has many SMBs. Suhartanto and Leo (2018) stated that Indonesia has 3,668,873 Micro and Small to Medium Businesses (MSMBs) which employ 96.2% of the national workforce and is a major part of the national economy. MSMBs in Indonesia are critical to job creation, economic growth, and foreign currencies (Tambunan, 2005; Umar et al., 2018). Tambunan and Busnetti (2018) and Tambunan (2019) indicated that the Indonesian economy is dominated by MSMBs, with figures increasing from 39.7 million in 1997, to 59 million in 2017 (Figure 3). According to Indonesia's 1986 census, SMBs (which was defined as businesses with 5 to 199 workers) generated 21% of the national industrial output and employed 52% of the national workforce (Hill, 2001). Further, the Indonesian Government declared SMBs as its national priority and included it in its five-year national development plan (REPELITA) and government policy outline (GBHN) (Hill, 2001). Additionally, the Indonesian Government established the Small Business Ministry in 1993 to provide support and ensure welfare and advancement of SMBs nationwide (Hill, 2001).

In 1997, the growth of Indonesian SMBs was negatively impacted by the country's financial crisis (Berry et al., 2002; Tambunan, 2019). The national currency depreciated by 500% by mid-1998, resulting in sharp decline in domestic product demand and a national crisis in the banking and loan sector (Berry et al., 2002; Tambunan, 2019). More recently, Indonesian SMBs have underperformed due to issues such as financial constraints and limitations in market and technology access (Suhartanto & Leo, 2018). Despite the large presence and growth of SMBs in Indonesia, SMBs that use Internet and online technology remain low due to factors such as low SMB literacy in technology (Tambunan & Busnetti, 2018). SMB technology implementation is particularly low in rural areas, where traditional business practices and paradigms remain standard practice and strong IT infrastructure has not yet been established (Tambunan & Busnetti, 2018).

Figure 3

Number of MSMBs in for the Period 1997-2017 (million units) (Tambunan & Busnetti, 2018)



While cybercrimes have become an increasing threat, many SMBs continue to be reluctant to invest in cybersecurity protection (Alahmari & Duncan, 2020; Balan et al., 2017; Choi & Allison, 2017; Dojkovski et al., 2007). Chen (2016) indicated that SMBs generally do not assume they will become victims of cybersecurity breaches and have little desire to allocate their limited resources for what they perceive as speculative risks (i.e., cybersecurity threats) that may not even occur. Hayes and Bodhani (2013) indicated that SMBs often plan cybersecurity under the misconception that their networks and data are relatively safe because they do not possess anything that would interest criminals. On the contrary, because SMBs generally have limited resources to invest in cybersecurity like larger businesses, cybercriminals opportunistically view them as easy targets (Paulsen & Toth, 2016).

In their study, Gafni and Pavel (2019) examined how SMBs, despite being targets for cyberattacks, routinely used Internet and computer systems without cyberthreat awareness or preparedness due to lack of cybersecurity knowledge or access to cybersecurity information - referred to the 'invisible hole'. Gafni and Pavel (2019) studied multiple media channels, technological and professional cybersecurity websites, and academic journals, and their findings affirmed that few studies, articles, and news items were published in the field of SMB cybersecurity. The reasons cited to this 'invisible hole' were lack of knowledge and awareness; lack or reporting; lack of media interest; and lack of public attention and information overload (Gafni & Pavel, 2019).

The U.S. Government provides information resources on SMB cybersecurity, but SMBs find it difficult and cost-prohibitive to implement cybersecurity frameworks, such as NIST 800-53 and ISO/IEC 27001, due to lack of resources and scale of frameworks (Alshboul & Streff, 2015). While these cybersecurity standards are intended for organizations of different scales, these frameworks are considered too large and complex for SMBs to operationalize (Alshboul & Streff, 2015). Shivhare and Savaridassan (2015) indicated that the complexities of securing SMBs combined with the maze of regulatory compliance puts a significant burden on SMBs. Berry and Berry (2018) indicated that while larger businesses possess the resources to address cybersecurity, SMBs often do not, and consequently, due to this lack of resources, many SMBs lack policies, procedures, and training to secure their resources, and are at great risk of cybersecurity compromise. Burns et al. (2006) also stated that many SMBs fail to implement information security policies and suffer the consequences of a security breach from threats that could have been avoided, if an IS policy had been in place. SMBs may have cybersecurity procedures and policies to counter cyberthreats, but there may be doubts on its efficacy due to the SMBs not being adept in selecting optimal cybersecurity technologies (Burns et al., 2006; Gupta & Hammond, 2005).

Dojkovski et al. (2007) found that SMB security cultures that the trend in in promotion of organizational information security cultures has been to expect organizations to be independently proactive; but while large organizations may possess more resources and technical expertise, SMBs need external support to develop information security culture internally.

Despite these costly barriers, SMBs need to implement Information Security Policies (ISPs) rather than face risk of jeopardizing their business and operational and financial viability (Almeida et al., 2018; Burns et al., 2006). Therefore, despite formidable costs, SMBs should dedicate more resources to cybersecurity risk management because of the large impact of potential cyberattacks on them (Alahmari & Duncan, 2020). Park et al. (2008) stated that cybersecurity needs to be addressed at four levels: organizational, workflow, information, and technical.

Cybersecurity experts have proposed methods to mitigate SMB cybersecurity risks. Many SMBs have also themselves implemented cybersecurity countermeasures ranging from improvement in technologies, policies, governance, training, and organizational culture. For example, Chelly (2016) recommended the outlining of three risk profiles for workers:

- High Risk Profile, which describes individuals not recognizing online risks and having very limited cybersecurity profile (Chelly, 2016).
- Medium Risk Profile, which describes individuals with partial cybersecurity knowledge. Individuals with compliance and guideline knowledge (Chelly, 2016).
- Low-Risk Profile, which describes cybersecurity knowledgeable individual with wide online responsibilities (Chelly, 2016).

Choi and Allison (2017) proposed Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) for SMB detection and defense against cyberattacks. IDS functions as passive security systems that detect and flag irregular network activities that fall outside acceptable behavior, while IPS performs control functions that take active roles in securing networks and restricting potential and actual network threats (Choi & Allison, 2017). IPS and IDS work in tandem, with IDS identifying cyberthreats and IPS interdicting them (Choi & Allison, 2017).

Kabanda et al. (2018) provided a list in Table 2 of cybersecurity methods in prevention and mitigation of cyberattacks.

Table 2

Approaches to Tackling Cybersecurity

Cybersecurity Approach	Description
Intrusion detection	Security tools that, like other measures such as antivirus software, firewalls, and access control schemes, are intended to strengthen the security of information and communication systems.
Anomaly intrusion detection	A type of intrusion detection which attempt to estimate the “normal” behavior of the system to be protected, and generate an anomaly alarm whenever the deviation between a given observation at an instant and the normal behavior exceeds a predefined threshold
Signature patterns	A type of intrusion detection which seek defined patterns, or signatures, within the analyzed data.
Hybrid approach (anomaly and signature intrusion detection methods)	Generalized use of a principal signature-based detection module, combined with a complementary anomaly-based scheme
Honeypot	Computer connected to the Internet that offers services and data that appear to be of value to an attacker but in fact is a deception traps used to monitor and log the activities of attackers
Web server logging	Gain knowledge of the state of a web server, given suitable web server log information

Ključnikov et al. (2019) found that security controls which include technical and procedural information security controls, risk management and application of standards, reflect the success of Information Security management, and is the most important success factor in Information Security management. The second most important factor was supportive management, followed by organizational awareness in the short-term (Ključnikov et al., 2019).

For information security awareness and training in SMBs, Furnell et al. (2002) stated, security policies can be effective only if workers know, understand, and can accept necessary precautions, which leads to the requirement for training and awareness in the organization to cultivate the appropriate culture. Gundu and Flowerday (2013) indicated that unintentional mistakes by employees can pose significant threats through actions, such as visiting malware infested sites, using weak passwords, storing login passwords unsecurely, which is a result of inadequate employee training. They added that information security weaknesses can never totally be eliminated, but that a well-structured security awareness campaign can help mitigate risk to acceptable levels (Gundu & Flowerday, 2013). Gupta and Hammond (2007) also indicated that information security training to employees is an additional preventive measure for the organization.

This chapter provided an overview of SMBs in the United States and Indonesia. SMBs are a critical portion of the U.S. economy because it comprises over 95% of all businesses in the U.S. income and 99% of all U.S. employers and produced over 47% of the country's Gross National Product. At the same time, 70% of cyberattacks are reported to occur at SMBs, and are targeted because they are considered easier targets than large organizations, due to their lower cybersecurity standards. Contributing to this vulnerability is the reluctance or limitations of many SMBs to invest in better cybersecurity primarily due to resource constraints. Despite the costly barriers, SMBs are still recommended to invest in cybersecurity, otherwise face risk of jeopardizing their reputation and financial viability if they are breached by a cyberattack. Indonesia has 3.6 million SMBs which employ 96% of the national workforce and SMBs play a vital role in its national economy. Despite the large SMB numbers, the overall portion that are online remain low due to low due to low literacy in IT among many SMBs and many of their remote rural locations. Improvements that are recommended for SMB cybersecurity include upgrade of cybersecurity technology, policies, governance, training, and organizational change. The studies discussed in this section are summarized in Table 3.

Table 3

Summary of Small to Medium-sized Businesses and Cybersecurity Literature

Study	Methodology	Sample	Instruments/ Constructs	Findings/Contributions
Alahmari and Duncan (2020)	Literature review and analysis	None (review of literature only) 15 of 50 published papers reviewed.	Review of literature NVivo software used in the analysis.	SMEs must give more attention to cybersecurity risk management because of the size of their market shares, and the significant impact of potential cyberattacks on them. There are five management perspectives which play a significant role in combatting and reducing cybersecurity risks —threat, behaviour, practice, awareness, decision-making— which illustrate the importance of the management role for the stability of SMEs in the current cybersecurity world.
Almeida et al. (2018)	Literature review and analysis. Data and statistical analysis	n=144	Survey/questionnaire	The top three most important elements in the structure of a security policy are asset management; security risk management; and definition in the scope of the policy. On the other hand, the three least relevant elements include the executive summary, contacts and manual inspection.

Study	Methodology	Sample	Instruments/ Constructs	Findings/Contributions
				The importance given to each element of the security policy is changed according to sectors of activity. The elements that show the greatest variability are review process, executive summary and penalties. On the other hand, the purpose of the policy and the asset management present a stable importance for all sectors of activity.
Alshboul and Streff (2015)	Literature review and analysis.	None (review of literature only)	Review of literature. Study reviews the National Institute of Standards and technology (NIST) framework for security in SMBs.	Proposed methodology is introduced and examined to provide an information security framework suited for SMBs. Among many information security frameworks are available, all frameworks have fatal flaws that leave SMBs unable to fully implement, leaving SMBs open to attacks. Study proposed a new framework that addresses the fatal flaws of existing frameworks for SMBs to use. Study recommends a melding together of the prescriptive and phased approach and recommended using the PDCA phased approach with the NISTIR 7621 prescriptive approach.
Balan et al. (2017)	Literature review and analysis. Data and statistical analysis	n = survey data sample of 35,596 businesses	Data statistical analysis using R programming.	The majority of businesses detected at least one incident involving a local area network (LAN) breach.
Berry and Berry (2018)	Literature review and analysis. Data and statistical analysis	n=370	Survey-Questionnaire	SMBs are likely to have the basic tools related to technology risk management in place, but lack the policies, procedures, and training to secure their information resources. Most respondents do not use strong passwords to protect their information assets.

Study	Methodology	Sample	Instruments/ Constructs	Findings/Contributions
Burns et al. (2006)	Literature review and analysis. Data and statistical analysis	n=470	Survey-Questionnaire	SMBs do not usually have a policy standard operating procedure, but many are using components that would normally form part of such policy within their staff employment manuals. This is a cheaper and less time consuming using more important and relevant components that make up such a policy.
Choi and Allison (2017)	Literature review and analysis.	None (review of literature only)	Review of literature	Due to the upward trend of cyberattacks and their economic effects, the need for all business firms to invest in their network security is obvious. Security threats are increasing, and cybercriminal tactics are continuously evolving. The digital arms race is taking place whether business owners participate. Contrary to the SME assumptions, cybercriminals are directly targeting their companies resulting in significant financial consequences for their inaction. As SMEs face increasing cyberthreats, and the need for securing their systems must be made a top business priority.
Dojkovski et al. (2007)	Literature review and analysis	n=12	Analysis of literature using Glaser-adapted inductive grounded approach.	Eisenhardt theoretical sampling strategy SME owners may benefit from adopting a risk-based approach to IS and should be educated about the strategic role of IT/IS.
Furnell et al. (2002)	Literature review and analysis.	None (review of literature only)	Review of literature Presentation of System/tool that enables users to pursue self-paced security training.	Study identifies the need for security awareness. Proposes a prototype implementation of a software tool that enables individuals to pursue self-paced security training.
Gundu and Flowerday (2013)	Literature review and analysis.	None (review of literature only)	Review of literature	Study presents an Information Security awareness process that seeks to cultivate positive security behaviour using a behavioral intention model based on the Theory of Reasoned Action, the Protection Motivation Theory and the Behaviorism Theory.

Study	Methodology	Sample	Instruments/ Constructs	Findings/Contributions
Gupta and Hammond (2005)	Literature review and analysis. Data and statistical analysis	n=138	Survey/questionnaire Regression analysis.	The small business owners may have procedures and policies in place, and may use technologies to counteract the security threat, but this research raised doubts about its effectiveness.
Hayes and Bodhani (2013)	Literature review and analysis.	None (review of literature only)	Review on literature	Small businesses need to upgrade Cybersecurity awareness and capabilities to avoid becoming vulnerable targets in the fight against hackers and cyberthreats
Kabanda et al. (2018)	Literature review and analysis. Data and qualitative study and analysis.	n=8	Data analysis utilizing NVIVO v.10	An SME's perception of cybersecurity is constrained by internal factors of budget, management support, and attitudes. SME cybersecurity practices are affected by the landscape of cybersecurity as well as institutional pressures.
Kisell et al. (2009; 2014)	Literature review and analysis. Data and statistical analysis	Government metadata	Statistical analysis on data.	SMBs represent 99.7% of all U.S. employers and are an important segment of the U.S. economy. SMBs totaling more than 28.2 million, create over 60% of all new U.S. private sector jobs and produce over 47% of the country's Gross National Product (GNP). SMBs are increasingly reliant on information technology as they store, process, and communicate information. Because information is one of the most valuable assets of an organization, protection of the information is critical.
Ključnikov et al. (2019)	Literature review and analysis.	None (review of literature only)	Review of literature	Security Controls and Supportive top management are the most important factors in general, while the factor of organizational awareness is the most obvious and important in the short-term period. SMEs should promote organizational awareness in Information Security management in line with implementation of the security controls at the first line of the defense.

Study	Methodology	Sample	Instruments/ Constructs	Findings/Contributions
Park et al. (2008)	Literature review and analysis	None (review of literature only)	Literature review and analysis	Security needs to be addressed at four levels: organizational level; workflow level; information level; and technical level. SMBs differ from large companies in many aspects, which explain why IT security is not that well addressed in SMBs, even though SMBs increasingly depend on their IT systems as much as larger businesses do. SMBs may be more often attacked in the future, as large businesses become increasingly difficult to hack.
Paulsen and Toth (2016)	Government Report	Government metadata	NIST Framework	Government report as a reference guideline about cybersecurity for small businesses. Report presents the fundamentals of a small business information security program in non-technical language.
Shivhare and Savaridassan (2015)	Literature review and analysis.	None (review of literature only)	Review of literature. System Analysis	OSSIM is a viable pen-source Security Information and Event Management (SIEM) solution and a free alternative to other commercial SIEM products, but since it is an open source, some features may not be present.

Cybersecurity Landscape in Developing Countries

From 2000 to 2008, Internet diffusion increased approximately 290% globally, and an estimated 1.46 billion people per year are on the Internet (Karake-Shalhoub et al., 2010). Developing countries in Africa and Asia account for the largest portion of this growth, with Asia and Africa growing 406% and 1,031% respectively (Karake-Shalhoub et al., 2010).

Cybercrime is a serious challenge not only for developing countries, but also for developed ones (Karake-Shalhoub et al., 2010). Cybersecurity and cybercrimes are activities of major concern to society and especially developing economies (Karake-Shalhoub et al., 2010).

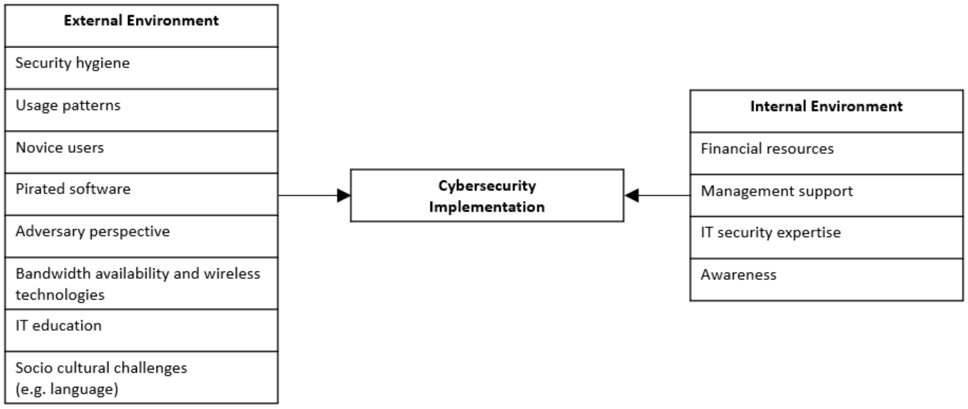
But there is also lack of research in the areas of information security in developing countries, and additional factors such as national and organizational culture, information security environment, and level of information security awareness, which relates to people's attitudes towards Information Security (Arage & Tesema, 2016; Kabanda et al., 2016).

Indeed, cyberspace is an intrinsic part of the development of any country, and resilient cyber capacity is crucial for countries to progress and develop in economic, political, and social sectors (Muller, 2015). One cybersecurity challenge in developing countries is that proper network, security, and legal frameworks are often deficient, and they have fewer capabilities to deal with these challenges than their developed counterparts (Muller, 2015). The aggregate result is that developing countries have increasing access to cyberspace, but often with insufficient security measures (Kabanda et al., 2018; Muller, 2015).

Ben-David et al. (2011) indicated five attributes of cybersecurity in developing countries: (1) poor security protocols, namely protocol and how up-to-date software patches and recent malware protections are run; for example, Abubakar et al. (2014) also found Nigerian IT practitioners to be less concerned with risks in security, privacy, and data loss; (2) usage patterns unique to developing economies, such as the use of mobile phone technology to run financial transactions from remote locations; (3) novice online users lacking knowledge of online risks, and limitations of cybersecurity education and tools; (4) wide use of pirated software which may pose as a security risk, but difficult to determine if software is not malicious; and (5) limited understanding on the adversary cybersecurity capability. Von Solms and Kritzinger (2011) also stated that developing countries are particularly vulnerable to multiple factors that include increased Internet penetration rates, widespread computer illiteracy, and ineffective legislation; this in turn, introduces higher cybersecurity risk to critical infrastructures in the region. Figure 4 was developed by Kabanda et al. (2018) to illustrate the common cybersecurity landscape in developing countries.

Figure 4

Factors Influencing Cybersecurity Implementation in Developing Countries



Kabanda et al.'s (2018) research on decisions influencing cybersecurity implementation by SMBs in developing countries identified five decision factors: budget; lack of management support; IT complexity and legacy systems; attitude toward security; and compliance to regulations. SMBs consistently cited small budgets as a constraint to having stronger SMB cybersecurity mechanisms in place (Kabanda et al., 2018). Tied to this is lack of management support mainly due to financial resources and other competing projects (Kabanda et al., 2018). One justification cited by SMBs for their lower posture toward cyberthreats is that they do not have complex legacy systems in place, are less vulnerable due to their smaller size, and therefore do not face the security threats compared to larger businesses (Kabanda et al., 2018).

SMBs in developing countries also indicated challenges in using and maintaining cybersecurity tools in their organization (Kabanda et al., 2018). A popular cybersecurity tool used by SMBs is web server logging, which is out of reach for some SMBs with limited resources (Kabanda et al., 2018). In the context of affordability, Kabanda et al. (2018) also stated that Intrusion Detection (ID) for SMBs in developing countries may be inadequate due to the time and money required to implement it. Further, SMBs expressed that open-source ID/IPS software that uses signature detection was available, but challenges among SMBs arose from perceived weakness in the method, and a preference for anomaly detection, which was perceived to be stronger but also more costly to acquire, implement, and maintain (Kabanda et al., 2018).

Cybersecurity deficiency has been recognized as a threat to SMBs in developing countries, and SMBs are encouraged to escalate their cybersecurity posture; but SMBs have also indicated that cybersecurity comes with its own real-world implementation challenges, which include budget constraints, management, and employee support, and commitment towards security concerns of the IT systems (Kabanda et al., 2018). Additionally, Muller's (2015) research on Cybersecurity Capacity Building (CCB) in developing countries found that a holistic model which encompasses all areas of society, such as judicial, social, economic, governmental, and educational, would be needed. Success in cybersecurity capability building will need to involve coordination and oversight in diverse areas beyond technological implementation.

Cybersecurity Landscape in Indonesia

Within similar context of developing countries, Indonesia is a developing country with about 140 million Internet users facing significant cybersecurity challenges and lacking a strong cybersecurity history (Rahayu, 2018; Setiyawan, 2019). Fahlevi et al. (2019) indicated law enforcement against cybercrime in Indonesia is still minimal, and Nugraha and Putri (2016) indicated that general understanding of cybersecurity in Indonesia remains low.

In 2009, Indonesia was one of the targets of the Stuxnet attack previously noted, and in 2016, the Indonesia Central Bank (BI) system was also a target of a large-scale cyberattack (Setiyawan, 2019). In 2018, there were more than 50 million cybersecurity threats in Indonesia, which represented a 240% increase compared to the previous year (Saputra et al., 2019). In 2019, Indonesia's Cyber and Cryptography Agency (Badan Siber dan Sandi Negara [BSSN]) reported 98.25 million cyberattacks, an almost twofold increase from the previous year (BSSN, 2019; BSSN, 2020). Saputra et al. (2019) further cited Indonesia as one of 20 countries with the highest rates of cyberattacks in the world. Saputra et al. (2019) also indicated that while the cybersecurity domain requires an increase in the role of the Indonesian Government through comprehensive policies, their efforts to adopt a comprehensive cybersecurity strategy have been slow and fragmented. Rahayu (2018) indicated that cybersecurity under the Indonesian Government has not been properly managed due to lack of interagency cooperation, lack of national cybersecurity strategy and governance, and infrastructure not yet integrated. Karake-Shalhoub et al. (2010) stated a major issue is cybersecurity in developing countries was outdated legal systems inadequate to deal with cybersecurity issues. Karake-Shalhoub et al. (2010) also indicated that for any country to move forward on the e-world map, it cannot be accomplished without a comprehensive, well-devised strategy at the highest government levels.

As Rahayu (2018) indicated, the 2015 Asia Pacific Cybersecurity Dashboard reported cybersecurity deficiencies in Indonesia which included:

1. Indonesia is still at the developmental stage of national cybersecurity strategy, with legality of cybersecurity framework still weak, with no legal regulation and policies on cybersecurity oversight. Although, operational cybersecurity entities, such as the Indonesia Incident Security Response Team on Internet Infrastructure Coordinating Center (IDSIRTII/CC) as the national CERT-ID (Computer Emergency Response Team) has been established, it is still in its infancy (Rahayu, 2018).

2. Indonesia does not have official public-private partnerships focusing on cybersecurity oversight. CERT-ID is the acting government cybersecurity liaison for the private sector, but there is no specific party handling cybersecurity. Additionally, Indonesia does not possess a joint cybersecurity plan between public and private sector (Rahayu, 2018).
3. Indonesia controls its domestic cybersecurity service providers with bureaucratic regulations requiring burdensome testing requirements and data flow restrictions (Rahayu, 2018).

Nugraha and Putri (2016) reiterated these points, indicating that Indonesia faces a multitude of ongoing cybersecurity challenges in establishing proper mechanism to coordinate across various ministries, agencies, and sub-national governments. This has resulted in Indonesian being vulnerable in cybersecurity. Although cyberattack cases indicate that Indonesia is moving toward appropriate response levels, reactive rather than proactive approach remain the norm (Nugraha & Putri, 2016). And despite the number of threats that have been recorded during the last three years, Indonesia has yet to update its cybersecurity management (Nugraha & Putri, 2016). Nugraha and Putri (2016) identified four cybersecurity stakeholders in Indonesia, and their key attributes, as illustrated in Table 4.

Kabanda et al. (2018) stated that SMB perception of cybersecurity in developing countries is constrained by internal factors of budget, management support, and attitudes, as well as the cybersecurity landscape and institutional pressures. Onwubiko and Lenaghan (2007) stated that a distinguishing factor in managing security for small businesses is budget: small businesses work on limited budgets for information security, compared to medium-sized enterprises. Osborn

(2015) indicated a lack of focus from the cybersecurity industry on what cybersecurity resources SMBs need within their budgets.

Table 4

Cybersecurity Stakeholders in Indonesia

No	Indonesia Stakeholder	Key Attributes
1.	Government	Mostly focused on national threats and the protection of critical national infrastructure. Coordinating Ministry of Politics, Law, and Security, and the Ministry of Communication and Technology (MCIT) are two ministries principally responsible for national cybersecurity policy and governance. Indonesian Armed Forces, National Intelligence Agency, Ministry of Foreign Affairs, and the National Encryption Agency are additional government stakeholders with respective cybersecurity focuses and missions.
2.	Private Sector	In technological development and cybersecurity governance, private sector more advanced than the government and civil society. More active in the discussion of cybersecurity policy and cybersecurity management. Main priority is protection of infrastructure and business development
3.	Civil Society & Academia	Civil society lagging – notably on privacy and personal data protection. Few communities actively involved in cybersecurity issues, with most are taking a human rights approach.
4.	Technical Communities	Indonesia has CERTs and critical security incident response teams (CSIRTs) organized by government and the private sector. Most frequent instances are ID-CERT and ID-SIRTII/CC due to their roles and history. ID-CERT is first computer emergency response team in Indonesia. ID-CERT is a community-based team for independent technical coordination.

Kimwele et al. (2017) stated that cybersecurity policies were not widely adopted by SMBs in developing countries. SMBs need to accomplish more to optimize their IT benefits without compromising their cybersecurity (Kimwele et al., 2017). Therefore, the range of cybersecurity challenges SMBs face in developing countries are not a drastic contrast to cybersecurity challenges SMBs in developed countries face.

Muller (2015) addressed the multiple challenges faced by developing countries in Cybersecurity Capacity Building (CCB). Developing countries need to deal with challenges in activities connected to CCB, although it is important to emphasize that all countries face different challenges in CCB implementing (Muller, 2015). Linking challenges to CCB in a country or region requires recognition of the specificities of a given context (i.e., cultural, political and social factors) (Muller, 2015).

This chapter provided an overview of the cybersecurity landscape in developing countries. Cybersecurity has become a serious challenge for both developing and developed countries, as users are increasingly connected to the Internet globally. A particular concern, however, is for developing countries mainly due to limitations in their cybersecurity resources (e.g., network security, policy, training) and lower computer user security awareness, which puts them at a higher cybersecurity risk. Cybersecurity deficiency is also a threat to SMBs in developing not just for these reasons, but also due to internal challenges from SMB management in budget constraints and resistance to allocate more resources to cybersecurity. The cybersecurity landscape in Indonesia is typical in challenges that many developing countries face. One of Indonesia's major challenges is the lack of clear cybersecurity policy, guidance, and implementation by the government. This is in part due to cybersecurity being relatively new to Indonesia, combined with the Indonesian Government's slow bureaucratic processes in legislation and implementation of laws. The studies discussed in this section are summarized in Table 5.

Table 5

Summary of Cybersecurity Landscape in Developing Countries Literature

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
Ben-David et al. (2011)	Literature review and analysis.	None (review of literature only)	Review of literature	The goal of computing security is to ensure users of computing systems can trust and rely upon those systems to accomplish their desired tasks. Failures in computing security present direct impacts, but they undermine the utility of a society's computing infrastructure. Increasing access to and reliance upon ICTs in developing regions promises significant development benefits. While the problems that poor computing security presents to these users may be merely inconveniences today, without the trust and reliability that are provided by strong computing security the promise of ICTs for development will not be fully realized. Issues such as shared computers, limited training and literacy, and piracy all require a combination of disciplines to achieve real improvements in security. The problems are only part technical; new research and technical leadership are required to drive policy, education, and the deployment of more secure systems.
Butler (2018)	Literature review and analysis. Data and statistical analysis	n=6	Interviews with subjects.	Study findings can be used to support older employees working longer than traditional retirement age, which might benefit society with increased economic productivity through decreased costs of retirement benefits, healthier living, and greater longevity.

Ciutiene and Railaite (2014)	Literature review and analysis	None (review of literature only)	Literature review and analysis	In the context of population aging, a person's better health and productive life assurance are becoming not only the individual's purpose, but also the organization's. Age management practices at an organizational level can not only help to keep more valuable employees, but also to overcome other aging workforce challenges. To avoid possible challenges in population aging, organizations should pay more attention to significant age-management areas such as job recruitment, learning and knowledge management, health management, flexible working conditions, workplace environment and ergonomics.
Dols (2009)	Literature review and analysis. Data and statistical analysis	n=653	Survey - Questionnaire	There are differences in attitude and behavior between nationality, gender, and age. The results did not establish clear links with poor Business – IT alignment or with reduced capacity or funding for IT projects and IT Governance.
Hughes et al. (2019)	Literature review and Analysis	None (review of literature only)	Review of literature.	Technology can sometimes provide better information, quicker so employees can make faster decisions; however, employees must ensure that the initial data inputted within the technology systems are accurate. Errors made with inaccurate data can sometimes lead to unrecoverable consequences, especially in the healthcare and airline industry. The continuous push and pull of the importance of people or technology in the workplace brings to fore many ethical concerns regarding the role and benefit of the uses of technology.
Study	Methodology	Sample	Instruments/ Constructs	Findings/Contributions
Karake-Shalhoub et al. (2010)	Literature review and analysis. Data and statistical analysis	n=44 (countries)	Multiple Regression Analysis	Literature on cyberspace use and adoption in developing countries is limited, although evidence exists describing the impediments, which include limited Internet accessibility; a lack of competition in international telephone traffic that makes access to the international network expensive; a lack of regional infrastructure; and a

				disproportionate penetration of the telephone in the urban as opposed to rural, more populated areas. For developing countries, the financial resources needed to invest in communication infrastructure are one of the major barriers since most countries rely on foreign aid. Physical infrastructural resources may be necessary for the creation of cybersecurity laws in developing and emerging economies, but they are not sufficient. Institutional environment is as important as physical infrastructure as a driver for the development and implementation of cybersecurity laws. These institutional environments facilitate the building of transactional integrity in online transactions.
Kessler et al. (2019)	Literature review and analysis. Data and statistical analysis	n = 252	Survey–Questionnaire Likert Scale SPSS Software	The Information Security Climate Index was related to better employee information security motivation and information security behaviors. There were observed differences between occupational groups with pharmacists reporting a more favorable climate and behaviors than physician assistants.
Kimwele et al. (2017)	Literature review and analysis. Data and statistical analysis	n=21	Survey-Questionnaire Likert Scale	IT security policies are not widely adopted, and the benefits harnessed by Kenyan SMEs. Much more needs to be done if SMEs are to realize the benefits of information technology without compromising their security status.

Study	Methodology	Sample	Instruments/ Constructs	Findings/Contributions
Li and Hoffman (2018)	Literature review and analysis. Data and statistical analysis	n = 285	Survey – Questionnaire Model based on Hu, West and Smarandescu (2015)	General Deterrence Theory does not provide an effective strategy for preventing security breaches.

Muller (2015)	Literature review and analysis. Data and statistical analysis This study: 1. Collected and assessed work conducted to date, and examines its feasibility and applicability. 2. Built on the analysis of this work and give an assessment of what can be built upon for successful implementation. 3. Mapped out general challenges facing CCB on the donor as well as the recipient end	n=35 (countries)	Data and statistical analysis using Oxford GSCSSs pilot model.	A holistic model is needed. The focus cannot be solely on one area, but must include all areas of society: the judicial, social, economic, governmental and educational sectors. Developing countries will need to deal with challenges in all types of activities connected to CCB – from human resource development, institutional reform, organizational adaptions, to the support provided to increase their access to, and ability to benefit fully from, the Internet and other elements of cyberspace. All countries face different challenges in implementing CCB. Mapping out the challenges to CCB in a country or a region requires the recognition of the specificities of a given context (i.e., cultural, political and social heritage) and needs to ensure local ownership.
Mutchler (2019)	Literature review and analysis. Data and statistical analysis.	n=211	Survey-Questionnaire	Even at low levels, response awareness has a strong influential effect on the behavioral intent to perform the secure response and on the self-efficacy to instruct others to perform the response. Instructional self-efficacy was also found to be a significant predictor of behavioral intent to perform the response. Instructional self-efficacy mediates the response awareness to the behavioral intent relationship.

Study	Methodology	Sample	Instruments/ Constructs	Findings/Contributions
Onwubiko and Lenaghan (2007)	Literature review and analysis.	None (review of literature only)	Analysis of literature. Security Conceptual Framework	The study framework aims to assist SMEs to prevent and effectively mitigate threats and vulnerabilities in assets. The framework models security issues in context of owner, vulnerabilities, threat agents, threats, countermeasures, risks and assets, and their relationship.

Study	Methodology	Sample	Instruments/ Constructs	Findings/Contributions
			Asset Classification Model Classification of Human-made fault	Asset classification is a value-based approach, and threat classification is based on attack timeline.
Ortman and Guarneri (2009)	Literature review and analysis. Data and statistical analysis.	Data was from 2009 National Population Projections.	Analysis of data.	The level of net international migration in the coming years will play an important role in shaping changes in the size, growth rate, age structure, and racial and ethnic composition of the U.S. population. International migration also plays a part in shaping the racial and ethnic diversity of the U.S. population over the next four decades.
Osborn (2015)	Literature review and analysis. Data and statistical analysis.	n=33	Survey-Questionnaire	Refined understanding of the barriers faced by SMEs can influence development of future SME security solutions.
Pahnila et al. (2007)	Literature review and analysis. Data and statistical analysis. Theoretical model combines General Deterrence Theory, Protection Motivation Theory, the Theory of Reasoned Action, Information Systems Success, and Triandis' Behavioral Framework and Rewards.	n=245	Survey-Questionnaire	Information quality has a significant effect on actual IS security policy compliance. Employee attitude, normative beliefs and habits have significant effect on intention to comply with IS security policy. Threat appraisal and facilitating conditions have significant impact on attitude towards complying, while coping appraisal does not have a significant effect on employee attitude towards complying. Sanctions have insignificant effect on intention to comply with IS security policy and rewards do not have a significant effect on actual compliance with IS security policy.
Pattinson et al. (2019)	Literature review and analysis. Data and statistical analysis.	n=1,048	Survey-Questionnaire	The extent to which the training that an individual received matched their learning preferences is positively associated with their Information Security Awareness (ISA) level However, the frequency of such training did not directly predict ISA levels.

Rahayu (2018)	Literature review and analysis.	None (review of literature only)	Literature analysis	BSSN (the Indonesian Cybersecurity Agency) has strengths in regulation, management, and technical fields as the organizer and provider of a national cybersecurity, as well as strategic function to be the coordinator in realizing synergy among parties who have interests in national, regional and international cybersecurity system. BSSN can be relied upon to become the leading sector of national cybersecurity development in Indonesia.
Soja and Soja (2020)	Literature review and analysis	None (review of literature only)	Review of literature Technology Acceptance Model (TAM)	The most important issues related with ES acceptance perceived from the older workers viewpoint are perceived compatibility/ Fit; attitude toward ES; communication and training computer self-efficacy; perceived benefits of ES readiness for change; and computer anxiety.
Strand (2018)	Literature review and analysis. Data and statistical analysis.	n=2,000 (Data was from an Information Security awareness campaign administered in a company of 2,000 knowledge workers	Semi-structured Interviews (6 from each group) Survey-Questionnaire (web-based)	It is important that employees understand the security risks of the company, understand their individual role in the security picture, and that they comply with company policies. One way to raise the awareness level of employees is to implement Information Security awareness campaigns/programs. People have different opinions on the effectiveness of such campaigns, but not many studies have been done with regard to measuring the effect. Also, many kinds of people work in an organization, having different attitudes and approaches to Information Security and its campaigns.
Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
Von Solms and Kritzinger (2011)	Literature review and analysis.	None (review of literature only)	Review of literature	Study reviewed negative views about Critical Information Infrastructure Protection (CIIP) and Cybersecurity in Africa. The study addressed the expressed negative views that Africa can become the vehicle or platform from where cyberattacks could be launched against the rest of the world.

				The study evaluated the reasons for such negative views and suggests steps which should be taken in Africa to counter negative impressions and to protect its cybersecurity.
Wallen and Mulloy (2006)	Literature review and analysis. Data and statistical analysis.	n=350	Survey-questionnaire Three versions of computer-based respiratory safety training was shown to older and younger workers, who then took a high and a low-level learning test.	Younger workers did better overall. Both older and younger workers did best with the version containing text with pictures and audio narration.
Zukowski and Brown (2007)	Literature review and analysis. Data and statistical analysis.	n = 199	Survey-Questionnaire	Demographic factors, such as age, education and income level influence Internet user concerns for information privacy. Other factors such as gender and Internet experience were found to have no influence.

Older Workers

The labor force across regions which includes the United States, Europe, and Japan, is aging, and by 2060, the size of the labor force in these regions is expected to decline, and the age composition within the workforce will shift with the youngest age group (16 to 24 years old) projected to decrease, while the older age group (55 years old and above) expected to grow (Hughes et al., 2019). Hughes et al. (2019) reported that the 55 and above age group will continue to occupy a significant portion of the workforce and continue to work beyond the traditional age of retirement.

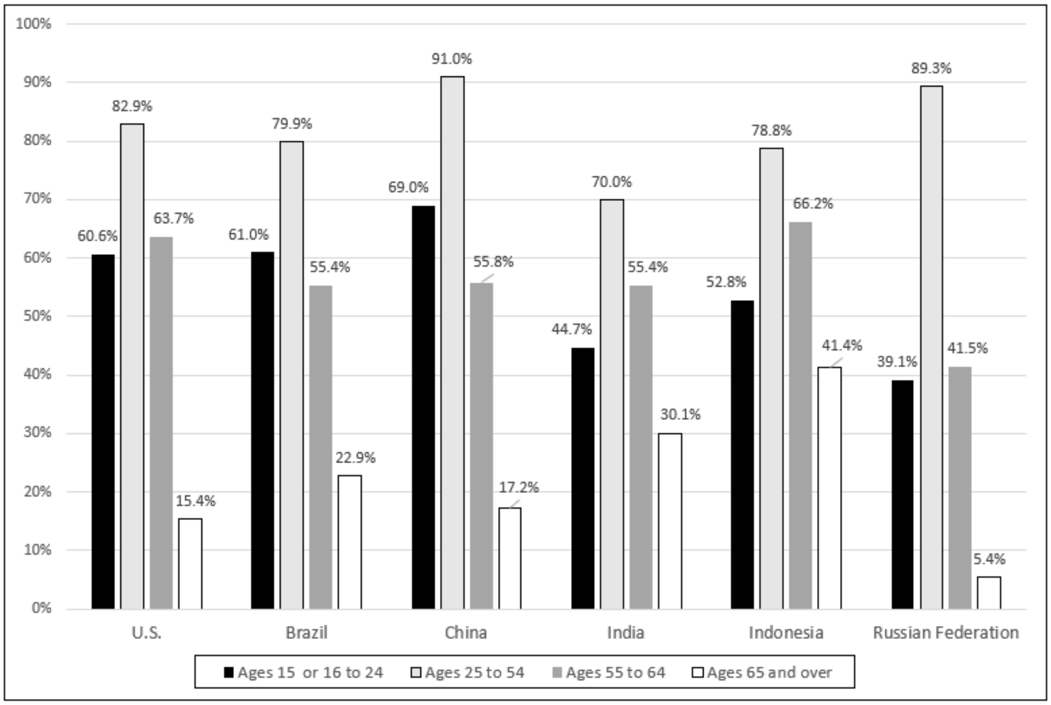
Older adults are the fastest growing demographic in the U.S. with the labor force population of individuals aged 55 and older projected to increase from 22.4% to 24.8% by 2026

(Ortman & Guarneri, 2009; Wallen & Mulloy, 2006). The U.S. Bureau of Labor Statistics (BLS) projected that by 2012 the number of workers aged 55 years and older would increase by 49%, while workers aged 25 to 54 years would only increase by 5% (BLS, 2004). Similarly, the European Commission forecasted a participation rate of older people (55–64) by 15% between 2013 and 2060 — signaling that the future labor force would not only shrink, but also gradually age (Soja & Soja, 2020).

Indonesia is similar in geographic scope to the U.S. and its growing elder population, but at a less advanced level of socioeconomic development (McKee, 2006). The age of retirement in Indonesia is 55 for civilians and 50 for military members. They may subsequently qualify for a selection of retirement plans (McKee, 2006). McKee (2006) found a significant number of Indonesians still working at older ages; for example, 60% of men in rural areas and 30% of men in urban areas at age 75 are still in the labor force. Samorodov (1999) indicated that most elder people in Indonesia are uneducated with no formal education, and their employment is mainly in the agricultural sector. In the Chartbook of International Labor Comparisons, the U.S. Department of Labor (2008) indicated similar comparison between the U.S. and Indonesia in their number of older workers in the 55 to 64 age group. However, at the 65 and above age group category, about 30% of older Indonesians continue to work, while only 15% older Americans still work (BLS, 2008), inferring that most Americans have retired by 65.

Figure 5

2006 Labor Force Participation Rates by Age



The value of the older workers in organizations is also well-documented. Older workers can provide valuable talent and knowledge to organizations and often possess greater experience, knowledge, skills, maturity, professionalism, work ethic, quality awareness, and lower rates of turnover than younger workers (Ciutiene & Railaite, 2014; Hughes et al., 2019). Older workers also have great capacity for teamwork, leadership, and high social competence in soft skills (Hughes et al., 2019). Studies have been conducted on older workers IS practices, awareness, and compliance in their work environment, with multiple studies indicating older workers having higher compliance with IS policies of their organizations (Dols, 2009; Kessler et al., 2019; Li & Hoffman, 2018; Mutchler, 2019; Pahnila et al., 2007; Pattinson et al., 2019; Strand, 2018; Zukowski & Brown, 2007).

Pahnila et al. (2007) found that among workers with knowledge of their organization's security policies, older workers were more likely to be compliant. Pattinson et al. (2019) indicated that both older workers and female workers tended to have better IS awareness, and that age and gender were stronger predictors of IS awareness than training. Li and Hoffman (2018) found age as a significant factor for IS compliance, and that older workers were more likely to comply with IS policies of the organization.

Kessler et al. (2019) stated that IS risk practices among healthcare workers found that older workers were significantly less likely to engage in high-risk IS behaviors. They also found that older workers were more careful than their younger counterparts in the handling of confidential data, which was attributed to older workers generally being more conscientious and careful with patient data (Kessler et al., 2019). Dols (2009) found in IT security policy practices in organizations that older workers demonstrated more compliance and familiarity with information security policies, compared to younger counterparts.

Cummings et al. (2012) found in IS breaches in organizations that in one-third of cases involving theft of personally identifiable information by insiders or external actors, younger workers were more often the perpetrators, compared to their older counterparts. Mutchler's (2019) found that in IS security, older workers were less likely to misuse IS resources; less likely to engage in risky IS behaviors; and more likely to possess higher levels of IS awareness. Strand (2018) found in an IS awareness campaign in an organization of 2,000 workers that older workers expressed more interest than younger workers, and that older workers learned the most from the campaign and from their co-workers, due to lower degree of independent judgment of technology, and low perceived efficacy.

This chapter provided an overview of the current situation with older workers. The population of older workers (categorized as those 55 and older) in the labor force are projected to increase and occupy a significant portion of the workforce. Older workers are also projected to work beyond their expected retirement age. Older workers are the fastest growing workforce demographic in the U.S. with their population projected at 25% in 2026, and in Europe, the older worker population are projected to increase by 15% between 2013 and 2060. Older workers contribute significantly to organizations in professionalism, talent, knowledge, and work ethic. Studies also indicate that older workers are more likely to be compliant with organization security policy and engage less in risk information systems behaviour, such as committing security breaches, and engaging in risky IS behaviour. The studies discussed in this section are summarized in Table 6.

Table 6

Summary of Older Workers Literature

Study	Methodology	Sample	Instruments Constructs	Findings/Contributions
Ciutiene and Railaite (2015)	Literature review and analysis.	None	Key age management areas matrix Workplace flexibility matrix. Ergonomic Control Measures matrix.	To ensure the productivity of aging workers, organizations should implement appropriate measures of human resource management and dedicate more attention to their needs. When employees are satisfied with their working environment, they are motivated to hold their positions for a longer period of time (Ciutiene & Railaite, 2015). To avoid potential challenges in population aging, organizations should dedicate more resources to age-management areas such as job recruitment, learning and knowledge management, health management, flexible working conditions, workplace environment and Ergonomics (Ciutiene & Railaite, 2015).

Study	Methodology	Sample	Instruments Constructs	Findings/Contributions
Cummings et al. (2015)	Literature review and analysis. Case study and analysis. Data and statistical analysis.	n=80 Technical and behavioral pattern analysis from 67 insider fraud cases, and 13 external fraud cases between 2005 and 2012.	Data modeling and analysis.	Criminals who executed a "low and slow" approach accomplished more damage and escaped detection for longer. Insiders' means were not very technically sophisticated. Fraud by managers differs substantially from fraud by non-managers by damage and duration. Most cases do not involve collusion Most incidents were detected through an audit, customer complaint, or coworker suspicion. Personally identifiable information (PII) is a prominent target of those committing fraud.
Dols (2009)	Literature review and analysis. Data and statistical analysis	n=653	Survey - Questionnaire	There are differences in attitude and behavior between nationality, gender, and age. The results did not establish clear links with poor Business – IT alignment or with reduced capacity or funding for IT projects and IT Governance.
Hughes et al. (2019)	Literature review, data and statistical analysis.	None	Review of literature.	Middle-skill, low-skill, and disadvantaged adult workers present a significant challenge to the working community. They make up a large proportion of the worldwide workforce, but there is evidence about how to address their training and development needs (Hughes et al., 2019).
Kessler et al. (2019)	Literature review and analysis. Data and statistical analysis	n = 252	Survey–Questionnaire Likert Scale SPSS Software	The Information Security Climate Index was related to better employee information security motivation and information security behaviors. There were observed differences between occupational groups with pharmacists reporting a more favorable climate and behaviors than physician assistants.

Study	Methodology	Sample	Instruments Constructs	Findings/Contributions
Li and Hoffman (2018)	Literature review and analysis. Data and statistical analysis	n = 285	Survey – Questionnaire Model based on Hu, West and Smarandescu (2015)	General Deterrence Theory does not provide an effective strategy for preventing security breaches.
Mutchler (2019)	Literature review and analysis. Data and statistical analysis.	n=211	Survey-Questionnaire	Even at low levels, response awareness has a strong influential effect on the behavioral intent to perform the secure response and on the self-efficacy to instruct others to perform the response. Instructional self-efficacy was also found to be a significant predictor of behavioral intent to perform the response. Instructional self-efficacy mediates the response awareness to the behavioral intent relationship.
Ortman and Guarneri (2009)	Data and statistical analysis.	U.S. Census Bureau 2008, 2009 data.	Data and statistical analysis of current and historical data.	Over the next four decades the U.S. is projected to experience rapid growth in its older population, accompanied by a significant increase in racial and ethnic diversity. These changes will be partly shaped by international migration.
Pahnila et al. (2007)	Literature review and analysis. Data and statistical analysis. Theoretical model combines General Deterrence Theory, Protection Motivation Theory, the Theory of Reasoned Action, Information Systems Success.	n=245	Survey-Questionnaire	Information quality has a significant effect on actual IS security policy compliance. Employee attitude, normative beliefs and habits have significant effect on intention to comply with IS security policy. Threat appraisal and facilitating conditions have significant impact on attitude towards complying, while coping appraisal does not have a significant effect on employee attitude towards complying. Sanctions have insignificant effect on intention to comply with IS security policy and rewards do not have a significant effect on actual compliance with IS security policy.

Study	Methodology	Sample	Instruments Constructs	Findings/Contributions
Pattinson et al. (2019)	Literature review and analysis. Data and statistical analysis.	n=1,048	Survey-Questionnaire	The extent to which the training that an individual received matched their learning preferences is positively associated with their Information Security Awareness (ISA) level. However, the frequency of such training did not directly predict ISA levels.
Soja and Soja (2020)	Literature review and data analysis.	n = 187	Study examined how employees at various age perceive barriers during enterprise system (ES) adoption and use.	Emphasis on employees' perception of mandatory ICT implementation projects is shifting from technology to human factor considerations. Job security and workload appear most important to older workers on such projects. Multi age collaboration appears necessary to address the problems posed by technology and demographic changes (Soja & Soja, 2020).
Strand (2018)	Literature review and analysis. Data and statistical analysis.	n=2,000 (Data was from an Information Security awareness campaign administered in a company of 2,000 knowledge workers	Semi-structured Interviews (6 from each group) Survey-Questionnaire (web-based)	It is important that employees understand the security risks of the company, understand their individual role in the security picture, and that they comply with company policies. One way to raise the awareness level of employees is to implement Information Security awareness campaigns/programs. People have different opinions on the effectiveness of such campaigns, but not many studies have been done about measuring the effect. Also, many kinds of people work in an organization, having different attitudes and approaches to Information Security and its campaigns.
Wallen and Mulloy (2006)	Literature review and data analysis.	n = 50	Computer-based respiratory safety training was shown to older and younger workers who then took a high and a low-level learning test.	Younger workers performed better overall, in computer-based training than their younger coworkers. Both older and younger workers did best with the training version containing text with pictures and audio narration.

Study	Methodology	Sample	Instruments Constructs	Findings/Contributions
Zukowski and Brown (2007)	Literature review and analysis. Data and statistical analysis.	n = 199	Survey-Questionnaire	Demographic factors, such as age, education, and income level influence Internet user concerns for information privacy. Other factors such as gender and Internet experience were found to have no influence.

Deterrence Theory in IS

Studies have proposed that organizations adopt deterrence philosophy to mitigate IS misuse (D'Arcy & Hovav, 2005). Deterrence theory can be defined as the application of security countermeasures to deter IS misuse in organizations (D'Arcy & Hovav, 2005; Gibbs, 1968; Straub, 1990). Deterrence theory is one of the most widely applied theories in IS research, particularly in behavioral IS studies (D'Arcy & Herath, 2011).

Deterrence theory in IS misuse evolved from a classical deterrence model in criminology where informal sanctions (e.g., public embarrassment, social disapproval) and formal legal sanctions (e.g., criminal punishment, employment probation and termination) could serve as deterrents to criminal acts; but deterrence theory is now considered a prominent perspective in IS misuse (D'Arcy & Herath, 2011; Gibbs, 1968). Deterrence is practiced in organizations through security countermeasure programs (D'Arcy & Hovav, 2005). D'Arcy et al. (2009) indicated that security countermeasures can be an effective preventative measure to deter security threats.

Research has examined the impact of deterrence theory through IS misuse countermeasures, which in several cases resulted in lower workplace incidents of IS misuse, improved IS security effectiveness, and lower illegal software use (D'Arcy & Hovav, 2005). D'Arcy and Hovav (2005) used deterrence theory to examine whether organizational use of security policies, security awareness, and computer monitoring, increased employee perceived risk of sanctions from IS misuse, and discouraged intentions of IS misuse. D’Arcy and Hovav (2005) surveyed 33 subjects with a questionnaire on their self-reported intentions of IS misuse; the result of this study suggested that some IS countermeasures, such as perceived sanction risk and security awareness programs, may deter certain IS misuse behaviors.

D’Arcy et al. (2009) also suggested that perceived severity of sanctions is more effective in reducing IS misuse than certainty of sanctions, and that impact sanction perceptions are relative to the worker’s level of morality. In addition to individual level of morality, Dhillon et al. (2020) defined the role of psychological empowerment as a mediator between structural empowerment and a worker’s intention to comply with information security policy. Dhillon et al. (2020) suggested that empowerment group work structures which included worker information security training and participation in information security decision-making, can boost psychological empowerment of the worker and encourage IS policy compliance.

Saffa and Von Solms (2016) recommended knowledge sharing in IS due to its positive impact on employee IS awareness and proposed the IS Knowledge Sharing (ISKS) model to form and decrease the risk of IS incidents. The findings categorized job reputation and promotion as an extrinsic motivation, and curiosity satisfaction as an intrinsic motivation, and both aspects had positive effects on worker attitude towards ISKS (Saffa & Von Solms, 2016). Additional findings indicated that attitude, perceived behavioral control, and subjective norms had positive effects on ISKS intention, which in turn impacted ISKS behavior, and organizational support influenced worker ISKS behavior more than trust (Saffa & Von Solms, 2016).

Despite the popular theoretical argument for security countermeasures as a deterrent to IS misuse, effectiveness of this method has remained inconclusive (D’Arcy & Hovav, 2005).

D’Arcy and Hovav (2005) attributed this to the body of research still lacking accurate measurement of individual perceptions of punishment certainty and severity, as well as reliance of the research on aggregate misuse data, which makes it difficult to trace impact of security countermeasures to individual IS misuses. They also attributed this lack of conclusiveness in security countermeasures as a deterrent to IS misuse to a paucity in research that explored relationships between formal and informal sanctions in IS misuse deterrence (D’Arcy & Hovav, 2005).

Additionally, D’Arcy and Hovav (2009) examined whether individual characteristics or work arrangement among workers moderated the influence of deterrence mechanisms on IS misuse. The results indicated that workers with higher computer proficiency were less deterred by IS training awareness and computer monitoring, while workers who teleworked were less influenced by the deterrence mechanisms (D’Arcy & Hovav, 2009).

Wiley et al. (2020) also studied the relationship between security culture and IS awareness in organizations by exploring the relationship between IS awareness, organizational culture, and security culture. Wiley et al. (2020) administered an online survey to 508 Australian workers and collected their demographic and self-reported responses to the survey. The findings suggested that security culture played an important mediating relationship between organizational culture and information security awareness (Wiley et al., 2020). Wiley et al. (2020) recommended for organizations to focus on security culture rather than organizational culture to improve information security awareness and conserve organization resources.

Other case studies have also not succeeded in demonstrating the effectiveness of deterrence of IS misuse in organizations. D’Arcy and Hovav (2005) cited multiple case studies where deterrent-based security countermeasures were enforced in organizations but failed to accomplish the desired outcome. They concluded that while some studies suggested correlation between security countermeasure use and lower information system misuse, other studies indicated little to no benefit of the countermeasures (D'Arcy & Hovav, 2005). Abed and Weistroffer (2016) also found that deterrence constructs were not necessarily strong predictors of compliance behavior, but that sanctions influenced compliance.

D'Arcy and Devaraj (2012) indicated that although research provided evidence of deterrent effectiveness through formal sanctioning, unexplained variance in many of the studies showed that deterrence theory alone did not provide a complete understanding of IS misuse. For example, D'Arcy and Hovav (2005) pointed to additional factors beyond perceived sanction risk that influenced IS misuse behavior; the outcome of their study accounted for only 10 % of intention variance for sending inappropriate e-mails and unauthorized data manipulation, compared to 26% of intention variance for software piracy. They recommended that organizations focus on increasing perceived risk of punishment for software piracy (D'Arcy & Hovav, 2005). Another finding of study was the impact of IS awareness education and training in deterring IS misuse: while researchers and practitioners credited the benefits of IS training awareness programs, actual supporting evidence was sparse (D'Arcy & Hovav, 2005).

D'Arcy and Green (2014) studied the influence of security-related and employment relationship factors on worker IS compliance, which found that an organization's security culture was a strong driver for worker IS compliance. D'Arcy and Green (2014) further indicated that worker job satisfaction was influenced by their desire to comply with security standards, which could be influenced by the worker's status, position, and tenure in the organization. To these points, D'Arcy and Devaraj (2012) recommended for deterrence theory in IS to be augmented with individual and situational variables specific to the organization. D'Arcy and Hovav (2004) also attempted to reconcile divergent findings in deterrence theory by developing a proposition framework which included deterrent security countermeasures, sanction perceptions, individual characteristics, and IS misuse. The propositions were: (1) deterrent security countermeasures increase perceived certainty and severity of sanctions leads to lower IS misuse intention; (2) relationship between deterrent countermeasures and perceived certainty and severity of sanctions is moderated by an individual's computer self-efficacy, computer experience, gender, age, risk propensity, and employment context (D'Arcy & Hovav, 2004). D'Arcy and Hovav (2004) argued that the effect of deterrent security countermeasures was mediated by perceptions of the certainty and severity of sanctions from IS misuse by the individual. However, one basis for D'Arcy and Hovav's (2004) research was survey questions of subjects which asked them their future misuse intentions. This was a flaw which invalidated their research.

In another effort to reconcile the variability in outcomes on deterrence theory, D'Arcy and Herath (2011) conducted a multi-disciplinary literature review, which discovered equivocality throughout much of the deterrence literature, and identified methodological issues on measurement and treatment of deterrence constructs within the IS deterrence studies. One key issue they identified in this analysis was that the IS deterrence research was focused on only one aspect of the rational decision process, namely perceived costs, while it overlooked competing influence of perceived benefits (D'Arcy & Herath, 2011). Similarly, Cram et al. (2019) also addressed the competing theoretical perspectives and inconsistencies with reported findings in information security compliance; they conducted a meta-analysis of literature, reviewing 95 empirical papers and classifying 401 independent variables into 17 distinct categories and analyzed their relationship with information security compliance. The results of their study suggested that much of information security compliance literature suffered from sub-optimal theoretical framing (Cram et al., 2019).

There have also been concurrent efforts within the industry to mitigate cybersecurity threat through other methods such as risk analysis, policymaking, and training. Agrawal (2017) stated that risk analysis is an integral part of good management practice and corporate governance, but there are many risk analysis methods, and it is a tedious task for organizations, particularly SMBs, to choose a proper method. Organizations have also implemented cybersecurity education programs as part of their cybersecurity strategy (Bada & Nurse, 2019). Large organizations struggle to educate and train their workforces, and SMBs face the same issues but with less resources (Bada & Nurse, 2019).

This chapter provided an overview of deterrence theory in IS. Research has proposed for organizations to adopt principles of deterrence and implement security countermeasures to mitigate IS misuse. Deterrence in IS originated from classical deterrence theory in criminology, where punishment to acts of wrongdoing can serve as a deterrent to those acts. Research found that the application of IS misuse countermeasures have resulted in lower incidents of US misuse, improved IS security effectiveness, and illegal software use in the workplace. These positive outcomes provide justification for the increase in security countermeasure resources. Other research on the correlation of increase in information security enforcement and decreased in IS misuse in the workplace found deterrence to be inconclusive. To escalate their efforts, organizations have implemented multi-pronged approaches which combine cybersecurity risk analysis, policymaking, employee training, and system security upgrades. The studies discussed in this section are summarized in Table 7.

Table 7

Summary of Deterrence Theory in IS Literature

Study	Methodology	Sample	Instruments/ Constructs	Findings/Contributions
Abed and Weistroffer, (2016)	Literature review and analysis. Data and statistical analysis.	None (review of literature only)	Analysis on data using quantitative meta-analysis.	Deterrence theory has no significant impact on employee compliance behavior.
Agrawal (2017)	Literature review and analysis. Data and statistical analysis.	None (review of literature only)	Qualitative and qualitative analysis using IS risk analysis with Campbell et al. classification scheme.	Based on analysis and comparison of four Information Security risk analysis methods, the analysis scheme of Campbell can better help organizations, risk experts to find major attributes related to each method.
Almeida et al. (2018)	Literature review and analysis. Data and statistical analysis.	n=144	Survey-questionnaire	The top three most important elements in the structure of a security policy are: asset management; security risk management; and definition of the scope of the policy. The three least relevant elements include the executive summary, contacts and manual inspection. The importance given to each element of the security policy is changed according to the sectors of activity. The elements that show the greatest variability are the review process, executive summary, and penalties. On the other hand, the purpose of the policy and the asset management present a stable importance for all sectors of activity.
Bada and Nurse (2019)	Literature review and analysis.	None (review of literature only)	Review of literature. Theoretical analysis. Case study analysis.	Literature can be informative at guiding education and awareness programs, but it may not always reach real-world programs.

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
Brisola and Curry (2016)	Literature review and analysis.	None (review of literature only)	Review of literature	Heuristic Inquiry is a unique method in which the lived experience of the researcher becomes the main focus of the study, and it is used as an instrument in the process of understanding a given phenomenon. Heuristic Inquiry recognizes the importance of intuition and tacit knowledge as elements that enable comprehending a phenomenon and its meanings
Cram et al. (2019)	Literature review and analysis.	None (review of literature only)	Review of literature Meta-analysis	Security policy compliance literature can be influenced by substandard theoretical framing.
D'Arcy and Herath (2011)	Literature review and analysis.	None (review of literature only)	Literature Review Analysis on contingency variables and methodology and theories presented.	Identified that findings of studies on efficacy of Information Security deterrence are mixed and inconclusive.
D'Arcy and Hovav (2004)	Literature review and analysis.	None (review of literature only)	Review of literature Model linking deterrent security countermeasures to Information Security misuse intention	General Deterrence Theory (GDT) is mediated by perceptions of certainty and severity of sanctions for committing Information Systems misuse.
D'Arcy and Hovav (2005)	Literature review and analysis. Data and statistical analysis.	n=56	Survey-Questionnaire Scenario-based instrument.	Security countermeasures are effective in deterring certain Information Systems misuse behaviors, with security awareness program being particularly effective.

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
D’Arcy et al. (2009)	Literature review and analysis. Data and statistical analysis.	n=238	Survey-Questionnaire Partial Least Square (PLS) Analysis	User-awareness of security policies, SETA programs, and computer monitoring have some deterrent effect on IS misuse intention and is achieved indirectly through perceived certainty and severity of sanctions.
D'Arcy and Devaraj (2012)	Literature review and analysis. Data and statistical analysis.	n=183	Survey-Questionnaire	Predisposition toward the need for social approval and moral beliefs regarding the behavior are key determinants of technology misuse.
D'Arcy and Greene (2014)	Literature review and analysis. Data and statistical analysis.	n=127	Survey-Questionnaire PLS Structural Model	Security culture is a driver of employee security compliance in the workplace. Employee job satisfaction influences their security compliance intentions, although this relationship appears to be contingent on the employee’s position, tenure, and industry.
Dhillon et al. (2020)	Literature review and analysis. Data and statistical analysis.	n = 290	Survey-Questionnaire Mediation Test. Chi-Square Test.	Empowerment work structures, which include information security education, training, and awareness (SETA), access to information security strategic goals, and participation in Information Security decision-making all increase employee feelings of being psychologically empowered, which leads to positive intentions to comply with information security policy.
Djuraskovic and Arthur (2010)	Literature review and analysis. Heuristic Method	n=6	Interviews	Heuristic methodology represents a disciplined pursuit of the experience of the phenomenon and cab require significant commitment research, coresearchers, and personal exploration of the experience of acculturation and ethnic identity reconstruction. Heuristic methodology can be a demanding method and process.

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
Fahlevi et al. (2019)	Literature review and analysis. Qualitative research	n=4	Interviews	Digital business growth in Indonesia is mainly in e-commerce. The total loss caused by e-commerce crime each year reaches IDR Rp. 1.5 trillion. Enforcement of cybersecurity laws against criminals is still minimal Existing cybersecurity laws and regulations in Indonesia are still problematic.
Gibbs (1968)	Literature review and analysis. Data and statistical analysis. Review of FBI Crime Data	None (review of literature only).	Statistical Analysis. Chi Square Analysis.	The study challenges the common notion that no evidence exists of a relationship to crime and rate. The study caveats the notion that harsher sentences reduce criminal homicide rates, i.e., the efficacy of deterrence.
Kenny (2012)	Literature review and analysis. Heuristic method	None (review of literature only)	Review of literature	Nursing practice and research are ideally placed to engage with questions that emerge heuristically from the on-the-job experience.
Nugraha and Putri (2016)	Literature review and analysis.	None (review of literature only)	Review of literature	The study identifies three key gaps: different understandings and approaches towards cybersecurity; human resources capacity; and coordination Without secure and reliable access to the internet, customers will be reluctant to provide confidential information online. The business sector in Indonesia is leading the push for faster developments in cybersecurity, more so than the government. The Indonesian government has started considering cybersecurity mitigation tactics, including encouraging internet companies to store citizens' personal data on data centers within local jurisdictions.

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
Safa and Von Solms (2015)	Literature review and analysis. Data and statistical analysis.	n=482	Survey-Questionnaire Confirmatory Factor Analysis (CFA)	Information Systems Knowledge Sharing (ISKS) is beneficial to organizations. Organizations should consequently establish environments to cultivate this culture.
Saputra et al. (2019)	Literature review	None (review of literature only)	Review of literature	The Indonesian Government needs to increase its cybersecurity awareness in the face of cybersecurity threats. Indonesia needs to develop policies and strategies in the cybersecurity domain. This policy can be based on international best practices and international mechanisms. The Indonesian Government security strategy also requires collaboration with the private sector, which has large resources to take an active role in building the national cybersecurity architecture. The Indonesia Government needs to be more proactive in international cybersecurity cooperation.
Setiyawan (2019)	Literature review and analysis.	None (review of literature only)	Review of literature	Strengthening policies in the form of laws are needed to clarify, reinforce cybersecurity domains as part of Indonesia's sovereignty domain and provide a legal basis that can reach complex, dynamic and multidomain levels of cybersecurity threats. Indonesian cyber laws must be able to collaborate on authority, strength and all relevant stakeholders considering the handling of the nature of cyber threats that are complex, dynamic and multidomain towards security, defense, and national interests of Indonesia. The Indonesian government must harmonize the laws and regulations related to defense, security, and national interests, such as provisions concerning the country's infrastructure / vital objects.

Study	Methodology	Sample	Instruments/Constructs	Findings/Contributions
Straub (1990)	Literature review and analysis. Data and statistical analysis.	n=37	Survey-Questionnaire Multitrait/Multimethod (MTMM) Analysis	Security countermeasures that include deterrent administrative procedures and preventive security software can result in lower computer abuse
Wiley et al. (2020)	Literature review and analysis. Data and statistical analysis.	n=508	Survey-Questionnaire Mediation Analysis.	Security culture can mediate the relationship between organizational culture and Information Security awareness.

Summary of What is Known and Unknown

This chapter provides an overview of knowledge hiding in the context of cybersecurity, current and emerging threats in the field of cybersecurity, and cybersecurity practices in SMBs in developed and developing countries — with an emphasis on Indonesia. The overview includes current state, progress, issues, and challenges that these entities face in knowledge sharing, knowledge hiding, and cybersecurity. This chapter also provides an overview on older workers with an emphasis on their role and function in the technology and IT sector. The overview also includes the current state, progress, issues, and challenges those older workers face in this environment and industry sector. The remainder of this chapter is a review on the theories and methodologies proposed for this study. Deterrence theory, which includes its history, applicability, and efficacy in cybersecurity, specifically for the SMB environment, is also reviewed.

Much in the field of knowledge sharing within the context of cybersecurity remains unexplored. The field of cybersecurity is rapidly evolving, with new cyberattacks methods discovered daily, and cybersecurity innovations being developed at a rapid pace. This research cannot cover the full scope of cybersecurity; rather, it will focus on key points and issues in current cybersecurity. Literature review on cybersecurity practices in developing countries is also still limited; there is not yet the accrual of substantive body of knowledge in cybersecurity in developing countries, particularly in Indonesia. There is considerable literature on aging workers in the workforce and in IT; but there is limited literature on aging workers in the IT sector in developing countries. As in the case of many developing countries, government cybersecurity laws and regulations are still in infancy and there remains significant delays between government legislation and enforcement of most aspects of the cybersecurity laws. The effectiveness of government cybersecurity enforcement on SMBs in Indonesia is still unknown, as is how vigilant Indonesian SMBs and their employees are in the cybersecurity practices.

Deterrence theory is proposed for this study in part because of its role in mitigating criminal behavior, specifically cybercrime. Organizations have attributed lower IS misuse to security countermeasures based on deterrence principles. At the same time, literature indicated that while punishment to IS violations in organizations was designed for deterrence, measurable benefits have remained inconclusive and attributable to variable factors. Furthermore, despite the significant resources that governments, law enforcement, private companies, and other stakeholders commit to cybersecurity, cybercrime has continued to escalate alarmingly.

Summary

The review of literature highlighted relevant topics and research studies that support the research problem and proposed research goal and questions. Cybercrime is an ongoing threat which indiscriminately targets organizations of all types. Attackers are using increasingly sophisticated methods and continuously adapt and evolve their attack techniques and tactics. Email is the most common route for cybercrime attacks. The aggregate of these attacks has resulted in billions of dollars in financial losses to organizations worldwide, with Indonesian organizations not being an exception.

IS threats often originate from inside the organization due to IS misuse by insiders of the organization. Insider IS misuse is the intentional misuse of computer systems by users authorized to access those information and networks systems. Frequent insider IS misuse are a security threat and impose costly burdens to the organization.

BEC represents an IS threat, where attackers target business organizations and individuals, then deceive them into illegally transferring funds in large volumes. Countermeasures such as spam filters have been largely unsuccessful in thwarting BEC attacks. Like cybercrimes, BEC causes significant financial losses to organizations.

To combat cybercrimes and insider threats such as IS misuse, organizations have adopted a deterrence posture by enforcing IS countermeasures, such as information security policies, cybersecurity training, and computer network monitoring. While many organizations have reported benefits in implementing deterrence practices, other organizations have not for reasons unclear.

Chapter 3

Methodology

The goals of this research were to assess what older workers at Indonesian SMBs do to acquire, apply, and share information security countermeasures aimed at mitigating cyberattacks, as well to assess if and how younger workers share information security countermeasures with their older colleagues. In this chapter, a description of the research methodology is provided along with specific research methods that were employed. Data collection and analysis methods are described both conceptually and operationally along with an explanation of how results were presented in Chapter 4. Chapter 3 concludes with a summary.

Overview of Research Methodology

Yin’s (2018) exploratory case study research combined with Moustakas’ heuristic methods of inquiry (Moustakas, 1990; 1994) were used to answer the research questions in this study. After reviewing research approaches that would best fit the goals and research questions, the case study methods of Yin and Moustakas were selected. Yin (2017) defined case study methodology as empirical inquiry that investigates a contemporary phenomenon within its real-life context when the boundaries between phenomenon and context are not entirely clear. Aailtio and Heilmann (2010) stated that case studies based on Yin’s methodology are especially suitable to understand variable social phenomena in real-life business environments. The utility of Yin's methodology became apparent during the implementation of the study, where it sought to understand the real-world IS practices of older workers in the Indonesian SMB environment. Participant responses were both literal and nuanced.

Yin (2015) described the process of conducting qualitative research in the following phases:

1. Defining something to investigate. Yin (2015) posited the question to researchers: what are the distinctive features of the study, and are there potentially new insights that have emerged? Yin (2015) also emphasized the importance of originality (i.e., a study that has not been undertaken before) in the research topic, in that the researcher should be of the researcher's own making, ideas, words, and data, including efforts to determine otherwise. The specific topic of this research was not found anywhere in academic literature and databases, and was selected for its originality, as were the ideas and data that was subsequently gathered after the participant interviews. The topic of this research was searched in academic literature and databases, and no instance was found. Based on this, this research topic was selected for its originality, as were the ideas and data that was subsequently gathered in the participant interviews.
2. Collecting relevant data, meaning dealing directly with the primary source of data (e.g., field observations and interviews) and not secondary sources. Data collection activities include interviewing, observing, collecting, and examining, and feeling (Yin, 2015). Yin (2015) stated that one of the challenges with a qualitative study is to conceive a study topic where the researcher can access and collect the source data. Yin (2015) also indicated the relativity in defining a desired number of instances for a broader or narrower unit of data collection in qualitative studies, where larger

numbers generally create greater confidence in the study's findings. This study falls in the narrower category. Yin's data collection methods —which include distinguishing between firsthand, secondhand, and thirdhand evidence, and triangulating evidence from multiple sources — were adopted in this study. The subsequent data gathered from the participant interviews were an indication of Yin's relativity in defining a narrower unit of data collection (i.e., ten participants) in this qualitative study. Triangulation was subsequently conducted following the data collection, mainly by cross-referencing participant responses to their interview questions which were inter-related to each other, and cross-referencing responses to the same questions by older and younger workers from the same dyads. Discrepancies, variances, and consistencies were identified from cross-referencing participant responses.

3. Analyzing and interpreting the results. Yin's key analytical methods were used in this phase. This phase also incorporated Yin's (2015) qualitative research analysis phases (i.e., compiling, disassembling, reassembling, interpreting, and concluding) and recommended actions for analysis (i.e., reverifying data accuracy, comprehensive analysis, and acknowledgement of researcher's personal biases) and interpretation (i.e., completeness, fairness, empirical accuracy, value-added, and credibility). Yin (2015) also recommended the implementation of structured and orderly data management in the data analysis process, including the adoption of data textual-based dictionaries versus numbers for qualitative analysis. Additionally, Yin (2015) recommended the construction of hierarchical and matrices data arrays to facilitate analysis of the qualitative data and noted data matrices as a central form of qualitative

analysis. These approaches and methods were incorporated in this phase of the study. Following Yin's (2015) recommendation, data management and analysis methods were subsequently implemented with the participant data. Hierarchical and matrices data arrays were also constructed to perform qualitative analysis on the datasets and interpret the key data findings.

4. Drawing conclusions based on the empirical findings. Yin (2015) defined a conclusion in qualitative research as a statement that raises the findings of a study to a higher conceptual level or broader set of ideas, which captures the broader significance of a study, and which conclusion lies in such concepts as lessons learned, implications of the research, as well as practical implications. Yin (2015) also emphasized the validity of a study and its findings, indicating that it is one where data are properly collected and interpreted and the conclusions accurately reflect and represent the real world that was studied; on the other hand, studies are worthless if they result in false findings. One postface of the conclusion of a study’s findings point to new research in need of being undertaken, with the conclusion declaring what is still unclear, or unknown (Yin, 2015). Yin (2015) indicated that research conclusions typically include questions to be addressed in future research, which may be also accompanied by suggestions for the needed research and design methods. Recommendations for future research are presented in Chapter 5 along with the broader significance of this study, lessons learned, and implications.

Yin’s (2017) case study approach also allows latitude for both quantitative and qualitative studies, as well as both single and multiple case studies. The latitude that this case study approach enables is conducive to this research, where outcomes of in-person interviews with the participants were difficult to predict and subject to different interpretations. Interview data were carefully analyzed, structurally codified, and then interpreted into findings. The findings were in turn consolidated into common themes and their implications were discussed, and the recommendations and suggestions for needed research and design methods were finally presented. Indeed, as Yin (2017) indicated, the outcomes of in-person interviews with the participants were nuanced and subject to different interpretations. The participant responses to the questions could be interpreted in different ways, as was articulated in the findings section.

Yin (2015; 2017) indicated that every research study has a design, and indicated that study design is primarily concerned with:

1. A study's question, which can be distilled to: 'who', 'what', 'where', 'how', and 'why'.
2. Propositions, which point to something that should be examined within the scope of the study.
3. Unit of analysis, which is the fundamental problem of defining what the case is, or a problem that was established at the onset of the case study.
4. The logic linking the data to the propositions, pattern-matching where elements of information from the same case may be related to some theoretical proposition.

Yin (2015) also stressed the importance of conducting qualitative research methodically and in an orderly manner, while also allowing adequate room for discovery and unanticipated events, which this study observed.

Trustworthiness and Adherence to Evidence

Yin (2015) also underscored the importance of transparent research procedures in building trustworthiness and credibility into qualitative research, and ability of the research to withstand scrutiny by others. Sinkovics et al. (2008) stated that credibility, dependability, transferability, and confirmability need to be established to gain trustworthiness in qualitative research. Law (2002) stated that establishing trustworthiness of research improves reader confidence that the findings of the research are worth of attention (as cited in Curtin & Fossey, 2007). Several methods and approaches can be taken to improve trustworthiness. For example, Krefting (1991) recommended for researchers to clearly describe the strategies they used within their research articles (as cited in Curtin & Fossey, 2007).

Denzin (1970) also proposed the use of triangulation in qualitative research through the combination of multiple observers, theories, methods, and data sources can overcome intrinsic bias originating from single method, observer, and theory studies (as cited in Curtin & Fossey, 2007). For these reasons, this research used triangulation and a clear articulation of strategies used in this research.

One triangulation method that was implemented was to cross-reference and compare responses from participants from the same dyads to the same questions asked to them. For example, dyad participant responses to the questions such as "How often is Information Security is discussed at work?" and "What is your opinion about Information Security practices at work?" were contrasted against each other to identify possible variance in the responses. Aguilar-Solano (2020) discussed triangulation through observation of audio-recorded interaction with participants. Another triangulation method implemented was to observe the duration participants spent in responding to interview questions, and the length and substance of their responses. There were participants who, during the interviews, took their time to carefully read the questions, take pauses, and provide thoughtful and detailed answers, were triangulated. There were other participants who, in contrast, appeared hurried, impatient, and aloof during the interviews, rushing through the questions, and only providing curt responses. These non-verbal cues were also noted and triangulated to this latter category of participants, and consequently, the research assigned less weight and validity to their responses.

Yin (2013) stated the importance of the actual language of the subjects and the context in which that language is articulated. All interviews with the participants were conducted in Bahasa Indonesia, the country's national language, and then translated into English. One interview with participant A-01-OE-0 began in English, but subsequently transitioned into Indonesian because the interviewee felt more comfortable expressing himself in his native Bahasa language.

Yin (2013) indicated adherence to evidence as well as the importance of the actual language of the subjects and the context in which that language is articulated. Regarding analysis of case study evidence, Yin (2013) provided four strategies: the reliance on theoretical propositions that lead to the case study; the development of a case description to organizing the case study; the use of qualitative and quantitative data; and an examination of rival explanations. These strategies were be adopted for this study. Regarding original language, Yin (2013) indicated that actual language of the subjects is valued as representation of reality. For this reason, interviews with the subjects who are Indonesian, were conducted in their native language (i.e., Bahasa), then audio recording and notes were subsequently translated from Bahasa into English.

To build trustworthiness and transparency towards participants for the research, the interview questions were sent in advance to the participants so they could review the questions and ask any questions or requests ahead of the actual interview, if they desired. The interviewer was fully transparent with the participants about the purpose and process of the interview and offered to answer any questions the participants had any time before, during, and after the interview. The interviewer was careful to ensure that the interview participants were comfortable with the interview time, length, and format. Before the interview, the researcher attempted to put the participants at ease by building rapport with them. The interview began with five to ten minutes of informal conversation, for example, about local events, the weather, etc. After establishing rapport with the participant, the researcher initiated the interview.

Moustakas' Heuristic Method

Elements of Moustakas' heuristic method (Moustakas, 1990; 1994) were incorporated in this study, specifically for its philosophy grounded in human compassion (Kenny, 2012). Moustakas developed heuristic research and was a proponent of the humanistic movement of the 1960s (Brisola & Curry, 2016). Moustakas defined heuristic inquiry as a qualitative and phenomenological research model as well as an autobiographical approach to qualitative research (Sultan, 2018). Moustakas utilized the heuristic research process which begins with the identification of a question that is deeply felt, and a question that has an emotional effect on the researcher that cannot be ignored (Kenny, 2012).

Moustakas developed his research style in part from influence of fellow humanistic psychologists, but also in large part from his personal experience with his young daughter who had been recovering from a serious illness, which motivated him to write books with loneliness themes and subsequently his book on heuristic research (Brisola & Curry, 2016). Moustakas (1990) stated that the heuristic inquiry process begins with questions or problems which the researcher seeks to illuminate or answer and is followed by a research process.

Moustakas interpreted heuristic as an open-minded attitude towards discovery throughout the entire study (Brisola & Curry, 2016). His heuristic research focused on the search for the discovery of meanings and essence in significant human experiences (Brisola & Curry, 2016). Heuristic inquiry does not exclude the researcher from the study, but integrates the researcher's experience, and views the researcher as the participant (Djuraskovic & Arthur, 2010). Under Moustakas' method, during the investigation of the research, the research topic must become the researcher's companion—a constant presence in his or her thoughts, relationships, and reflections (Brisola & Curry, 2016). For these reasons, Moustakas' approach was fitting for research on aging workers in Indonesia nearing their mandatory job retirement age of 56 in the private sector category (Gajimu, 2021). The mandatory retirement ages of Indonesian employees based on their occupation classification, as indicated by Indonesian Labor Laws No.13/2003 are provided in Appendix B.

In keeping with the Moustakas method (Brisola & Curry, 2016), the researcher maintained an open-minded attitude towards discovery throughout the participant interviews and focused on the significant human experiences (Brisola & Curry, 2016). The researcher attempted to be mindful throughout the interview process of the potentially sensitive topic of aging workers in Indonesia who are nearing their mandatory job retirement age (Gajimu, 2021). The interviewer conducted interviews with all participants in a friendly, polite, and respectful manner. The interviewer extended deference to older participants with Moustakas' philosophy in mind. However, the reality that the researcher discovered during the interviews with older workers was different: all older participants demonstrated optimism, vigor, and youthful energy during the interviews. This was in stark contrast with the interviewer's biased and preconceived notion of aging, fatigued, and uncheerful workers nearing their mandatory retirement phase.

Specific Research Methods Employed

Qualitative research, specifically Yin's case study methodology, was the central research framework for this study (Yin, 2014). It is a well-established and accepted methodology in the academic domain and is the most suitable research approach for the requirements of the study.

To add depth to this research, the heuristic research paradigms, and philosophy of Moustakas were also used. While the selection for Yin and Moustakas' methods were based on its expected benefits, research was also conducted on limitations of case and heuristic research methodologies. Among the limitations cited was that case study method may lack scientific rigor and provide limited basis for a wider population (Yin, 2017).

Semi-Structured Interviews

Data were collected via semi-structured interviews supplemented by an interview guide (Appendix F). A pilot test of the interview process was developed and implemented. Appendix H outlines the interview pilot process. The intent of the pilot test was to administer a prototype of the interview guide to assess whether the questions were effective in eliciting useful responses from the participants and make revisions and refinements to questions if necessary. An updated and improved version of the interview guide could then be used with study participants. The interview guide was tested with a college professor (older worker) and program manager for curriculum development (younger worker) at an Indonesian university. Feedback from the questions asked during the pilot test was used to improve the guide. There were minor revisions, which included revising the length of discussion topics, timing of questions, and presentation format of the interview questions in Zoom.

Data Collection

Participants

The original target data sample were 30 Indonesian employees working at five SMBs in Jakarta, Indonesia. The 30 target participants included fifteen male or female subjects aged 50 to 55, and fifteen male or female subjects aged 25 to 35. The additional plan was to maintain one older and one younger employee for each SMB and representing a dyad — the unit of analysis for this study.

After receiving approval from Nova Southeastern University's Institutional Review Board (IRB) (Appendix A), a subsequent three-month campaign to locate and recruit participants resulted in a total of 16 participants agreeing to be interviewed. The participants were Indonesians employed by ten Indonesian organizations in the Jakarta metropolitan area. The participants were six employee dyads (12 employees) and four non-dyad employees from six SMBs defined as businesses with 1-299 employees, and four MLBs, defined as businesses with 300 employees or more.

In keeping with the design of this research which limited the scope to employees at Indonesian SMBs, participants from organizations G to J and employees 11 to 16 were omitted from this research because they were employed by MLBs, which was outside the scope of this research design. SMB F was also omitted because it did not represent a compete dyad, despite the interview with a younger worker participant F-06-YE-06 being completed.

In advance of the interviews, participants were sent a list of interview questions (Appendix E) along with a general informed consent form (Appendix K). Fifteen of the sixteen interviews were conducted via Zoom videoconferencing, with one interview conducted using the WhatsApp audio calling feature due to connectivity issues during the interview with participant E-05-YE-05. All interviews averaged approximately 45 minutes and resulted in approximately nine hours of raw video and audio recordings. Interviews with participants were conducted in the Indonesian language (Bahasa Indonesia) with exception of one interview, which was conducted partly in English in the beginning.

The video and audio recordings of the participant interviews were repeatedly reviewed and annotated. The participant responses were not translated word for word, but rather gisted into summary responses of one to two key sentences (e.g., "SMB Management is lacking in its financial support for IS training programs for employees."; "Older workers are slower to comprehend IS and IT."; "Younger workers are aloof in IS SMB policy."), and then translated into English, analyzed, codified into a spreadsheet according to the methodology outlined in Chapter 3. A copy of the spreadsheet (i.e., Participant Interview Translated and Gisted Response Data) is in Appendix C.

The ten participants representing dyads 1-5 (SMBs A-E) represent the final study sample that was used for analysis (Table 8). The nomenclature of each subject's coding (e.g., A-1-OE-1) identifies which worker age group category, dyad, and organization the subject belongs to. Participants were invited to participate either via a WhatsApp IP or email invitation from the researcher. The email solicitation to prospective interview participants is provided in Appendix D.

Table 8.

Sample of Matrix of Organization, Dyad, and Participant Coding (n=10)

Organization	Dyad	Older Employee (OE)	Younger Employee (YE)
A	1	A-1-OE-1	A-1-YE-1
B	2	B-2-OE-2	B -2-YE-2
C	3	C-3-OE-3	C-3-YE-3
D	4	D-4-OE-4	D-4-YE-4
E	5	E-5-OE-5	E-5-YE-5

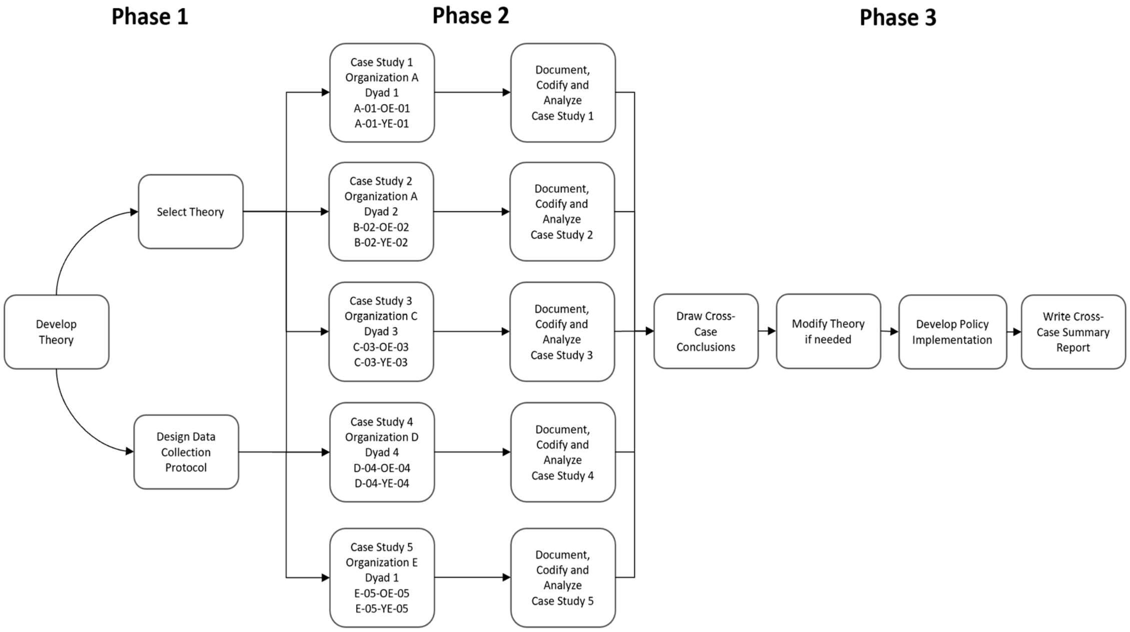
The purpose of the dual age group categorization was part of this study's design to compare information and insights derived from subjects from their differing age groups. Participants were interviewed separately using an interview guide (Appendix F) for one to two hours each in-person or via Zoom video teleconference. Information (e.g., audio/video recordings, notes, etc.) captured from all interviews were consolidated, coded, and analyzed (See Appendix G for a sample interview coding grid) with word-processor and spreadsheet software. In keeping with the multiple subjects interviewed for this research, the multiple-case study design was implemented (Yazan, 2015).

Research Framework

The following multiple case study design construct as illustrated in Figure 6 was a modified version derived from Yin (2013) and was adopted for this study. The Dyad Matrix in Figure 6 was incorporated in this framework in the first column on the left of the Prepare, Collect, and Analyze phase.

Figure 6

Proposed Research framework based on Yin (2013)


Phase 1
Phase 2
Phase 3
Develop Theory
Select Theory
Design Data Collection Protocol
Case Study 1 Organization A Dyad 1 A-01-OE-01 A-01-YE-01
Case Study 2 Organization A Dyad 2 B-02-OE-02 B-02-YE-02
Case Study 3 Organization C Dyad 3 C-03-OE-03 C-03-YE-03
Case Study 4 Organization D Dyad 4 D-04-OE-04 D-04-YE-04
Case Study 5 Organization E Dyad 1 E-05-OE-05 E-05-YE-05
Document, Codify and Analyze Case Study 1
Document, Codify and Analyze Case Study 2
Document, Codify and Analyze Case Study 3
Document, Codify and Analyze Case Study 4
Document, Codify and Analyze Case Study 5
Draw Cross-Case Conclusions
Modify Theory if needed
Develop Policy Implementation
Write Cross-Case Summary Report

The planned research framework in Figure 6 consisted of three sequential phases from the beginning to the end of the process: Define and Design; Prepare, Collect, and Analyze; and

Analyze and Conclude. In the initial Define and Design phase, the theories for this research were developed, the data collection protocol was designed, and the cases were selected. The second Preparation, Collection and Analysis phase, involved the administration of five case studies, each encapsulating two interviews with a dyad of a younger and older employee working for the same SMB. The purpose of this dyad format was to maintain consistency of two subjects working in a same or similar work environment and work culture. After each of the five case studies were completed, case reports were written based on their respective analyses and findings. Upon completion of the five case study reports. Then the third and final Analysis and Conclusion phase began, where the five case study reports were cross-analyzed and consolidated for the summary findings. Modifications to theory and development in policy implementations were enacted as needed during this phase if additional findings and insights were discovered. Finally, cross-case report detailing the findings and conclusions of the analysis across these five reports were implemented.

The following describes the actual implementation of the planned data collection research framework in Figure 6 as it unfolded. After phase 1, including the theory development, selection, and design was completed, participant data were collected from interviews from dyad one to five based on scheduling sequence of the ten participant interviews from the five SMBs. After each participant interview dyad was completed for each organization, the data batch was categorized into a case study, and documented, coded, and analyzed before or during the subsequent participant interviews and case study. These tasks were part of phase 2. Once all tasks for the five case studies were completed in the second phase, then in the third and final phase, the five case studies were cross-analyzed against each other and summarized. It was discovered through this cross-analysis that the data findings and the theory were consistent with no significant deviation; modification was therefore not needed. The cross-summary analysis report was written as the conclusion of this dyad matrix workflow process.

Data Analysis

Thematic analysis was used to analyze the interview data. Thematic analysis was first developed by Gerald Holton and is regarded as a distinctive method with clearly defined social science procedures (Damayanthi, 2019). Braun and Clarke (2006) further developed thematic analysis and defined it as a data analysis method that helps the researcher to identify themes, patterns, and meanings across datasets within the context of specific research questions. Braun and Clarke (2006) deconstructed thematic analysis into phases as illustrated in Table 9.

Using Braun and Clarke's (2006) thematic analysis methodology in Table 9 as a research guideline, the following describes the phases that were undertaken for this research:

Phase 1: Data Familiarization and Generation of Initial Codes

This research phase encompassed Braun and Clarke's (2006) phases 1 and 2 (data familiarization and generation of initial codes). Following the interview with each participant, the researcher carefully transcribed the audio recordings. During the transcription process, recordings were anonymized, and participant codes substituted participant names to mask their identities. Once the audio recordings of the participant interviews were transcribed, the researcher read and re-read the audio transcripts along with hand-written notes and organized them into initial codes that included key words, phrases, and expressions. These initial codes were organized by media source, date, participant code, and participant comments as illustrated in Table 10. At this point, the review and identification of common themes were not yet initiated.

Table 9

Braun and Clarke (2006) Phases of Thematic Analysis Matrix

	Phases	Description of Analysis Process
1	Data familiarization	- Transcribing data - Reading and re-reading data noting initial ideas
2	Generation of initial codes	- Coding interesting features of the data in a systematic fashion across the entire data set. Collating data relevant to each code
3	Searching for themes	- Collating codes into potential themes - Gathering all data relevant to each potential theme
4	Reviewing themes	- Checking if the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2) - Generating a thematic 'map' of the analysis
5	Defining and naming themes	- Ongoing analysis to refine the specifics of each theme and the overall story the analysis tells - Generating clear definitions and names for each theme
6	Producing the report	- Final opportunity for analysis. - Selection of vivid, compelling extract examples - Final analysis of selected extracts, relating back of the analysis to the research question and literature - Producing a scholarly report of the analysis.

Phase 2: Search, Review, Identification and Naming of Themes

This research phase encompassed Braun and Clarke's (2006) phases 3, 4, and 5 (searching for themes, reviewing themes, and defining and naming themes). At this phase, the participant codes and remarks were gathered, reviewed, and categorized into common themes using a thematic map of analysis, as illustrated in Figure 7. Participant codes were linked to their responses; therefore, each instance of a participant response was tracked to the participant (e.g., B -2-YE-2), the participant's age group, the participant's dyad, and the participant's SMB. Participant interview feedback/comments in Table 10 (with sample data), was categorized into general themes (e.g., Level 1 (L-1)), and further categorized into sub-themes (e.g., Level 2 (L-2)). An example of theme hierarchy is provided in Figure 7 and could drill-down multiple levels if necessary. All opinion and theme development fell under the overall topic of this research.

Table 10

Sample Data Transcription from Data Coding Matrix with Dummy Data (n=7)

	Data Source	Date	Subject Code	Response Extract	Theme (L1)
1	Interview - Audio	8/1/2021	A-1-OE-1	"Lack IT policy…"	(Not yet)
2	Interview - Audio	8/2/2021	A-1-YE-1	"Unnecessary policy"	(Not yet)
3	Interview - Audio	8/6/2021	C-3-OE-3	"Mitigate IT threat…"	(Not yet)
	Data Source	Date	Subject Code	Response Extract	Theme (L1)
4	Interview – Notes	8/6/2021	C-3-OE-3	"Too costly…"	(Not yet)
5	Interview – Notes	8/13/2021	C-3-YE-3	"Necessary for security"	(Not yet)
6	Interview - Video	8/13/2021	C-3-YE-3	"Favors older workers."	(Not yet)
7	Interview - Video	8/15/2021	B -2-YE-2	"Indifferent to policy…"	(Not yet)

Figure 7

Sample Thematic Map of Analysis with Dummy Data (n=13)

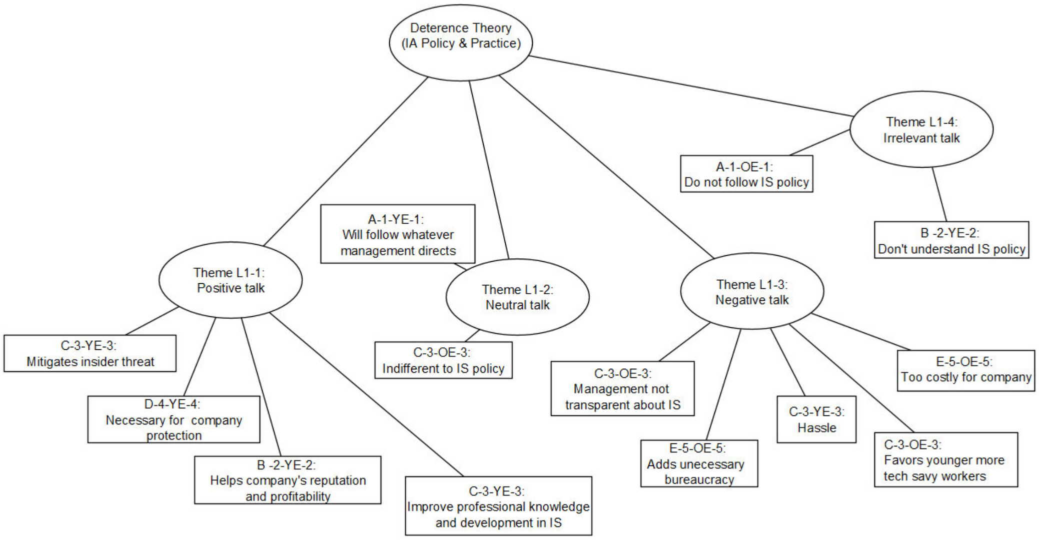
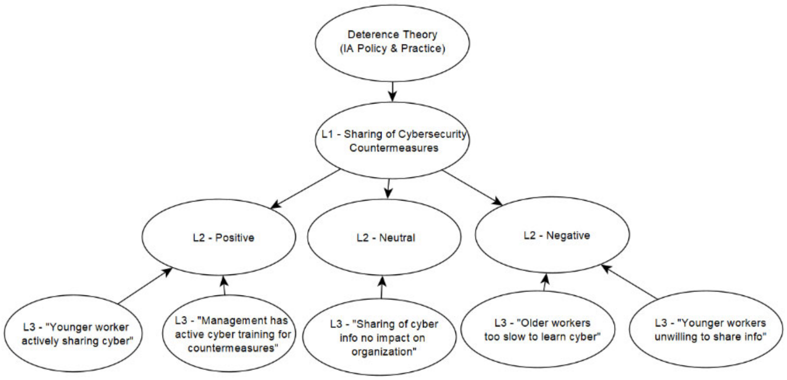


Figure 8

Sample Theme Hierarchy Level 1 (L-1) to Level 3 (L-3) with Dummy Data (n=5)



After completion of the thematic map of analysis, the themes were further refined and divided into applicable sub-categories (e.g., L2, L3) as illustrated in Table 11.

Table 11

Continuation and Refinement of Data-Coding Matrix with Sample Data (n=7)

	Participant Code	Participant Comment	Theme (L1)	Sub-Theme (L2)
1	A-1-OE-1	"Lack IT policy"	Negative Talk	IS Policy
2	A-1-YE-1	"Unnecessary policy"	Negative Talk	IS Policy
3	C-3-OE-3	"Mitigate IT threat"	Positive Talk	IS Countermeasure
4	C-3-OE-3	"Too costly"	Negative Talk	IS Expense/Budget
5	C-3-YE-3	"Necessary for security"	Positive Talk	IS Implementation
6	C-3-YE-3	"Favors older workers"	Negative Talk	Employee Relations
7	B -2-YE-2	"Indifferent to policy"	Neutral Talk	IS Policy

Following the refinement of data coding, the data-coding matrix were manipulated, analyzed, and summarized to explore for possible insights in the data, such as one summary data view and perspective presented in Table 12. This is provided as just one example, but there could be multiple summary presentations of the data analysis.

Phase 3: Report Production

This research phase was parallel to Braun and Clarke's (2006) phase six (producing the report). In this phase of the research, the final analysis of the data would be conducted and presented, which will relate back to the analysis of the research question and literature (Braun & Clarke, 2006).

Table 12

Summary Table from Data Analysis with Sample Data

	Theme (L1)	Theme (L2)	Older Employee (OE)	Younger Employee (YE)	Total
1	Positive	Policy necessary for security	73%	27%	100%
	Theme (L1)	Theme (L2)	Older Employee (OE)	Younger Employee (YE)	Total
2	Neutral	Indifferent to policy	28%	72%	100%
3	Negative	Too costly/bureaucratic	68%	32%	100%

Format for Presenting Results

The results of the study were presented as an MS-Word document in compliance with APA 7th Edition and the Nova Southeastern University Dissertation Guide, and guidance from the Dissertation Mentor and IRB Committee.

Resource Requirements

This research was originally intended and planned as an in-country field study in Jakarta, Indonesia. If the plan had proceeded the requirements would have included travel and accommodation expenses in Jakarta; an Indonesian travel visa; a computer installed with software (MS-Word, MS-Excel, Qualitative Analysis software, Zoom, etc.) required for the research; and a digital audio recorder and notepads and pen stationary to record and document interviews with the interview participants. But due to the emergence of the COVID-19 pandemic and the current Indonesian Government travel restrictions, subject interviews will be conducted remotely via Zoom audio teleconference application.

Summary

This chapter provided detailed overview of the research methodology and design that was used for this research. The proposed sample for this research was also defined and explained, as was the data collection and analysis methods and format for presenting the results of the research.

Chapter 4
Results

Chapter 4 begins with an overview of the research methodology and methods that were used to guide the data collection and analysis. Following this overview, the results of the data analysis and its findings are included. The chapter concludes with a summary of the results.

Research Methodology

Yin's (2014) qualitative case study methodology was the central research framework for this study, with Moustakas' heuristic research paradigm and philosophy applied. Yin (2015) recommended implementation of structured data management in the data analysis process, and hierarchical and matrices data arrays to facilitate analysis of the qualitative data and noted data matrices as a central form of qualitative analysis. This approach was implemented for the collection of the participant interview data and subsequent codification and analysis.

The data collected from the participant interviews were compared and analyzed against Yin's (2015) qualitative research discussed in Chapter 3. Yin's (2018) exploratory case study method, combined with Moustakas' (1994) heuristic methods of inquiry were used to guide the interviews with the participants. Yin's (2015) case study methodology empirically investigates a contemporary phenomenon within a real-life context when the boundaries between phenomenon and the context are unclear. This phenomenon is what was discovered because of the thematic analysis of participant interviews.

In defining investigation on studies, Yin (2015) challenged researchers on whether new insights could emerge from the study that would justify its undertaking. The data from participant interviews revealed insights not previously available in the literature. Yin (2015) also underscored the importance of originality in the research topic. The goal of this research was to assess what older workers at Indonesian SMBs do to acquire, apply, and share IS countermeasures aimed at mitigating cyberattacks, and to assess if and how younger workers share information security countermeasures with their older colleagues. This research topic is original, unique, and was not found in existing literature, and the data from the participant interviews support this assertation.

Yin (2015) stated that one of the challenges with a qualitative study is to conceive a study topic where the researcher can access and collect the source data. The source data were collected from video and audio interview recordings with 16 participants in Jakarta, Indonesia. The interview recordings of ten participants that matched this research criteria were ultimately selected. These data were subsequently reviewed, analyzed, codified, and the results interpreted, which became the basis of this research.

In analyzing and interpreting the results of the data, Yin's analytical methods were adopted and applied, which incorporated his qualitative research analysis phases, namely compiling, disassembling, reassembling, interpreting, and concluding; recommended actions for analysis, namely reverifying data accuracy, comprehensive analysis, and acknowledgement of researcher's personal biases; and interpretation, namely completeness, fairness, empirical accuracy, value-added, and credibility.

Yin (2015) recommended the implementation of structured data management for the data analysis process. He also recommended the construction of hierarchical and matrices data arrays to facilitate analysis of the qualitative data and noted data matrices as a central form of qualitative analysis (Yin, 2015). These approaches and methods were implemented for this research and are presented in this chapter.

In the analysis of case study evidence, Yin (2013) provided four strategies: the reliance on theoretical propositions that lead to the case study; the development of a case description to organizing the case study; the use of qualitative and quantitative data; and an examination of rival explanations. These strategies were adopted for this study. Finally, in drawing conclusions from empirical findings, Yin (2015) defined a conclusion in qualitative research as a statement that raises the findings of a study to a higher conceptual level or broader set of ideas and significance of a study, which leads to lessons learned, implications of the research, as well as practical real-world implications. The findings of the participant interview data are in keeping with this research philosophy.

Yin (2015) also emphasized the validity of a study and its findings, indicating that the data should be properly collected and interpreted, and the conclusions accurately reflect and represent the real world that was studied and analyzed. Takeaways from the conclusion should also point to new research in need of being undertaken, with the conclusion disclosing what is still unclear, or unknown (Yin, 2015). Additionally, he indicated that research conclusions would include questions to be addressed in future research, and recommendations for the needed research and design methods (Yin, 2015). The conclusion section of this qualitative research includes this format.

Data Analysis Results

Braun and Clarke's (2006) six-phase thematic analysis matrix introduced in Chapter 3 was used to implement the thematic analysis for this research. Table 13 presents the data results of participants who were interviewed. The identities of participants were anonymized and masked with identification (ID) codes. The coding method of the participants were also explained in Chapter 3, Table 8. The ID coding nomenclature is: [SMB A-E] – [Dyad 1-5] – [Older Employee (OE) / Younger Employee (YE)]- Employee 1-2. For example, participant A-01-OE-01 would indicate that he or she is employed by SMB A; Dyad 1; an older worker, and employee 1 of 2. The participants are coded according to this nomenclature and listed in Table 13.

Table 13

List of Coded Interview Participants (n=10)

SMB	Dyad	Older Employee (OE)	Younger Employee (YE)
A	1	A-01-OE-01	A-01-YE-01
B	2	B-02-OE-02	B-02-YE-02
C	3	C-03-OE-03	C-03-YE-03
D	4	D-04-OE-04	D-04-YE-04
E	5	E-05-OE-05	E-05-YE-05
~~F~~	~~6~~	~~-~~	~~F-06-YE-06~~
~~G~~	~~7~~	~~G-07-OE-07~~	~~G-07-YE-07~~
~~H~~	~~8~~	-	~~H-08-YE-08~~
~~I~~	~~9~~	-	~~I-09-YE-09~~
~~J~~	~~10~~	-	~~J-10-YE-10~~

Note. SMB F, Participant F-06-YE-06, was omitted from study due to being an incomplete dyad. SMB G to J participants were omitted from study due to being outside this research's organization criteria. MLB (Medium-to-Large Business) is officially categorized by the Indonesian Government as an organization with 300 employees and above, and was outside of the scope of SMB, which is categorized as 1-299 employees.

There were five different industry types of the SMBs that the ten participants belonged to, which is listed in Table 14. The five SMBs were assigned code A to E. The diversity in the industry types contributed to greater depth of analysis of the source material for this study.

Table 14

SMB and Industry Type

SMB	Industry Category
A	Consulting - Information Technology (IT)
B	Consulting - Corporate Social Responsibility (CSR)
C	Insurance (Life & Health)
D	Sports Medicine
E	Construction (Water Treatment/Piping)

Participants' job occupations were relevant to the research because it could provide insight into their feedback relative to their IS knowledge. For example, participants who were Chief Technology Officers, IT Project Managers, and IS Managers tended to discuss IS and IT topics with more familiarity and detail due to their related IT and IS professions. At the same time, participants who were non-IT or IS practitioners discussed IS less, but also demonstrated a functional understanding of IS and its risks. The job descriptions and occupations of the participants, cross referenced to the SMB coding and their industry categories are listed in Table 15.

Coding Participant Interview Data

Following each interview, its audio recording was anonymized, and the participant's response to the 13 questions from the interview guide (Appendix F) were carefully reviewed, transcribed, and categorized into topics and sub-topics. Participant interview responses that resonated but could not be categorized into any specific theme or idea were categorized under 'miscellaneous.'

Table 15

Job Description/Occupation of Participants (n=10)

SMB	Industry Category	Older Employee Code Job Description	Older Employee Code Job Description
A	Consulting – IT	A-01-OE-01 Chief Technology Officer	A-01-YE-01 IT Project Manager
B	Consulting – CSR	B-02-OE-02 Manager	B-02-YE-02 Office Administrator
C	Insurance	C-03-OE-03 HR Mgr. – People Svcs	C-03-YE-03 HR Mgr. – Bus Dev
E	Sports Medicine	E-04-OE-04 Chief Executive Officer	E-04-YE-04 IT Project Manager
F	Construction	E-05-OE-05 Site Manager	E-05-YE-05 Office Manager

The participant interview data were divided into two categories. The first category was qualitative data from participant responses to interview questions 1 through 9, and 12, which were quantifiable and directly measurable (e.g., how many years a worker worked at an SMB; what age bracket the worker was); but topics and themes could also be developed from these data. The second category was qualitative data from open-ended participant responses from questions 10, 11, and 13. These data were non-numerical and not directly quantifiable but could be developed into topics and categories that were quantifiable by frequency of recurrence (e.g., the instances of participants confirming that IS compliance is a problem at an SMB). The coding of participant responses was implemented with these two data categories in mind.

1. Participant demographic and SMB data:
    - Question 1: Participant length of employment
    - Question 2 : Participant job description/occupation
    - Question 3: Participant SMB older to younger employee ratio
    - Question 4: Participant SMB measurement method of employee IS skills
    - Question 5: How IS can protect participant SMB from IS threats
    - Question 6: How IS information is distributed at SMB.
    - Question 7: Participant SMB IS training methods
    - Question 8: Participant frequency of discussion on IS topics
    - Question 9: How IS information and protocols are socialized at work.
    - Question 12: Participant SMB frequency of IS discussion with senior workers

Results from this data category were analyzed, measured, and presented in structured data format in tables and figures, and themes were then sought, validated, and defined. The results of this data category are presented in Tables 12, 13, 14, and 15.

2. Participant responses to open-ended questions:
    - Question 10: IS challenges with coworkers
    - Question 11: Implementation at SMB and by Government
    - Question 13: IS differences with senior workers

Results from this data category were analyzed and categorized into topics and sub-topics, and themes were then sought, analyzed with thematic maps, validated, and defined from these data.

Participant Demographic and SMB Data Results

Demographic and SMB data from interview participants responses to questions 1 to 9, and 12, were collected, analyzed, organized, and then presented in structured table format for subsequent topic, sub-topic, and theme seeking.

Table 16

Dyad, Participant Interview Questions and Response Coding Matrix Template (n=10)

		Questions & Response Codes											
Dyad	Participant Code	Qualitative Responses Quantitative Coding									Qualitative Responses Qualitative Coding		
		1	2	3	4	5	6	7	8	9	10	11	12
1	A-01-OE-01												
	A-01-YE-01												
2	B-02-OE-02												
	B-02-YE-02												
3	C-03-OE-03												
	C-03-YE-03												
4	D-04-OE-04												
	D-04-YE-04												
5	E-04-OE-04												
	E-04-YE-04												

Table 17 presents the summary data results from participant responses to the question about IS protection and confidentiality at their SMB. Five participants responded to this question, while the other five participants did not address this issue or responded and expressed that they did not know enough about the question asked to respond or were not in the IT/IS department of the SMB, and therefore didn’t know the answer to the question. The summary response indicated that IS protection and confidentiality were important to several participants, first for their customer Personal Health Information (PHI) (40%), and second, for their SMB information (CFI) (20%) and customer personal financial information (PFI) (20%), and other unspecified (20%).

Table 17

Participant SMB Concerns for IS Protection and Confidentiality (n=10)

	Participant Concerns			
SMB/MLB Industry Type	PHI	PFI	CFI	OTHER
1. IT Consulting	0	1	1	0
2. Corporate Social Responsibility	0	0	0	0
3. Life Insurance	1	0	0	0
4. Sports Medicine	1	0	0	0
5. Construction – Water Treatment/Piping	0	0	0	1
Total	2	1	1	1
%	40	20	20	20

Note: Five responses related to the PHI, PFI, and CFI topics were received from ten participants. PHI = Customer Personal Health Information, PFI = Customer Personal Financial Information CFI = Company Financial Information.

Level of importance of IS and data confidentiality to some participants were possibly driven by the industry type of their SMBs. The data presented in Table 17 indicated the level of importance of IS that could be influenced by specific industries that hold data sensitivity to higher standards and accountability. For example, participants E-04-OE-04 and C-03-OE-03 from Sports Medicine and Health Insurance SMBs respectively, which routinely handle sensitive customer medical data, stressed the importance of confidentiality in Personal Health Information (PHI) of their customers and their strict adherence to protocol in handling and transmission of customer data. Participant E-04-OE-04 stated that worker mishandling of customer PHI data was not tolerated and could result in probation or termination. On the other hand, participant B-02-OE-02 from the CSR (Corporate Social Responsibility) Consultancy dealt mostly with less sensitive customer data (e.g., arts and craft inventories, etc.) and did not express serious concerns for data security and confidentiality.

Participant E-04-OE-04 also stressed the importance of confidentiality in handling data containing customer PHI, and their mandatory use of file encryption to transmit the data. Participants E-04-OE-04 and C-03-OE-03 discussed how they encrypted all customer data in password-protected files before transmitting via e-mail or online shared folder applications such as Google Drive and Drop Box. Participants E-04-OE-04 and C-03-OE-03 also indicated that they would send passwords for the encrypted files via separate channels. This suggested how participant perception of protecting sensitive customer data, such as PHI, could be tied to their professional reputation in the health insurance and sport medicine business. This can be compared to the U.S. Health Care providers which treat patient data confidentiality in serious regard and are subject to federal Health Insurance Portability and Accountability Act (HIPPA) regulations.

In another example, participant A-01-OE-01 indicated his SMB maintained business contracts with large telecommunication providers and stressed the importance of customer Personal Financial Information (PFI) protection. PFI confidentiality appeared to be important to Indonesian SMBs.

In response to the interview question “What is your opinion on Information Security at your company and in Indonesia?”, participant A-01-OE-01 indicated his SMB had important contracts with major telecommunication service providers and implemented strict IS countermeasures in his company. The participant expressed his frustration with the lack of concern of several of his clients in their handling of sensitive customer banking data. Participant A-01-OE-01 added that IS only became a top concern and priority to those clients after a serious IS incident (i.e., data breach) occurred, where credit card data and personal information of customers were stolen. Participant A-01-OE-01 previously indicated that his IT consulting company retained clients in the Indonesian banking sector.

Participant B-02-OE-02, a manager for a CSR consulting company, stated that their company submits data for Indonesian micro-businesses in arts and crafts products, and that product inventory data of these micro-businesses were not considered sensitive compared to other businesses such as those in the banking and medical sector. It was important to note the differences in categories in sensitivity levels between SMBs.

Table 18 presents the summary data results from participant responses to the question on training methods used at their SMBs. The data indicated that self-paced e-learning through Learning Management Systems (LMS) and virtual training classes (webinars) were the most popular form of IS training at these SMBs. The ‘None’ responses indicated that the SMB did not have an IS training program, which was the case with SMB B (CSR Consulting Company) and SMB E (Construction Company).

Despite data indicating complaints and frustration expressed by one participant (A-01-OE-01) for lack of SMB support in funding for IS training, and another older dyad (E-05-OE-05) indicating no IS training program for their SMB, the same data also indicated training programs that appeared adequate for all the other SMBs. IS training via virtual class (which most participants termed “webinar”) was the most popular IS training format for these Indonesian SMBs.

Table 18

IS Training Methods Used by SMBs (n=10)

#	IS Training Method	SMB					Total	%
		1	2	3	4	5		
1	Virtual Class / Webinar	0	0	0	1	1	2	28.57
2	In-Person Class	0	0	0	0	0	0	0
3	e-Learning	0	0	0	1	1	2	28.57
4	Self-Initiated Learning	0	0	1	0	0	1	14.29
5	None	1	1	0	0	0	2	28.57
	Total	1	1	1	2	2	7	100

Note. The above were the responses from ten participants from the question on what IS training methods were used at their SMBs. Several participants indicated their SMB had no IS training.

The Indonesian Government COVID-19 restrictions combined with the shifting work environment paradigm to teleworking was likely germane to this. Likely for the same reasons, no participants indicated In-Person Classroom instruction for IS training — although this could also be attributable to funding limitations, since classroom training is typically the costlier training format compared to other formats. e-Learning in the form of Computer Based Training (CBT) or training using a Learning Management System (LMS), ranked second in IS training format for SMBs. Participants indicated e-Learning IS training as an onboarding requirement and mandatory annual training requirement. The third training format was self-initiated learning, which Participant A-01-OE-01 indicated as the SMB management's expectation for its workers. It was also this participant who had complained about the lack of funding for his SMB's IT employees. A-01-OE-01 and A-01-YE-01 opined that there is an expectation for IT/IS practitioners to be self-motivated in their pursuit of IT/IS training to maintain currency of their skills.

Table 19 presents the summary data results from participant responses to the question on IS tools and methods used at their SMBs. The data indicated that the SMBs used a wide array of IS tools and methods to protect themselves, and there was no single dominant method. Password encryption on folders and files were most often cited by participants as their primary means of enforcing IS at their SMBs. Participants more knowledgeable in IT and IS indicated antivirus software and server firewalls (8) as one of the main methods of protection for their SMBs.

Table 19

IS Tools and Methods used by SMBs (n=10)

SMB IS Method Reported	1	2	3	4	5	Σ	%
Password-protection on folders	1	1	1	1	0	4	14.81
Password-protection on files	1	1	1	1	0	4	14.81
9Antivirus Software	1	0	1	1	1	4	14.81
Server Firewall	1	0	1	1	1	4	14.81
Network URL blocking	1	0	1	1	0	3	11.11
Computer port blocking	1	0	1	1	0	3	11.11
Two-Factor Authentication (2FA)	1	0	0	0	0	1	3.70
MS-Windows Folder permission	1	0	1	0	0	2	7.41
Company-issued computers	1	0	0	0	0	1	3.70
Password-protected WiFi	0	0	1	0	0	1	3.70
Total	9	2	8	6	2	27	100

Note. The above were the responses from ten participants from the question on what IS training methods were used at their SMBs. Several participants indicated their SMB had no IS training.

Data from some participant interviews appeared to differ from part of the literature review, which was that many SMBs placed lesser importance on IS. The results from the data analysis did not find SMB indicating lesser importance on IS. Even when SMBs of some of the participants (A-01-OE-01; A-01-YE-01; E-05-OE-05) possessed limited IS resources, they still articulated the importance of IS to their SMBs. Participant E-05-OE-05, a Field Manager for a Construction and Piping SMB, elaborated: “We deal with a sensitive internal contract and company files, and it would be important to protect them, but we don’t have an IT Department that would be able to provide support on this. Therefore, IS would be important to our company.”

Lack of SMB prioritization in IS and cybersecurity training and systems investment was a problem cited in the literature. For instance, Suhartanto and Leo (2018) stated that Indonesian SMBs have underperformed due to issues such as financial constraints and limitations in market and technology. Berry and Berry (2018) indicated that SMBs lack policies, procedures, and training to secure their resources. Chen (2016) also indicated that SMBs have little desire to allocate their limited resources for what they perceive as speculative risks, such as cybersecurity threats, that may not even occur. Participant A-01-OE-01expressed frustration with the lack of budget prioritization of IS training and expansion by the SMB. Instead, as he indicated, funding was allocated to other undisclosed business priorities of his SMB. Despite this, several participants (A-01-OE-01, C-03-OE-03, C-03-YE-03, E-04-OE-04, E-04-YE-04, E-05-OE-05) underscored the importance of IS in protecting their sensitive company and customer data.

While the IT/IS resource and infrastructure of larger SMBs, such as with SMB E (Sports Medicine Company), could afford to resource more IS assets and programs, participants from the smaller SMBs including A, B, and F used lower-cost IS tools and methods, such as with the use of password-protected file and folder encryption of sensitive data across almost all SMBs in this study. These results are displayed in Table 17, which lists all IS tools and methods that participants reported they used or was being used by the SMBs. SMBs A, C, and D which maintained IT departments and staff, implemented IS countermeasures over the network beyond the standard antivirus software and server firewalls. For example, Participants A-01-OE-01, A-01-YE-01, C-03-OE-03. and C-03-YE-03 stated that network policy blocked URLs, USB ports, and password-protected their Wi-Fi networks for business use only. Participants C-03-OE-03 and C-03-YE-03 indicated that the Wi-Fi at the office could only be used for job functions and nothing else. Only 1 SMB reported using two-factor authentication (2FA) as one of their IS countermeasures.

Participants B-02-OE-02 and B-02-YE-02 from SMB B, and C-03-OE-03 and C-03-YE-03 from SMB C, teleworked but indicated that they maintained strict oversight and protocol with protection of customer data through file and shared virtual folder encryption with password-protection.

One exception to the SMBs in deficient IS practices is SMB F (Construction Company). Participants E-05-OE-05 and E-05-YE-05 of the Construction and Piping SMB indicated that their SMB had no dedicated IT Department to implement IS, and no IT or IS policy or training in place for its workers. Participant E-05-OE-05 indicated antivirus software was used on employee computers not as part of any the SMB IT/IS policy, but rather as a standard procedure to remove viruses from their computers if there is a software virus infection. Participant E-05-OE-05 also expressed the need for his SMB to implement better data protection security measures to protect their sensitive business and contract software files.

Participant Results to Open-Ended Questions

Data from interview participant responses from questions 10, 11, and 13 in Appendix C were analyzed, coded, organized, and presented as thematic maps to help identify themes that might emerge from the topics and sub-topics.

Table 20

Initial Code Generation for Opinion Responses (Question 10) (n=10)

SMB	Worker Code	Q10 -What challenges in IS do you experience in the workplace?	Tentative Themes
A	A-01-OE-01	- Budget restrictions from SMB comptroller. - Low priority with IS until an incident occurs. - Younger coworkers aloof and not compliant with IS - Unauthorized use of USB thumb drive	- IS budget constraints - IS low priority - Younger workers - job performance - Insider threat
A	A-01-YE-01	- Budget restrictions impacting cybersecurity, IS training - Younger coworkers entitled and not loyal	- IS budget constraints - Younger workers - job performance
B	B-02-OE-02	- Younger coworkers more easily frustrated by IS/IT work	- Younger workers - job performance
B	B-02-YE-02	None	None
C	C-03-OE-01	- Network policy overly restrictive	- IS policy too restrictive
C	C-03-OE-02	None	None
D	D-04-OE-04	- Lack of compliance with IS policies - Potential employee disgruntlement/revenge	- IS lack of compliance - Insider threat - revenge
D	D-04-YE-04	- Lack of IS guidance from headquarters	- IS lack of guidance from leadership
E	E-05-OE-05	- No budget for IS - IS vulnerabilities with sensitive company data	- IS budget constraints - IS data vulnerabilities
E	E-05-YE-05	None	None

The approach to forming themes originated from the interview questions 10, 11, and 13. Table 20 shows the gisted participant responses (Column C) received to Question 10: “What challenges in IS do you experience in the workplace?” Column D contains the tentative themes that were identified during Phase 3 of the theme-searching process.

The question of challenges in the workplace widened the range of the responses from the participants, which could be associated with common topics, as was illustrated in Table 15.

Table 20 presents the gisted participant responses (Column C) from Question 10: “What challenges in IS do you experience in the workplace?” Column D contains topics that were identified during Phase 3 of the theme-searching process.

- Table 21 presents the gisted participant responses (Column C) from Question 11: “What is your opinion about IS governance and practices at the workplace and by the Indonesian Government?” Column D contains the topics that were identified during Phase 3 of the theme-searching process. The question regarding the state of IS practices in the workplace and Indonesian Government policy and oversight in IS widened the range of the responses from the participants, which could be associated with common themes in Table 16. Column D contains the topics identified during Phase 3 of the theme-searching process.
- Table 22 presents the gisted participant responses (Column C) from Question 13: “What are the differences or challenges to discuss or collaborate with older workers on IS? Column D contains the topics that were identified during Phase 3 of the theme-searching process. For this question, only the younger workers were asked these questions. Older workers were omitted from this section of the interview.

Table 21

Initial Code Generation for Opinion Responses (Question 11) (n=10)

SMB	Worker Code	Q11 - What is your opinion about IS governance and practices at the workplace and by the Indonesian Government?	Topics
A	A-01-YE-01	- IS awareness still low, particularly among the younger workers.	- Low SMB priority in IS - Low IS priority among younger workers
B	B-02-OE-02	- IS practices good. There has been no major IS incidents reported.	- SMB IS practices satisfactory
B	B-02-YE-02	- No issues with IS at the workplace. - Indonesian Government needs more regulations due to IS issues in the industry.	- SMB IS practices satisfactory - Stronger government oversight in IS needed.
C	C-03-OE-01	- Tighter IS regulations and oversight needed by the Indonesian Government	- Stronger government oversight in IS needed.
C	C-03-OE-02	- Internal hacking a potential issue with USB thumb drives	- Insider threat in SMB an issue
D	D-04-OE-04	- Tighter IS regulations and oversight needed by the Indonesian government - IS awareness still low among SMB employees - SMB taking strong IS precautions and protocols.	- Stronger government oversight in IS needed. - Employee IS awareness low - SMB committed to stronger IS practices
D	D-04-YE-04	- Breach of Indonesian Government systems a reason for them to increase their regulation of enforcement in IS	- Stronger government oversight in IS needed.
E	E-05-OE-05	- Lack of strong IS policies. Sensitive company files vulnerable to theft.	- Poor SMB implementation and oversight in IS
E	E-05-YE-05	None	None
A	A-01-YE-01	- IS awareness still low, particularly among the younger workers.	- Low SMB priority in IS - Low IS priority among younger workers

Table 22

Initial Code Generation for Opinion Responses (Question 13) (n=10)

SMB	Worker Code	Q13 - What are the differences or challenges to discuss or collaborate with older workers on IS?	Topics
A	A-01-OE-01	Question not asked to older workers	None
A	A-01-YE-01	- Older workers more responsible in IT/IS, vice younger workers who are more aloof about IS network policies. - IS competency more a product of skills and experience and not age	- Older workers more responsible in IS - Younger workers more aloof on IS - IS skills and knowledge more based on skills and experience, not age.
B	B-02-OE-02	Question not asked to older workers	None
B	B-02-YE-02	- Older workers slower in grasping IS concepts. - Older workers more dependent on IT/IS support.	- Older workers slower in grasping IS concepts - Older works dependent on IS/IT support.
C	C-03-OE-01	Question not asked to older workers	None
C	C-03-OE-02	- Older workers more forgetful on passwords - Older workers more IT/IS challenged - Older workers take more IS risks.	- Older workers more forgetful on passwords - Older workers more IT/IS challenged - Older workers take more IS risks.
D	D-04-OE-04	Question not asked to older workers	None
D	D-04-YE-04	- Older workers take more IS shortcuts - Older workers not as IS/IT literate/proficient. - Older worker slower to learn on IS/IT.	- Older workers engage in riskier IS practices - Older workers les IS proficient. - Older workers slower to learn IS.
E	E-05-OE-05	Question not asked to older workers	None
E	E-05-YE-05	Don’t know answer to question.	None

The participant responses were tabulated and developed into topics and sub-topics in Column D. At this stage, a pattern of similar responses in Column C emerged and tentative themes could already be conceived.

Phase 3: Searching for Themes

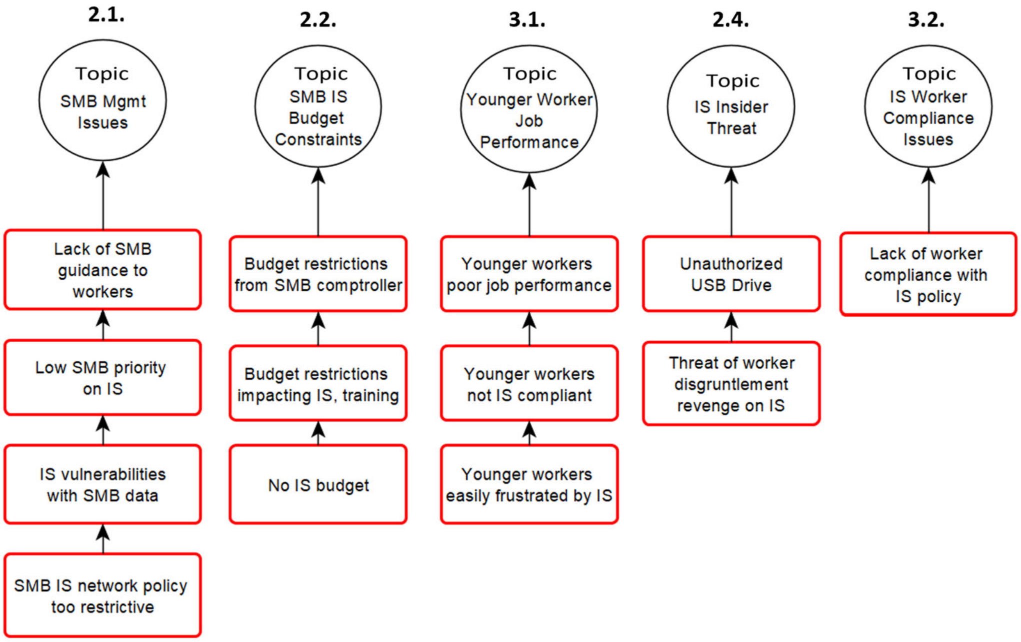
Data from participant interviews from questions 1 to 13 were carefully reviewed, analyzed, tabulated, and summarized as Tables 20, 21, 22 show. Analysis of these data revealed tentative themes based on recurring responses on similar topics. There were also diverging, converging, and overlapping topics, sub-topics and tentative themes which emerged from the data. As explained in Chapter 3, thematic mapping analysis served as an effective method to search through topics and sub-topics and explore for tentative themes. In the initial search for tentative themes, the following topics and sub-topics were identified from the participant responses:

1. Question 10: IS Challenges in the Workplace

Responses from Question 10 were captured in Table 20, rearranged, and categorized based on similar topics, and the consolidated as topics and sub-topics. Figure ten illustrates the result of this thematic analysis and mapping from Table 15. The initial outcome was five main topics: SMB Management Issues; SMB IS Budget Constraints; Younger Worker Job Performance; Insider Threat; and IS Worker Compliance Issues. A color-coding value was added to this thematic analysis to identify red as negative; green as positive; and blue as neutral. The numbers above the topics were the numerical coding assigned to each topic when the thematic map was finalized.

Figure 9

Thematic Mapping to Identify Potential Themes (Question 10)


2.1.
Topic
SMB Mgmt Issues
Lack of SMB guidance to workers
Low SMB priority on IS
IS vulnerabilities with SMB data
SMB IS network policy too restrictive
2.2.
Topic
SMB IS Budget Constraints
Budget restrictions from SMB comptroller
Budget restrictions impacting IS, training
No IS budget
3.1.
Topic
Younger Worker Job Performance
Younger workers poor job performance
Younger workers not IS compliant
Younger workers easily frustrated by IS
2.4.
Topic
IS Insider Threat
Unauthorized USB Drive
Threat of worker disgruntlement revenge on IS
3.2.
Topic
IS Worker Compliance Issues
Lack of worker compliance with IS policy

Note. Green = positive feedback; Red = negative feedback; Blue = neutral feedback

Several participants expressed dissatisfaction with the level of IS support and resourcing from their SMB Management which resulted in downgraded IS training, IS oversight, and compromised SMB IS and cybersecurity. Participants commented:

- Participant E-04-YE-04: “Lack of stricter IS governance and enforcement from management resulted in lax IS practices at the SMB. Workers are aware of this. IS oversights and mistakes that occur at work are therefore no surprise to workers.”
- Participant A-01-OE-01: “Requests for funding for IS training and development are rejected by SMB Management, downgrading the ability of our consultants to deliver better IS expertise and services to our customers.

Funding is instead prioritized for other SMB matters, such as business development."

- Participant A-01-YE-01: "Lack of funding support from SMB Management has resulted in no development in SMB cybersecurity systems and infrastructure, leading to SMB's compromised cybersecurity system."
- Participant A-01-OE-01 opined that SMB management do not place high priority or importance on IS awareness in the workplace until an IS incident, such as a security breach or data leak occurs, and then IS suddenly becomes a priority for the management. Participant A-01-YE-01 opined that non-IT and non-IS workers, regardless of their age category, lack IS serious awareness.
- Participant C-03-OE-03 opined that SMB Management network policies were too strict. The merits of this opinion, however, is subjective. Stricter network policy can offer stronger protection to the SMB. This participant did not, however, specify what aspects of the network policies were too strict. Participant E-04-YE-04 complemented her SMB Management in their rapid responses to IS incidents, and no news of IS incidents as 'good news' and testimony to the SMB's IT department doing their job.

Some participants stressed the importance of IS to their SMBs, whether the IS policies and technology were being implemented. Three participants (A-01-OE-0; A-01-YE-01; E-05-OE-05) stressed the importance of IS investment which was absent from their SMBs. Participant E-05-OE-05, for example, expressed concern with his SMB's lack of IS governance and technologies to protect their financial and contract documents and indicated that his SMB did not maintain IT staff or a dedicated IT department due to budget limitations. Participants A-01-OE-01 and A-01-YE-01 expressed their frustrations for repeated funding disapproval from the finance department for IS training for his subordinate IT staff and added that his SMB had become more vulnerable due to his IT staff's cybersecurity training deficiency.

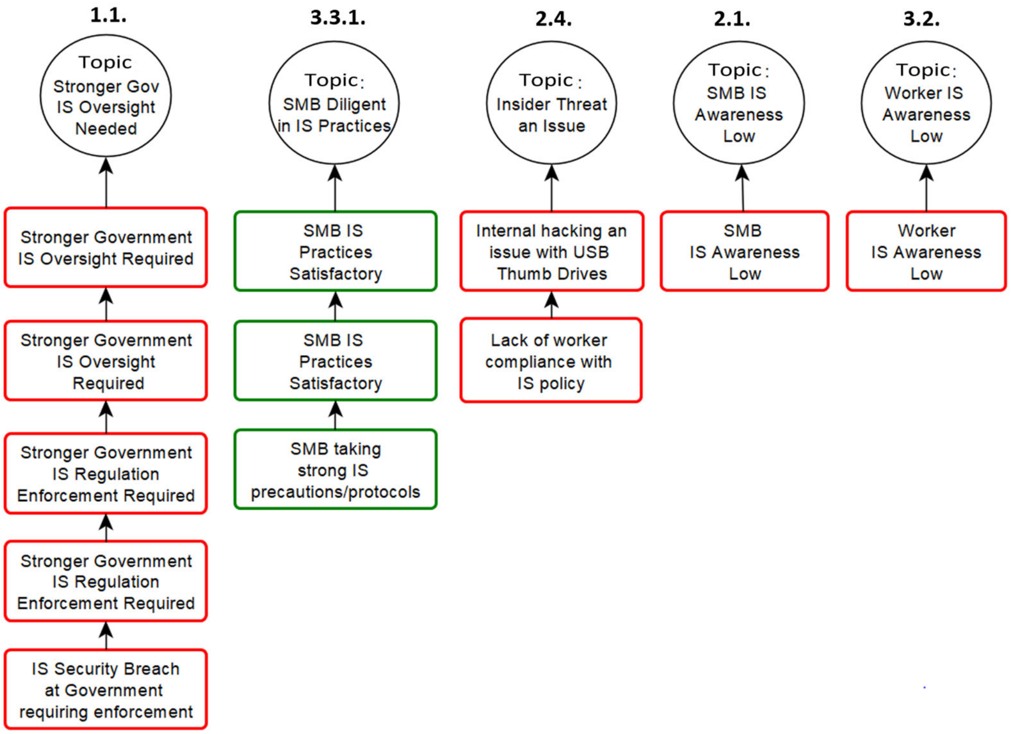
Indeed, findings on SMB budget constraints mirror the literature. Kabanda et al. (2018) indicated that SMBs consistently cited small budgets as a constraint to having stronger SMB cybersecurity mechanisms in place, echoing the complaints of participants of A-01-OE-01 and A-01-YE-01. Lack of management support due to financial resources and other competing projects reported by these participants was also indicated by Kabanda et al. (2018). Onwubiko and Lenaghan (2007) also indicated that a distinguishing factor in managing IS for small businesses is budget where small businesses work on limited budgets for IS compared to medium-sized businesses.

2. Question 11: SMB IS practices and Indonesian Government IS Oversight

Responses from Question 11 were captured in Table 21, rearranged, and categorized based on similar topics, and the consolidated as potential themes. Figure 11 presents the results of this thematic analysis and mapping from Table 21. The outcome was five topics: Stronger Indonesian Government IS Oversight Needed; SMB Diligent in IS Practices; Insider Threat an Issue; SMB IS Awareness Low; and Worker IS Awareness Low. What is apparent in this schema is the overlapping in topics with previous Question 10 theme map: Insider Threat, Worker IS Compliance and Awareness; and SMB IS Management overlapped with the same topics in Question 10. These topics and their converging themes will be consolidated in the final thematic analysis map.

Figure 10

Thematic Mapping Required to Identify Themes (Question 10)



Note. Green = positive feedback; Red = negative feedback; Blue = neutral feedback

Regarding Government IS Policy and Implementation, five participants (A-01-OE-01; A-01-YE-01; E-04-OE-04; E-04-YE-04; C-03-OE-03) indicated the need for increased government IS policy and oversight for SMBs and its workers. Participant E-04-YE-04 discussed a recent incident reported in the Indonesian media regarding the state-sponsored hacking incident of computer systems belonging to the Indonesian Government ministries and agencies, which included the Indonesian National Intelligence Agency (Badan Intelijen Nasional, also known as BIN) (Cimpanu, 2021). This participant cited this as proof for the need for the Indonesian Government to improve their national IS governance and oversight. This is also reflective of the literature which indicated that Indonesia users face significant cybersecurity challenges and lacks a strong cybersecurity history (Rahayu, 2018; Setiyawan, 2019). Rahayu (2018) also indicated that Indonesia is still at the developmental stage of national cybersecurity strategy, with legality of cybersecurity framework still weak, with no legal regulation and policies on cybersecurity oversight. Nugraha and Putri (2016) also indicated that Indonesia faces a multitude of ongoing cybersecurity challenges in establishing proper mechanism to coordinate across various ministries, agencies, and sub-national governments, which has resulted in Indonesia being vulnerable in its cybersecurity.

Regarding Insider Threat, participant A-01-OE-01 acknowledged a past IS breach with a former worker who used a USB thumb drive to exfiltrate sensitive data from the SMB. This incident resulted in ratcheted IS protocol and security standards in the SMB, which included issuing company laptops to workers with all the laptop data ports disabled, and mandating file encryption and password-protection for sensitive company files. Participant A-01-OE-01 added that all work-related computing had to be conducted on the company laptops without exception. Participant E-04-OE-04 indicated strict enforcement IS policy for his SMB, partially due to his concerns for insider threat from disgruntled employees seeking retaliation or revenge against the SMB. The participant did not elaborate on the background of his concern on this insider threat.

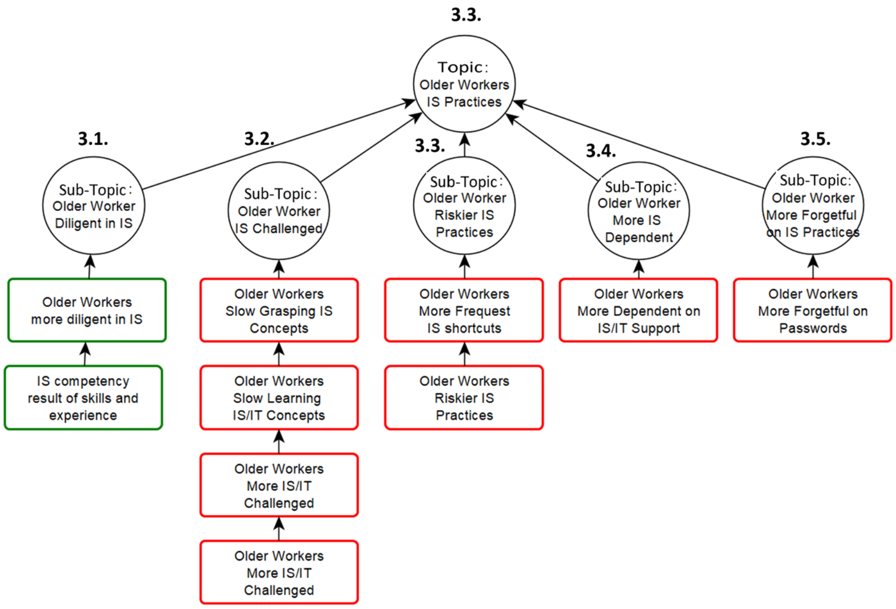
3. Question 13: Differences or challenges to discuss or collaborate with older workers on IS practices at work

Responses from Question 13 were captured in Table 21, re-arranged, and categorized based on topic and sub-topic similarity, then consolidated to the broader themes, based also on theme similarity. Figure 12 presents the result of this thematic analysis and mapping from Table 17.

The main topic was Older Worker IS practices which was divided by five sub-topics on older workers: Older Worker Diligent in IS; Older Worker IS Challenged; Older Worker Riskier IS Practices; Older Worker More IS Dependent; and Older Worker More Forgetful on IS Practices. What is noteworthy about this section is the frequency of critical remarks that the younger workers directed to their older co-workers which outweighed their complimentary remarks.

Figure 11

Thematic Mapping to Identify Potential Themes (Question 13)


3.3.
Topic: Older Workers IS Practices
3.1.
Sub-Topic: Older Worker Diligent in IS
3.2.
Sub-Topic: Older Worker IS Challenged
3.3.
Sub-Topic: Older Worker Riskier IS Practices
3.4.
Sub-Topic: Older Worker More IS Dependent
3.5.
Sub-Topic: Older Worker More Forgetful on IS Practices
Older Workers more diligent in IS
IS competency result of skills and experience
Older Workers Slow Grasping IS Concepts
Older Workers Slow Learning IS/IT Concepts
Older Workers More IS/IT Challenged
Older Workers More IS/IT Challenged
Older Workers More Frequest IS shortcuts
Older Workers Riskier IS Practices
Older Workers More Dependent on IS/IT Support
Older Workers More Forgetful on Passwords

Note. Green = positive feedback; Red = negative feedback; Blue = neutral feedback

Some younger worker dyads indicated older workers being slower to learn new IS technologies and less technically proficient. McCann and Keaton's (2013) found younger workers reinforcing negative stereotypes of older workers making more mistakes, being slower to adapt to new technology, and being more technology averse. Warr (1994) also reported a common tendency to view older workers as slower, less interested in new training, less flexible, and more likely to become weary compared to younger coworkers (as cited in Maurer et al., 2008). Additionally, Chiu et al.'s (2001) study on age discrimination practices in the U.K. and Hong Kong found Hong Kong workers more prone to negative age discrimination of their older co-workers.

In this research however, there appeared to be less of a divide in work habits between older and younger workers in the context of IS awareness and adherence. While some workers of both age groups had negative opinions of IS practices of their older and younger counterparts, both dyads of all SMBs appeared unified on the importance of protecting sensitive customer and company data.

As part of the design of the participant interview, one question was limited to the younger worker dyad to provide observation on older co-worker dyad on differences between them and older workers in their IS practices. Participant C-03-YE-03 stated that her older co-workers had more difficulty remembering passwords and had to repeat password information to them or resolve password issues more often than coworkers of her generation. She also indicated that more older workers had difficulty following technical IT instructions compared to younger coworkers. But she also indicated that other than these issues, there were no major differences in IS awareness and practices between older and younger workers at her SMB.

Participant A-01-OE-01 provided insightful feedback about younger co-workers in terms of their IS habits, practices, and attitudes at his SMB. He indicated that several younger ("millennial") coworkers tended to be aloof and more careless about IS protocol and mishandling sensitive data in their daily work habits. He opined that the carelessness and aloofness fit a pattern among his younger coworkers that were reflective of the millennial culture and lifestyle. In the literature, Cummings et al. (2012) found in IS breaches in organizations that in one-third of cases involving theft of personally identifiable information by insiders or external actors, younger workers were more often the perpetrators compared to older coworkers.

Feedback from older worker dyads (A-01-OE-01, B-02-OE-02, C-03-OE-03, E-04-OE-04, E-05-OE-05) gave no indication over concerns that the IS knowledge and skills of these older workers were inferior to their younger co-workers. Participant E-04-OE-04, the CEO of a Sports Medicine Company, stated the following regarding older worker IS practices: “Older workers tend to be more compliant on IS and learn from their IS mistakes or violations. After [older workers] commit an IS violation, they do not repeat it. Younger workers, on the other hand, continue to commit repeat IS violations after the same previous violations.” The participant’s opinion supports the literature regarding older worker and IS compliance. Dols (2009) indicated that in IT security policy practices in organizations, older workers were more compliance and familiar with IS policies, compared to their younger coworkers. Mutchler (2019) found that in IS security, older workers were less likely to misuse IS resources; less likely to engage in risky IS behaviors; and more likely to possess higher levels of IS awareness. Pahnila et al. (2007) indicated that among workers with knowledge of the organization’s security policies, older workers were likely to be more compliant. Li and Hoffman (2018) found age as a significant factor for IS compliance and that older workers were more likely to comply with organization IS policies than younger workers.

The focus of this research is on older workers at Indonesian SMBs, and the research questions were designed specifically with them in mind. Participants in the older worker category, however, contributed unsolicited opinions on their younger co-workers, who some of them referred to as ‘millennials’ and ‘Gen Z.’ While four older participants acknowledged younger workers at their SMB being generally more knowledgeable and proficient in IT, participants A-01-OE-01, A-01-YE-01, B-02-OE-02, and E-04-OE-04 opined the following:

- "Yes, younger workers are indeed more IT savvy, and we rely on them for their IT tech support, but they also tend to be less patient and become more easily frustrated with challenges in IT tasking, such as with system and data entry errors." (Participant: B-02-OE-02)
- "There is more of a lax work ethic and observance to IS protocol when it comes to our younger workers. They tend to ignore our IS protocols at the company, despite being aware of it." (Participant: A-01-YE-01)
- "Younger workers tend to be more aloof and dismissive of IS regulations at work compared to older workers." (Participant: A-01-OE-01)
- "Younger workers continue to violate IS protocols even after being advised or reminded. Whereas, with our older employees, once they are advised of an IS protocol violation, they are compliant and do not repeat it." (Participant: D-04-OE-04)

Regarding younger worker perception of older workers at SMBs, data showed multiple younger workers perceiving older co-workers to be fundamentally less literate or and competent in IS. Excerpts from younger participants (B-02-YE-02, C-03-YE-03, E-04-YE-04, D-03-YE-04, and E-04-YE-04) on older workers included the following:

- Participant B-02-YE-02: "Older workers are slower in grasping IS and IT concepts."
- Participant C-03-YE-03: "Older workers are not as literate or proficient in IS and IT."

- Participant E-04-YE-04: "Older workers depend on younger workers for technical support on IS and IT. For example, they have difficulty in encrypting and decrypting folders and files and need assistance from younger workers on this."
- Participant D-03-YE-04: "Older workers tend to be more forgetful on passwords for their IS habits. Passwords often need to be resent to them."
- Participant E-04-YE-04: "Older workers tend to bypass IS protocols for the sake of convenience due to their lack of technical knowledge."

From an aggregation of these responses, younger participants were mostly critical of older worker IS knowledge and competence. Stigma and negative stereotyping of older workers and their presumed lack of competence and ability in newer more complex disciplines, such as technology, as well as presumed decline in their ability to learn new disciplines and concepts, particularly new technology, is well documented in literature, with this study being no exception. There is significant research on stereotypical beliefs about older workers in Western societies (Tillsley 1990; Taylor and Walker 1998). Gringart et al. (2008) found that specific attributes where older workers were seen as inferior in comparison to younger workers which include trainability, adaptability, creativity, and interest in new technology. Peterson and Spiker (2005) stated that older workers are perceived to be unable to learn new technological changes; unable to keep pace; inflexible and unadaptable — but these are perceptions are flawed. McGregor and Gray (2002) stated that stereotypes about older workers related to individual characteristics such as poorer performance have only a limited factual basis.

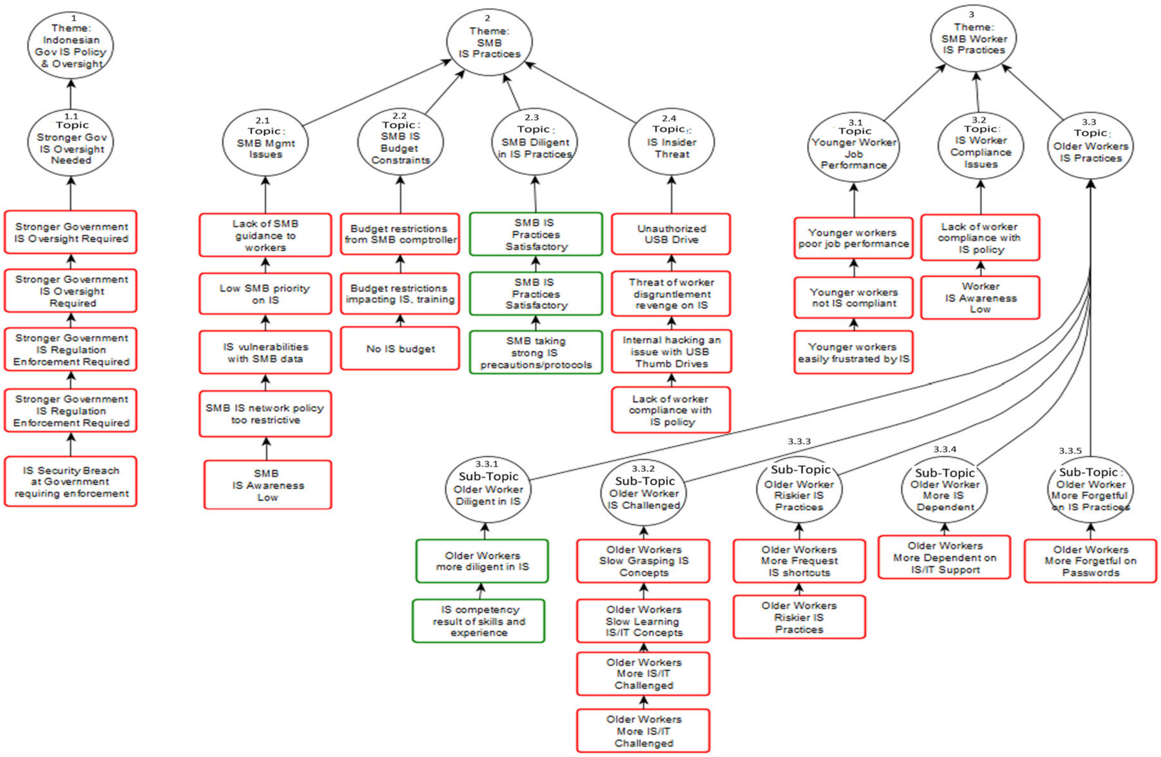
Regarding neutrality between older and younger worker IA knowledge, skills, and practices at SMBs, two participants, C-03-YE-03 and B-02-YE-02, from the younger worker category indicated there was no difference in IA knowledge and practices between older and younger workers. Participant B-02-YE-02 indicated that worker age or generation was not a determinant to superior or inferior IS Knowledge, Skills, and Abilities (KSAs), but rather the job function of the worker would influence their IS KSAs. For example, older workers who work at the IS department of their organization would be more knowledgeable and skilled in IS, relative to younger workers who do not work at the IS department.

Phase 4: Reviewing Themes

Between responses to questions 10, 11, and 13, there were overlapping topics that could be consolidated. Thematic maps 10, 11, 12 were subsequently analyzed against each other and topics and sub-topics were consolidated, and themes developed from the aggregate of the topics, and finally merged into one thematic map presented in Figure 13.

Figure 12

Consolidated Thematic Analysis Map Themes (Questions 10, 11, 13)



1 Theme: Indonesian Gov IS Policy & Oversight
1.1 Topic Stronger Gov IS Oversight Needed
Stronger Government IS Oversight Required
Stronger Government IS Oversight Required
Stronger Government IS Regulation Enforcement Required
Stronger Government IS Regulation Enforcement Required
IS Security Breach at Government requiring enforcement
2 Theme: SMB IS Practices
2.1 Topic: SMB Mgmt Issues
Lack of SMB guidance to workers
Low SMB priority on IS
IS vulnerabilities with SMB data
SMB IS network policy too restrictive
SMB IS Awareness Low
2.2 Topic: SMB IS Budget Constraints
Budget restrictions from SMB comptroller
Budget restrictions impacting IS, training
No IS budget
2.3 Topic: SMB Diligent in IS Practices
SMB IS Practices Satisfactory
SMB IS Practices Satisfactory
SMB taking strong IS precautions/protocols
2.4 Topic: IS Insider Threat
Unauthorized USB Drive
Threat of worker disgruntlement revenge on IS
Internal hacking an issue with USB Thumb Drives
Lack of worker compliance with IS policy
3 Theme: SMB Worker IS Practices
3.1 Topic Younger Worker Job Performance
Younger workers poor job performance
Younger workers not IS compliant
Younger workers easily frustrated by IS
3.2 Topic: IS Worker Compliance Issues
Lack of worker compliance with IS policy
Worker IS Awareness Low
3.3 Topic: Older Workers IS Practices
3.3.1 Sub-Topic Older Worker Diligent in IS
Older Workers more diligent in IS
IS competency result of skills and experience
3.3.2 Sub-Topic Older Worker IS Challenged
Older Workers Slow Grasping IS Concepts
Older Workers Slow Learning IS/IT Concepts
Older Workers More IS/IT Challenged
Older Workers More IS/IT Challenged
3.3.3 Sub-Topic Older Worker Riskier IS Practices
Older Workers More Frequest IS shortcuts
Older Workers Riskier IS Practices
3.3.4 Sub-Topic Older Worker More IS Dependent
Older Workers More Dependent on IS/IT Support
3.3.5 Sub-Topic: Older Worker More Forgetful on IS Practices
Older Workers More Forgetful on Passwords

Note. Green = positive feedback; Red = negative feedback; Blue = neutral feedback

2. Phase 5: Defining and Naming Themes

In the consolidated thematic mapping in Figure 13, patterns and commonalities in topics emerged from the data. The topics were arranged into a hierarchical taxonomy of sub-topics, topics, and then overarching themes. Codes were assigned to each theme, topic, and sub-topic in this taxonomy.

Based on this thematic mapping analysis, the research topic of IS practices of SMBs in Indonesia ultimately centered around the IS practices of IS workers; the management practices of the SMBs; and SMB IS policy and governance by the Indonesian Government. These three main themes are represented in Figure 13 as items 1, 2, and 3, and its categorizations were the result of aggregation of topics 1.1. to 3.3., and under topic 3.3, sub-topics 3.3.1. to 3.3.5.

The description of themes, topics, and sub-topics of the Figure 13 thematic map and its taxonomy is as follows:

1. Theme - Indonesian Government IS Policy & Oversight:

   Aggregated participant feedback related to SMB IS policy and governance from the Indonesian Government. All participant feedback related to their views and opinions on IS policy and governance for SMBs by the Indonesian Government were designated to a topic under this overarching theme.

   1.1. Topic - Stronger Government IS Oversight Needed:

      Aggregated participant feedback related to the need for stronger government IS oversight and governance for SMBs. This participant feedback was a consensus in that no participant disagreed that the Indonesian Government needed to be more proactive and involved in IS governance and support on a national level for its SMBs.

      Exemplar quote: “SMBs need stronger government guidance, oversight, and support.”

2. Theme: SMB IS Practices: Aggregated participant feedback related to IS practices at SMBs. All participant feedback related to their views and opinions on SMB IS practices were categorized in topics and sub-topics under this overarching theme.

   2.1. Topic - SMB Management Issues:

   Aggregated participant feedback related to SMB management issues and concerns.

   Exemplar Quote: "IS is not an important priority for the SMB."

   2.2. Topic - SMB IS Budget Constraints:

   Aggregated participant feedback related to SMB budget issues and constraints with IS spending.

   Exemplar Quote: "There is lack of SMB budget support for IS assets and training."

   2.3. Topic - SMB Diligent in IS practices:

   Aggregated participant feedback related to diligence in IS practices and implementation by SMB management.

   Exemplar Quote: "SMB Management is competent, as there have been no reported IS incidents or issues."

   2.4. Topic - IS Insider Threat:

   Aggregated participant feedback related to insider threat IS incidents or potential incidents.

   Exemplar Quote: "There have been insider IS threats from workers such as data theft via USB thumb drives."

3. Theme - SMB Worker IS Practices:

Aggregated participant feedback related to the IS practices of SMB workers. All participant feedback related to their views and opinions on SMB worker practices were placed under topics under this overarching theme.

3.1. Topic - Younger Worker Job Performance:

Aggregated participant feedback related to the IS job performance and practices of younger workers at SMBs.

Exemplar Quote: "Younger workers tend to be less compliant with IS policies, and are more aloof in their work ethic, which reflects in their IS practices."

3.2. Topic - IS Worker Compliance Issues:

Aggregated participant feedback related to worker issues in IS compliance.

Exemplar Quote: "IS compliance is a problem among SMB workers."

3.3. Topic - Older Worker IS Practices:

Aggregated participant feedback related to IS job performance and practices of older workers.

3.3.1. Sub-Topic: Older Worker Diligent in IS:

Aggregated participant feedback related to older worker positive performance and practices in IS.

Exemplar Quote: "Older workers tend to learn from their IS mistakes, and do not repeat them, unlike younger workers who repeat their IS mistakes."

3.3.2. Sub-Topic: Older Worker IS Challenged:

Aggregated participant feedback related to older worker challenges with IS.

Exemplar quote: "Older workers are more technically-challenged and slower to learn IS."

3.3.3. Sub-Topic: Older Worker Riskier IS Practices:

Aggregated participant feedback related to risky IS practices by older workers.

Exemplar Quote: “Older workers tend to engage in riskier IS practices.”

3.3.4. Sub-Topic: Older Worker More IS Dependent:

Aggregated participant feedback related to older worker dependence on other (younger and/or more IS-proficient) co-workers to perform IS tasks or resolve IS issues.

Exemplar Quote: “Older workers depend more on younger co-workers or the IT Department for IS support.”

3.3.5. Sub-Topic: Older Worker More Forgetful on IS Practices:

Aggregated participant feedback related to older worker tendency for forgetfulness in IS (and perhaps other as well) tasks and matters.

Exemplar Quote: “Older workers tend to forget their IS passwords more easily.”

Summary

This chapter began with a brief review of the research methodology and methods described in Chapter 3 that were implemented in the participant interviews and subsequent data consolidation, analysis, theme development and reporting. Yin's qualitative research methods combined with Moustakas’ heuristic philosophy were central to the implementation of participant interviews and data collection in this phase of the research.

Following discussion of research methods, this chapter documented the details of the proceedings of the interviews with the participants. Areas of interests and challenges that the researcher encountered during the interviews were also presented. The process of reviewing, translating, and analyzing the participant interview data was discussed.

The process of coding the participant interview data and separating the participant interview response data into categories, then assigning them into common sub-topics, topics, and themes, via tabulation of frequency in recurring topic instances, were detailed in this section. After the themes were identified, they were further discussed and elaborated in this section.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

In this chapter, conclusions are organized by each of the seven research questions followed by key findings from the thematic analysis. Next, an explanation of what these conclusions mean within a broader context are discussed as implications of this research. Recommendations for future research are provided followed by a summary of the study.

Conclusions

The first goal of this research was to assess what older workers at Indonesian SMBs do to acquire, apply, and share IS countermeasures aimed at mitigating cyberattacks. The second goal was to assess if and how younger workers share information security countermeasures with their older colleagues. Following are the seven research questions and their responses based on the findings that were reported in Chapter 4.

Research Question 1: What countermeasures are currently in place in Indonesian SMBs to mitigate cyberattacks? Indonesian SMBs used multiple methods, often in concert, to protect themselves from potential cyberattacks and insider threats. The most common methods reported included password-protection on folders and files; antivirus software; server firewalls; network URL blocking; and computer port blocking. Lesser used methods included two-factor authentication (2FA); MS-Windows folder permissions; company-issued laptop computers; and worker-only password-protected Wi-Fi. Additional countermeasures included SMB policy for worker situational awareness against social-engineering threats, which was not to discuss sensitive company topics in public areas such as break rooms and work cafeterias.

Research Question 2: How do older workers acquire information on IS countermeasures? Older and younger workers were alike in their acquisition of information and countermeasures in their SMBs. All SMBs that maintained an IS program delivered information and training on IS countermeasures to all employees. Older workers mainly acquired information on IS countermeasures from their SMB through periodic training and IS alerts and advisories. Trainings were held mostly via a virtual class or webinar and e-learning with one participant noting self-initiated learning. There were no in-person classes (likely due to government and workplace restrictions under the COVID-19 pandemic).

Research Question 3: How do older workers apply IS countermeasures to protect their organizations? Most older workers used password-protected file and folder encryption are their primary security countermeasure. The workers would transmit the passwords to their recipients through separate channels, such as e-mails, WhatsApp, or SMS text messages. Additional security countermeasures older workers implemented were to lock computer workstations when leaving the workstation or office during breaks or at the close of business day. No differences were found in the IS countermeasure practices between older and younger workers.

Research Question 4: How do older workers share their knowledge and skills related to cybersecurity countermeasures with other employees in their SMB? Older workers shared their knowledge and skills related to IS and cybersecurity countermeasures with all SMB co-workers verbally and via text-messaging such as WhatsApp first, SMS second, and e-mail third. Cybersecurity countermeasure information is, according to this study, shared mostly by the SMB IT/IS departments with all workers via e-mail, and if urgent, via WhatsApp and SMS text-messages. According to this research, the SMB is therefore the central source of cybersecurity information and guidance for all workers young and old.

Research Question 5: What knowledge related to cybersecurity countermeasures do older workers hide from younger employees in their SMB? No indication was found that younger workers hide cybersecurity countermeasure knowledge from their older colleagues. Older and younger SMB workers appeared to share cybersecurity measures freely and transparently with each other as a collective obligation and responsibility as employees of the SMB.

Research Question 6: How do younger workers share cybersecurity countermeasures with older workers? Younger workers share their knowledge and skills related to cybersecurity countermeasures with co-workers in their organization verbally via word-of-mouth, and via text-messaging applications such as WhatsApp and SMS, and e-mail. According to this study, younger works did not age-discriminate with co-workers in their cybersecurity information-sharing.

Research Question 7: What knowledge related to cybersecurity countermeasures do younger workers hide from older employees in their organization? There was no indication that older workers hid cybersecurity countermeasure knowledge from their younger colleagues. Older and younger SMB workers appeared to share cybersecurity measures freely with each other as a collective obligation and responsibility as workers of the SMB, presumably to protect their SMB, their co-workers, and their employment.

Key Findings

In addition to the responses to the research questions, following are key findings based on the thematic analysis of the data:

Older SMB workers in Indonesia share IS countermeasures in the same way as their younger coworkers. This research found that Indonesian SMBs enforce IS governance and oversight, and deliver IS training to all their workers through federated channels — regardless of age, gender, or other discriminators of their workers. In cases where SMB IS policy, procedures, or guidance were unclear or absent, this study also found no observable difference between older and younger workers in their IS countermeasure practices.

Older and younger workers mostly received SMB IS training via online video teleconferencing platforms and self-paced computer training. SMBs delivered IS threat-mitigation advisories and alerts, such as virus and service interruption notices mainly via WhatsApp instant messaging (IM) and SMS text-messaging. For decryption of SMB files and folders that were transmitted in close parallel via e-mail or File Transfer Protocol (FTP), SMBs transmitted file and folder decryption passwords mainly via WhatsApp and SMS. Older workers acquired and applied these protocols in their IS practices at SMBs in the same manner as their younger co-workers.

In SMB data security, older workers applied SMB-directed method of file encryption when sending and exchanging data between workers in the SMB and with clients. Several older SMB workers underscored the importance of data security to their SMBs. Older Workers in IT Management positions who had decision-making influence over IS policy applied IS safety protocols for their SMBs, such as file encryption, role-based access to shared folders on networks, blocking of ports on computers, and Wi-Fi password access and blocking of unauthorized sites.

No indication of knowledge-hiding activity was observed or reported among the SMB workers interviewed for this study, including younger workers and their older co-workers. Older and younger SMB workers appeared to exhibit a collaborative and transparent work culture in their IS practices.

This study found highly collaborative and collegial work relationships between both older and younger workers without semblance or reporting from participants on knowledge-hiding practices. IS appeared to be a collective concern and priority for all employees of an organization, and that knowledge-hiding as a form workplace competitiveness was set aside for the collective good of the SMB.

One question that emerged from this research observation was whether IS was a field that would be less prone to knowledge-hiding among workers compared to other fields such as sales and marketing, where workers can gain additional commissions and profits by withholding customer information leads from co-workers, which can drive knowledge-hiding behavior. Vinoa and Nastiti (2020) showed how personal competitiveness of employees in an Indonesian sales department lead to a high tendency of knowledge-hiding, while job function dependency had a moderating effect on knowledge-hiding. There is the tendency for knowledge hiding to occur in more competitive work environments. Sofyan and De Clercq (2021) also indicated how excessive work pressures could lead employees to conceal valuable knowledge and how this risk can be subdued by an organizational culture that avoids a strict focus on performance comparisons across employees.

The SMBs that were part of this study were: IT Consulting, Life Insurance, Construction, Sports Medicine, and Corporate Social Responsibility Consulting. The participants of these SMBs did not appear to possess jobs involving sales commissions and profits or performance-based competition that were tied to IS. Although worker commissions through sales of Life Insurance SMB may exist and encourage knowledge-hiding of prospective customers among the

SMB's Sales Agents; in this case however, the participants interviewed were workers from the Human Resource department of the Life Insurance SMB, thereby possibly mitigating knowledge-hiding behaviour, and in addition, IS unlikely being a strong driver of knowledge-hiding behaviour.

"Older workers are more technically-challenged and slower to learn IS."

While not the focus of this study, multiple younger SMB workers mentioned deficiency in IS skills, competency, and learning abilities of their older co-workers. Older and younger workers at the SMBs presented a collegial and unified front in IS knowledge-sharing and compliance, but the dynamic was not the same during one-to-one interviews with the participants; several younger workers candidly opined on shortcomings of the IS knowledge, skills, and abilities of their older coworkers. The younger-worker IS criticism toward older workers included: difficulties that older workers encountered in encrypting and decrypting files; poor memory recollection of passwords; slower grasp of IS concepts; riskier IS practices stemming from lack of IS knowledge and competency. The findings of this research partly corroborate literature regarding the stigma older workers often face with being perceived as less technically knowledgeable and competent, and slower to learn new technologies at work in comparison to their younger co-workers.

Findings emerged from this research which appeared to both corroborate and differ from the literature on older workers. This study indicated how SMB broadcasted IS training to its workers which did not discriminate against workers based on age or other denominations. Older SMB workers shared IS knowledge with co-workers no different than other workers. Contributing to this is the current state of technology which facilitates ease of delivery of IS requirements and training via online channels, such as audio and video teleconferencing and

VOIP text-messaging, which appears ubiquitous in Indonesian offices, and consumed by its workers.

Whether related to transparency in SMB IS requirements and training delivery, this study also found no observed or reported knowledge-hiding between older and younger workers. This research did not dismiss the possibility that the absence in knowledge-hiding and IS transparency could be tied to little to no financial, job, or career incentive that could be gained from knowledge-hiding, specifically in the field of IS when compared to other fields and industries where a worker's competitive advantage can be gained from hiding knowledge or information from co-workers.

The findings of this study also corroborated literature regarding stigma and conjecture of older workers being more technically-challenged and slower to learn IS, IT, and technology in general, compared to younger workers. The negative stereotyping of older worker and technology presented in this study as well.

While the focus of this research was on older workers and their IS practices at Indonesian SMBs, unanticipated themes emerged from the data during the course of the thematic analysis that needed to be shared. Several themes came to light regarding SMBs and its workers in Indonesia. First, the core of successful IS implementation at Indonesian SMBs appears to be the level of IS knowledge, competence, and skill of its workers; the level of competent IS leadership and support from SMB management, specifically IS competency and dedicated funding support; and to a more distant degree but still no less important, government IS policy oversight and support.

Implications

This research sought to assess what older workers at Indonesian SMBs do to acquire, apply, and share IS countermeasures to mitigate cyberattacks. It also sought to determine whether younger workers share IS countermeasures with their older coworkers. The research was accomplished by interviewing older and younger workers at Indonesian SMBs and collecting data from the interviews and conducting qualitative analysis through thematic mapping to address the problem statement and research questions of this study.

An important contribution of this research is that it provides valuable empirical data on direct views and opinions from workers at Indonesian SMBs. At the onset of this research, there was no known precedent on this particular research topic. This study contributes to the body of knowledge and future research on topics that include IS and cybersecurity practices and work culture among workers at Indonesian SMBs.

This study also sheds light on knowledge-hiding practices in Indonesian organizations within the context of the broad assumptions versus the realities of knowledge-hiding practices. The absence of knowledge hiding practices that were observed and documented in this research offers evidence that challenges literature reporting the pervasiveness of knowledge-hiding practices in organizations. Work cultures, as this research shows, also have the capability for goodness and to be devoid of unhealthy knowledge-hiding practices.

This research also challenges broad conjecture of the declining work spirit and productivity of the aging older worker at the twilight of their career and nearing their retirement mark. This conjecture is pronounced in some regions of the world where slowing down in preparation of retirement for the older worker is an expected cultural and societal decorum. On the contrary, this study has shown that through IT-powered training (e.g., video teleconferencing, webinars, LMS, etc.) and information dissemination on subject matter (such as IS in this case), this can energize and break down barriers between older and younger workers, and build their Knowledge, Skills, and Abilities (KSAs) democratically and agnostic of worker age. The study showed vibrant older workers responding to questions on IS practices at their SMBs in equal knowledge and confidence, notwithstanding ageist criticism from some of their younger workers.

This study also reinforces the cause for Security, Education, Training, and Awareness (SETA) implementation in developing countries to discourage IS misuse (D'Arcy et. al, 2009). This study presented the important role of SETA in raising awareness in safe IS practices at Indonesian SMBs. Most SMBs in this study implemented IS training programs which enhanced the IS knowledge, skills, and awareness of its workers. Some SMBs enacted strict penalties for worker violations of IS policy, which were promulgated through their IS training channels. Although this study did not measure the success of the IS training programs at these Indonesian SMBs, the clarity in responses and recollection from the workers on details of their IS training programs, and their clarification on the importance of safeguarding sensitive company and customers data, suggests that post-training IS awareness was enhanced as a result. D'Arcy et. al (2009) also recommended for organizations to dedicate more resources to support SETA programs to reinforce deterrence of IS misuse. Notably in this research, some SMB workers in this study protested the lack of funding from SMB management for IS and cybersecurity training for the IS workers and indicated that this training gap equated to a compromise in IS protection of the SMB. This study supports the case that resourcing and implementation of SETA programs at SMBs can be beneficial in raising IS awareness of its workers.

Recommendations

This study raises several opportunities and possibilities for future research in IS and cybersecurity and knowledge-hiding practices at Indonesian organizations. For example, regarding the knowledge-hiding practices in IS that was not found in this study, a different study could be conducted at Indonesian SMBs where profit or professional advantage can be gained by hiding knowledge and information from co-workers. Indeed, more research and refinement will be needed for this type of study.

It was evident from the aggregate response from the Indonesian SMB workers that budget restrictions on IS and lack of management prioritization of IS were obstacles to more effective implementation of IS at the SMBs. Without more accurate visibility of budgets and resourcing that SMBs have to commit to investment in building of IS/cybersecurity capability and training of its workers, it would be difficult to make recommendations on IS budget spending. Additionally, a cybersecurity impact study may need to be conducted on SMBs to assess cybersecurity compromises and vulnerabilities that are at risk as the result of the lack or absence in the SMB’s investment in their cybersecurity capacity building and training for their workers. This study therefore recommends cybersecurity vulnerability impact and threat assessments to be conducted on SMBs that the workers point to as lacking spending in their cybersecurity protection and worker training. The results of cybersecurity vulnerability impact and threat assessments that are presented to SMB managements that underspend on their cybersecurity may become an effective change agent to their future cybersecurity spending and investment.

In response to the negative views and criticism that some younger workers opined against their older co-workers in IS competence, knowledge, and agility, this study also proposes the need for an emphasis on organizational team-building skills among older and younger workers to mitigate negative perceptions and animus between the two age or generation groups and build bridges as pathway to enhance cybersecurity productivity and effectiveness at SMBs.

Limitations

Several limitations in this study were evident. First, this research was originally planned as an on-site study in Jakarta, Indonesia, where interviews would be conducted in-person with the participants. The COVID-19 pandemic, however, changed this, and participant interviews had to instead be conducted via Zoom and WhatsApp video teleconference between the researcher in Washington D.C. and the participants in Jakarta. While the Zoom interviews still managed to capture and extract significant data from the participants, it would not have measured up against face-to-face interviews with the participants, which would have captured significantly more details and nuances that were lost with the video teleconference platform.

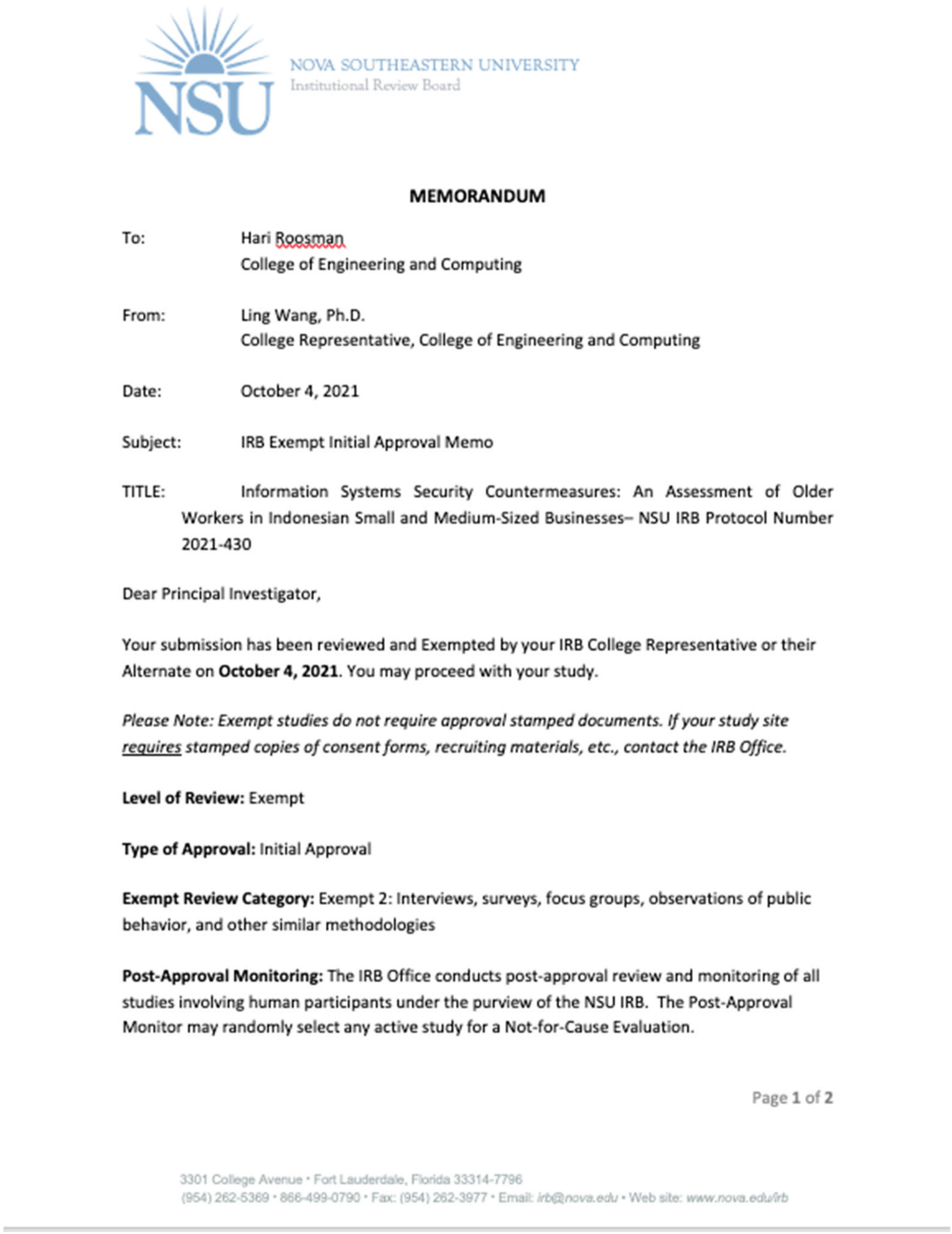
This research would have benefited significantly with a sample size larger than its final n=10 participants with five dyads. The sample size of n=30 with 15 dyads would have been richer with more granular detail and nuance from the wider range of participants and SMBs. Despite this, this research still managed to extract significant data and findings with its limited sample. This larger sample of n=30 would, however, have demanded more research time and resources, which meant that the study would have also taken longer to complete. It is unknown whether this additional research time would have been available for the researcher, as the n=10 sample study itself took two semesters or about eight months to complete; a n=30 sample would, on the other hand, have most likely taken significantly more time to complete. Nevertheless, the larger data sample would have likely resulted in a richer and more comprehensive study. As such, it is hoped that this study can serve as a springboard for future research with larger resources in research time and effort. Therein lies an additional limitation of this study in that there was no previous study like this that could be used as a research precedent to be further developed and built upon. It is also hoped that this study can in the future be replicated in-country through face-to-face interviews with SMB workers, as this would realize the original intent and aspiration of this research effort.

Summary

This study began with a research goal to assess what older workers within Indonesian SMBs do to acquire, apply, and share IS countermeasures aimed at mitigating cyberattacks, and to assess if and how younger workers share information security countermeasures with their older colleagues. The original plan was to conduct this research in-country in Jakarta, Indonesia, but was cancelled due to the travel restrictions enacted by the Indonesian Government in response to the COVID-19 pandemic. Instead, the research was diverted and conducted remotely via video teleconferencing with older and younger worker dyads at SMBs in Jakarta, Indonesia. Sixteen SMB workers agreed to be interviewed as participants of this research, and the interviews were conducted with them between September and November 2021. The data from ten of the 16 interviews with workers were subsequently reviewed, translated to English, and codified, which would become the basis of this research. The coded data from the participant interviews were then analyzed and elaborated in the context of the research topic and questions.

Using a thematic data analysis process, the data were organized into three main themes including 1) Indonesian government IS policy and oversight, which included one topic (stronger government IS oversight needed); 2) SMB IS practices, which included three topics (SMB management issues, SMB budget constraints, SMB diligent IS practices, and IS insider threat); and 3) SMB worker IS practices, which included three topics (younger worker job performance, IS worker compliance issues, older worker IS practices) and five sub-topics under older worker IS practices (older worker diligent in IS, older worker IS challenged, older worker riskier IS practices, older worker more IS dependent, and older worker more forgetful on IS practices). This analysis assisted in responding to the research questions and key findings. Implications, recommendations for future research, and limitations of this study were presented at the conclusion of this dissertation.

Appendix A: Nova Southeastern University IRB Exempt Initial Approval Memo



NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: Hari Roosman
College of Engineering and Computing

From: Ling Wang, Ph.D.
College Representative, College of Engineering and Computing

Date: October 4, 2021

Subject: IRB Exempt Initial Approval Memo

TITLE: Information Systems Security Countermeasures: An Assessment of Older Workers in Indonesian Small and Medium-Sized Businesses– NSU IRB Protocol Number 2021-430

Dear Principal Investigator,

Your submission has been reviewed and Exempted by your IRB College Representative or their Alternate on **October 4, 2021**. You may proceed with your study.

Please Note: Exempt studies do not require approval stamped documents. If your study site requires stamped copies of consent forms, recruiting materials, etc., contact the IRB Office.

Level of Review: Exempt

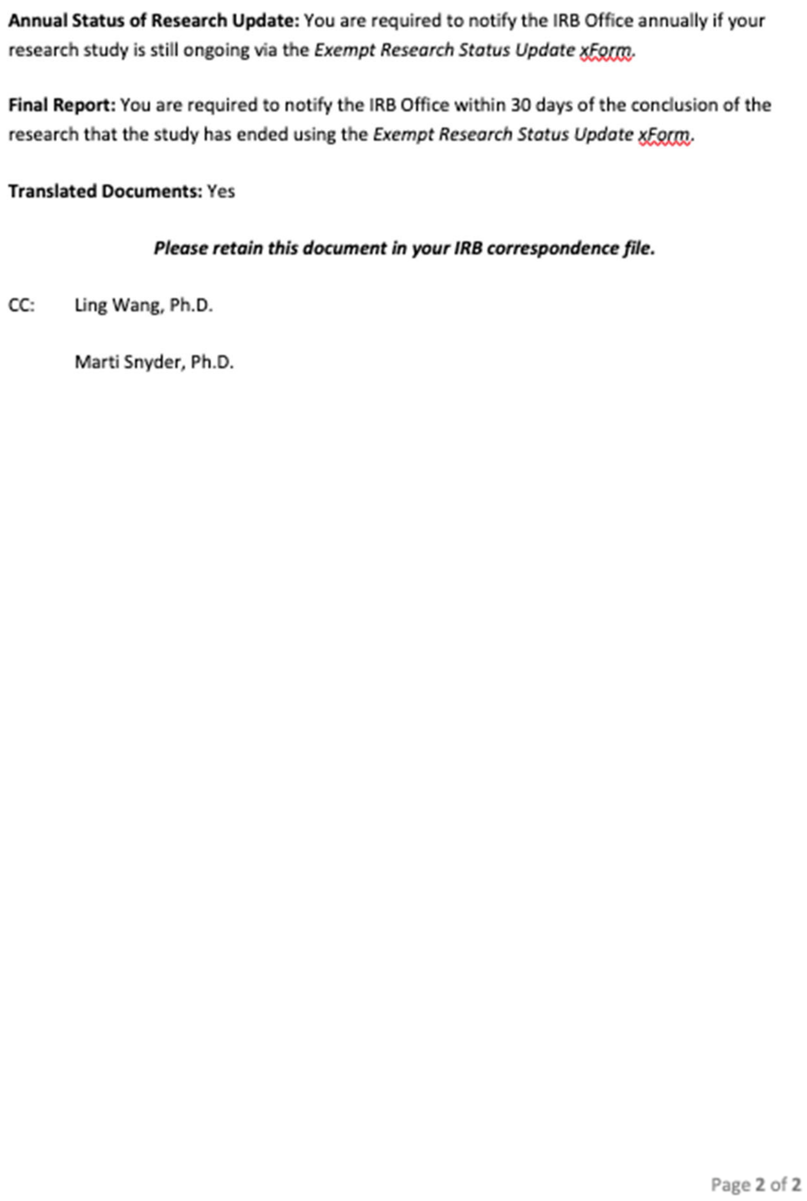
Type of Approval: Initial Approval

Exempt Review Category: Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies

Post-Approval Monitoring: The IRB Office conducts post-approval review and monitoring of all studies involving human participants under the purview of the NSU IRB. The Post-Approval Monitor may randomly select any active study for a Not-for-Cause Evaluation.

Page **1** of **2**

3301 College Avenue • Fort Lauderdale, Florida 33314-7796
(954) 262-5369 • 866-499-0790 • Fax: (954) 262-3977 • Email: *irb@nova.edu* • Web site: *www.nova.edu/irb*



Annual Status of Research Update: You are required to notify the IRB Office annually if your research study is still ongoing via the *Exempt Research Status Update xForm.*

Final Report: You are required to notify the IRB Office within 30 days of the conclusion of the research that the study has ended using the *Exempt Research Status Update xForm*.

Translated Documents: Yes

Please retain this document in your IRB correspondence file.

CC: Ling Wang, Ph.D.

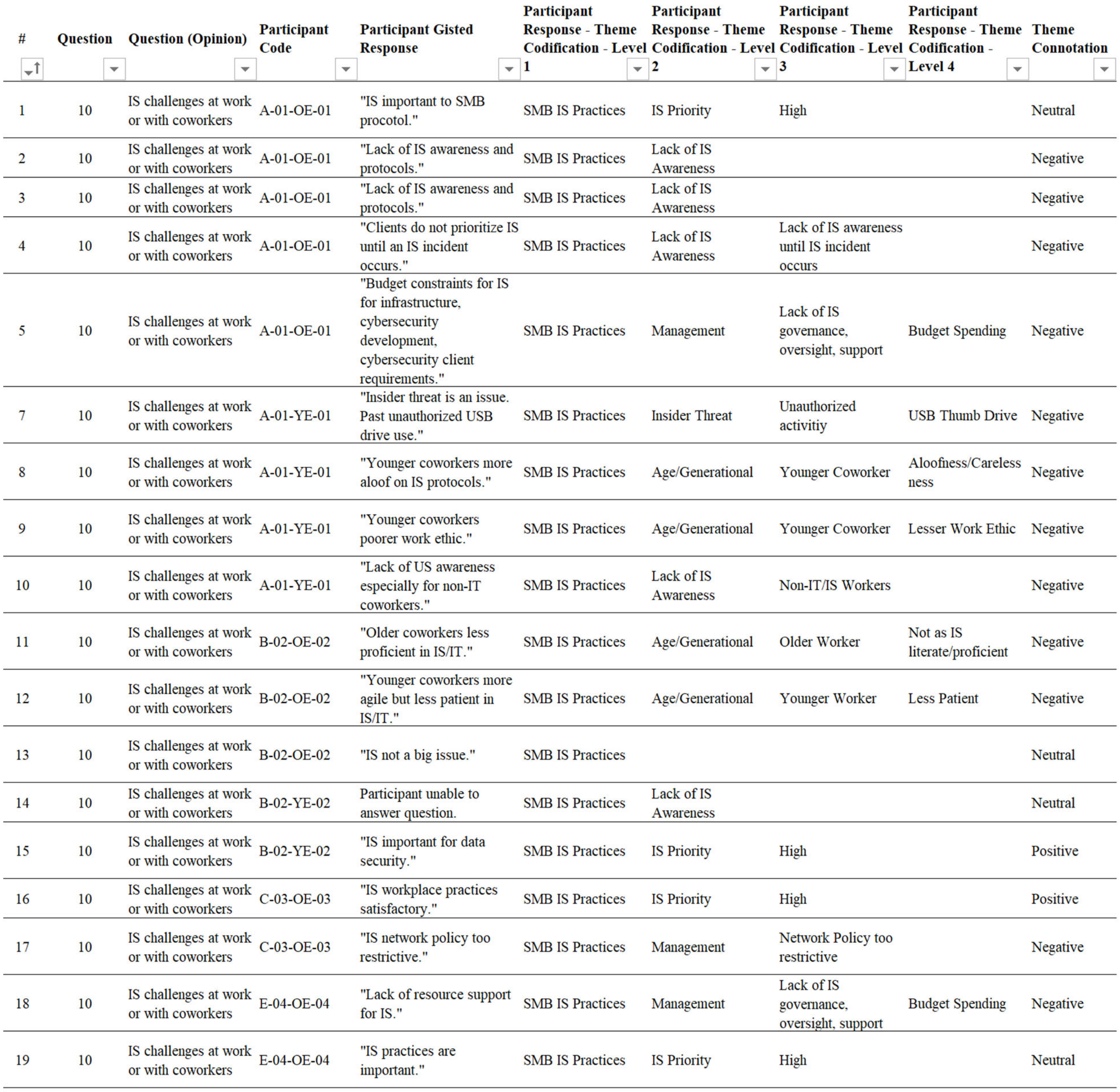
Marti Snyder, Ph.D.

Appendix B: Mandatory Retirement Ages of Indonesian Workers

	Occupation Classification	Mandatory Retirement Age	Indonesian Labor Law
1	Private Sector	56	Pasal 3 ayat 2 PP No. 32 Th 1979 tentang Pemberhentian Pegawai Negeri Sipil, yang diubah menjadi PP No. 65 tahun 2008
2	Research	65	Pasal 1 PP No. 65 tahun 2008
3	College Professor	65	Pasal 67 ayat 5 UU No.4 tahun 2005 tentang Guru dan Dosen
4	Lecturer	65	Pasal 40 ayat 4 UU No.4 tahun 2005 tentang Guru dan Dosen
5	Teacher	60	
6	Police Officer	58	Pasal 30 ayat 2 UU No. 2 tahun 2002 tentang Kepolisian Negara Republik Indonesia
7	Police Officer w/ Expertise	60	
8	Military Officer	58	Pasal 75 UU No. 34 tahun 2004 tentang Tentara Nasional Indonesia
9	Military Enlisted	53	
10	Judge	62	Pasal 12 UU No. 16 tahun 2004 tentang Kejaksaan Republik Indonesia
11	Government – Echelon 1	60	Pasal 1 PP Nomor 65 Tahun 2008 tentang perubahan kedua atas PP No.32 tahun 1979 tentang Pemberhentian Pegawai Negeri Sipil
12	Government – Echelon 2	60	
13	Government – Echelon 1 w Strategic Role	62	
14	School Inspector	60	Pasal 1 PP Nomor 65 Tahun 2008 tentang perubahan kedua atas PP No.32 tahun 1979 tentang Pemberhentian Pegawai Negeri Sipil
15	Judge	58	
16	Special Presidential Appointment	58	
17	Laborer	At discretion of PK, PP, PKB	Pasal 154 UU No. 13 tentang Tenaga Kerja

Source: Gajimu (2021)

Appendix C: Participant Interview Translated and Gisted Response Data



#	Question	Question (Opinion)	Participant Code	Participant Gisted Response	Participant Response - Theme Codification - Level 1	Participant Response - Theme Codification - Level 2	Participant Response - Theme Codification - Level 3	Participant Response - Theme Codification - Level 4	Theme Connotation
1	10	IS challenges at work or with coworkers	A-01-OE-01	"IS important to SMB procotol."	SMB IS Practices	IS Priority	High		Neutral
2	10	IS challenges at work or with coworkers	A-01-OE-01	"Lack of IS awareness and protocols."	SMB IS Practices	Lack of IS Awareness			Negative
3	10	IS challenges at work or with coworkers	A-01-OE-01	"Lack of IS awareness and protocols."	SMB IS Practices	Lack of IS Awareness			Negative
4	10	IS challenges at work or with coworkers	A-01-OE-01	"Clients do not prioritize IS until an IS incident occurs."	SMB IS Practices	Lack of IS Awareness	Lack of IS awareness until IS incident occurs		Negative
5	10	IS challenges at work or with coworkers	A-01-OE-01	"Budget constraints for IS for infrastructure, cybersecurity development, cybersecurity client requirements."	SMB IS Practices	Management	Lack of IS governance, oversight, support	Budget Spending	Negative
7	10	IS challenges at work or with coworkers	A-01-YE-01	"Insider threat is an issue. Past unauthorized USB drive use."	SMB IS Practices	Insider Threat	Unauthorized activitiy	USB Thumb Drive	Negative
8	10	IS challenges at work or with coworkers	A-01-YE-01	"Younger coworkers more aloof on IS protocols."	SMB IS Practices	Age/Generational	Younger Coworker	Aloofness/Careless ness	Negative
9	10	IS challenges at work or with coworkers	A-01-YE-01	"Younger coworkers poorer work ethic."	SMB IS Practices	Age/Generational	Younger Coworker	Lesser Work Ethic	Negative
10	10	IS challenges at work or with coworkers	A-01-YE-01	"Lack of US awareness especially for non-IT coworkers."	SMB IS Practices	Lack of IS Awareness	Non-IT/IS Workers		Negative
11	10	IS challenges at work or with coworkers	B-02-OE-02	"Older coworkers less proficient in IS/IT."	SMB IS Practices	Age/Generational	Older Worker	Not as IS literate/proficient	Negative
12	10	IS challenges at work or with coworkers	B-02-OE-02	"Younger coworkers more agile but less patient in IS/IT."	SMB IS Practices	Age/Generational	Younger Worker	Less Patient	Negative
13	10	IS challenges at work or with coworkers	B-02-OE-02	"IS not a big issue."	SMB IS Practices				Neutral
14	10	IS challenges at work or with coworkers	B-02-YE-02	Participant unable to answer question.	SMB IS Practices	Lack of IS Awareness			Neutral
15	10	IS challenges at work or with coworkers	B-02-YE-02	"IS important for data security."	SMB IS Practices	IS Priority	High		Positive
16	10	IS challenges at work or with coworkers	C-03-OE-03	"IS workplace practices satisfactory."	SMB IS Practices	IS Priority	High		Positive
17	10	IS challenges at work or with coworkers	C-03-OE-03	"IS network policy too restrictive."	SMB IS Practices	Management	Network Policy too restrictive		Negative
18	10	IS challenges at work or with coworkers	E-04-OE-04	"Lack of resource support for IS."	SMB IS Practices	Management	Lack of IS governance, oversight, support	Budget Spending	Negative
19	10	IS challenges at work or with coworkers	E-04-OE-04	"IS practices are important."	SMB IS Practices	IS Priority	High		Neutral

#	Question	Question (Opinion)	Participant Code	Participant Gisted Response	Participant Response - Theme Codification - Level 1	Participant Response - Theme Codification - Level 2	Participant Response - Theme Codification - Level 3	Participant Response - Theme Codification - Level 4	Theme Connotation
20	10	IS challenges at work or with coworkers	E-04-OE-04	Participant unable to answer question.	SMB IS Practices				Neutral
21	10	IS challenges at work or with coworkers	E-04-OE-04	"Insider threat: Potential revenge."	SMB IS Practices	Insider Threat	Potential employee disgruntlement/reven		Negative
22	10	IS challenges at work or with coworkers	E-04-OE-04	"Increased online activity resulting in increased invisible risk."	SMB IS Practices	Lack of IS Awareness			Neutral
23	11	IS challenges at work or with coworkers	E-04-OE-04	"IS awareness still low."	Government IS policy & implementation	Increased GOV IS policy and oversight needed			Neutral
24	11	Challenges on IS implementation by SMB/GOV	B-02-OE-02	"Government IS practices are important. More guidance needed."	Government IS policy & implementation	Increased GOV IS policy and oversight needed			Negative
25	11	Challenges on IS implementation by SMB/GOV	B-02-OE-02	"CSR not critical data, compared to other industries."	SMB IS Practices	Data Management	Critical vs. Non-Critical		Neutral
26	11	Challenges on IS implementation by SMB/GOV	C-03-OE-03	"With more online business transactions and activities, government needs to implement proportional IS governance and controls."	Government IS policy & implementation	Increased GOV IS policy and oversight needed			Neutral
27	11	Challenges in IS with Older Coworkers	C-03-YE-03	"Older coworkers tend to take IS shortcuts."	SMB IS Practices	Age/Generational	Older Worker	Takes IS shortcuts	Neutral
28	11	Challenges on IS implementation by SMB/GOV	C-04-YE-04	"Colleagues lack IS awareness and protocols."	SMB IS Practices	Lack of IS Awareness			Neutral
29	11	Challenges on IS implementation by SMB/GOV	C-04-YE-04	"Lack of IS governance and oversight from headquarters, resulting in high risk."	SMB IS Practices	Management	Lack of IS governance, oversight, support	Governance & Oversight	Neutral
30	11	Challenges on IS implementation by SMB/GOV	C-04-YE-04	"Government need to escalate posture in response to government hacking incident."	Government IS policy oversight	Increased GOV IS policy and oversight needed			Neutral
31	11	Challenges on IS implementation by SMB/GOV	E-04-OE-04	"IA awareness in industry generally low."	Government IS policy & implementation	Increased GOV IS policy and oversight needed			Neutral
32	13	Challenges in IS with Older Coworkers	A-01-YE-01	"No distinguishable difference between older and younger workers."	SMB IS Practices	Age/Generational	No difference		Negative
33	13	Challenges in IS with Older Coworkers	A-01-YE-01	"Challenges explaining IS to older coworkers and client."	SMB IS Practices	Age/Generational	Older Worker	Not as IS literate/proficient	Negative
34	13	Challenges in IS with Older Coworkers	B-02-YE-02	"When there is incident. Relay information."	SMB IS Practices	Management	Rapid incident reporting		Neutral
35	13	Challenges in IS with Older Coworkers	B-02-YE-02	"Differences not age-based, more skill based."	SMB IS Practices	Age/Generational	Skilled Based		
36	13	Challenges in IS with Older Coworkers	B-02-YE-02	"Older coworkers more practical due to senior rank in organization."	SMB IS Practices	Age/Generational	Older Worker	More pragmatic on IS	

#	Question	Question (Opinion)	Participant Code	Participant Gisted Response	Participant Response - Theme Codification - Level 1	Participant Response - Theme Codification - Level 2	Participant Response - Theme Codification - Level 3	Participant Response - Theme Codification - Level 4	Theme Connotation
37	13	Challenges in IS with Older Coworkers	C-03-YE-03	"No distinguishable difference between older and younger workers."	SMB IS Practices	Age/Generational	No difference		Negative
38	13	Challenges in IS with Older Coworkers	C-03-YE-03	"Older coworkers slower to grasp IS concept."	SMB IS Practices	Age/Generational	Older Worker	Not as IS literate/proficient	Negative
39	13	Challenges in IS with Older Coworkers	C-03-YE-03	"Older coworkers not as IT savvy."	SMB IS Practices	Age/Generational	Older Worker	Not as IS literate/proficient	Negative
40	13	Challenges in IS with Older Coworkers	C-03-YE-03	"Older coworkers tend to forget passwords more easily."	SMB IS Practices	Age/Generational	Older Worker	Forgetful on IS	Negative
41	13	Challenges in IS with Older Coworkers	C-03-YE-03	"Older coworkers more high maintenance for IS support."	SMB IS Practices	Age/Generational	Older Worker	More dependant for IS support	Negative
42	13	Challenges in IS with Older Coworkers	C-03-YE-03	"Older Workers tend to take risky IS shortcuts."	SMB IS Practices	Age/Generational	Older Worker	More IS risk-taking	Neutral
43	13	Challenges in IS with Older Coworkers	C-04-YE-04	"No distinguishable difference between older and younger workers."	SMB IS Practices	Age/Generational	No difference		Negative
44	13	Challenges in IS with Older Coworkers	E-04-OE-04	"No difference between older younger employees."	SMB IS Practices	Age/Generational	No difference		Neutral
45	13	Challenges in IS with Older Coworkers	E-04-OE-04	"Lack if IS awareness at lounge: confidentiality and gossip."	SMB IS Practices	Age/Generational	Older Worker	More IS risk-taking	Negative
46	13	Challenges in IS with Older Coworkers	E-04-OE-04	"Lack of IA savvy file encryption and decryption."	SMB IS Practices	Age/Generational	Older Worker	Not as IS literate/proficient	Negative
47	13	Challenges in IS with Older Coworkers	E-04-OE-04	"Older coworkers are more disciplined and compliant on IS."	SMB IS Practices	Age/Generational	Older Worker	More disciplined & compliant on IS	Negative
48	13	Challenges in IS with Older Coworkers	E-04-OE-04	"Young coworkers are more careless and aloof on IS."	SMB IS Practices	Age/Generational	Younger Worker	More careless & aloof on IS	Negative

Appendix D: Email Solicitation for Interview Participation

Dear [Participant Candidate]:

My name is Hari Roosman. I am a doctoral student in the Information Assurance program in the College of Computing and Engineering at Nova Southeastern University (NSU) in Florida, United States. My dissertation advisor is Dr. Martha Snyder. I am emailing you to request for your consent to participate in my research study to explore how employees in in Indonesian organizations acquire, use, and share information that may help mitigate cybersecurity attacks.

The interview for this research was initially planned an in-person face-to-face interview in Jakarta, Indonesia. But due to the ongoing COVID-19 travel restrictions and concerns, the interview is now proposed to be conducted remotely via a VOIP audio communication platform, such as Zoom or WhatsApp.

The interview will take approximately 30 to 60 minutes. The interviews will be semi-structured and consist of approximately 15 questions. You can take pauses anytime in between the questions. No response to the questions is also acceptable. You may also cancel the interview at any point.

I will be taking notes during our interview, and there may be pauses between questions due to this. If you consent, I will record the interview with a digital audio record to better capture key points of the interview.

I may request for documentation or references on your organization's cybersecurity policy and practices. I may search and collect information from your organization's public website.

Please let me know if you are interested and willing to participate in this interview. If you have questions, please do not hesitate to contact me. Thank you for your attention and I look forward to your participation.

Sincerely,

Hari Roosman.–

Hari S. Roosman
Doctoral Candidate Student
Nova Southeastern University
Ft. Lauderdale, Florida, U.S.A.

Appendix E: List of Interview Questions

1. Can you provide an overview and description of your company?
2. How long have you been employed at your company and what is your job title, and can you provide a description of your job duties and responsibilities?
3. Can you provide an estimate of older worker to younger worker percentage ratio at your company?
4. How are worker Information Security skills and knowledge measured at your company?
5. How do you think Information Security can protect your company from IS threats?
6. How is Information Security information and guidance distributed at your company?
7. How is Information Security training delivered at your company?
8. How often is Information Security discussed among your co-workers?
9. How are Information Security policies and protocols shared and delivered at your company?
10. What challenges do you encounter with Information Security implementation at your company and your co-workers?
11. What is your opinion on Information Security at your company and in Indonesia?
12. How often is Information Security discussed with your older co-workers? *
13. Are there any challenges in discussing Information Security with your older coworkers, or in Information Security implementation with your older co-workers? * Questions were only for younger workers to answer.

Appendix F: Interview Guide

The following questions will be used to guide the researcher in conducting the semi-structured interviews. Older workers will be asked questions from sections 1-4 and younger workers will be asked questions from sections 1-5. The interview is estimated to take approximately 30 to 60 minutes.

1. Organization

   IQ-1: Please describe your organization (type of organization, main purpose of business, approximate number of employees, how long has it been in business, etc.).

   IQ-2: How long have you worked for the organization and what type of work do you do?

   IQ-3: What is the general demographic composition of your organization? For example, there more younger workers or older workers, or is it about equal?

2. Familiarity with IT, Information Security, and Cybersecurity

   IQ-4: How would you assess your knowledge and skills level in IT and cybersecurity?

   IQ-5: How familiar are you with information security and cybersecurity, and how often do deal with it at work?

3. Cybersecurity Practices and Deterrence in the Organization

   IQ-6:What countermeasures that you are aware of are currently in place in at your organization to mitigate cybersecurity attacks?

   IQ-7: How do you learn about ways to protect you and your organization from cyber-attacks?

   IQ-8: How do you use this type of information to protect your organization against cybersecurity attacks?

   IQ-9: How do share what you know and do (i.e., your knowledge and skills) with colleagues in your organization to mitigate cyberattacks?

   IQ-10: What keeps you, if anything, from sharing your knowledge and skills relating to cybersecurity with others in your organization?

   IQ-11: What type of training and education does your organization provide on information and cybersecurity, and what format does it come in? Do you think management provides adequate information and cybersecurity training, and has is it been effective?

4. Miscellaneous (organization and government policy on retirement, etc.)

IQ-13: Can you provide an overview on your organization policy on employee retirement?

IQ-14: Can you provide an overview on what you know about government policy on retirement?

IQ-15: What are your thoughts on cybersecurity practices in Indonesia?

5. Knowledge Sharing in the Organization

IQ-16: How frequently do you discuss information security and cybersecurity among colleagues and at work?

IQ-17: Is there a difference in the way you communicate information about cybersecurity to older colleagues in your organization? If so, what is different and why?

Appendix G: Interview Coding Grid

#	Interview Question	Subject Answer	Subject Code	Subject Response	Theme (L-1)	Sub-Theme (L-2)
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						

Appendix H: Interview Pilot Test Process

This interview pilot test includes instructions that the researcher will use with the pilot testers and what questions the researcher might ask them to help refine the guide.

1. The researcher will contact potential pilot test participants to be interviewed to coordinate and confirm a meeting via video-teleconference (e.g., Zoom). For this pilot phase, the meeting will be conducted remotely. The actual interviews for the study will be conducted in-country and in-person with the participants (unless there are restrictions or objections from the subjects, in which case the interviews will be conducted remotely as well).
2. The researcher will send the pilot participant via e-mail the list of interview questions so that they can review them in advance so the participant can review the material for any questions or concerns. A few days before the pilot interview, the researcher will re-confirm the meeting with the participant.
3. Before the interview, the researcher will greet the participant and provide an overview of the interview process, format, protocol, and time allotment. The researcher will also request the permission from the participants to conduct the interview and to record the interview with video or audio, or both.
4. When the interview officially begins, the researcher will begin asking the interview questions sequentially from the interview guide. The researcher will pause after each question and provide the participant as much time as the participant needs to respond to the question. The participant may at their liberty opt not to respond to any of the questions if he or she is not inclined. The participant has the liberty to request the researcher for a pause during the interview, or to stop the interview. If the interview

runs over the scheduled time (60 minutes), it is at the mutual discretion of the researcher and participant to continue or stop the interview.

5. The researcher will ask the participant if there are any questions that are confusing or need clarification, if there are questions that were omitted and should be added, and if they have any additional suggestions for improvement or questions about the research. At the conclusion of the pilot interview, the researcher will thank the participant for his or her time.
6. After the pilot interview, the researcher will review the notes and video/audio recordings from the pilot interview and assess which questions and portions of the interview worked well, and portions that did not work as well that could be either revised and improved or omitted. The researcher will then revise the interview guide accordingly.

Appendix I: Email Solicitation for Interview Participation in Indonesian

Bapak/Ibu ____________:

Perkenalkan saya, Hari Roosman. Saya mahasiswa calon S3 di program Information Assurance program di fakultas Computing dan Engineering di Nova Southeastern University (NSU), Florida, Amerika Serikat. Pembimbing skripsi saya Ibu Martha Snyder, PhD.

Tujuan surat ini untuk memohon persetujuan Pak/Ibu __________ sebagai partisipan riset saya untuk meneliti bagaimana pegawai di organisasi Indonesia organizations mendapatkan, menggunakan, and membagi informasi dan pengetahuan untuk meningkatkan kemanan cybersecurity di organisasi mereka.

Wawancara untuk riset ini pada mulanya direncanakan sebagai wawancara-wawanancara di lokasi (Jakarta). Tapi berhubung pandemi COVID-19 dan kendala travel ke Indonesia, maka diputuskan wawancara-wawancara untuk dilaksakanan lewat Zoom atau WhatsApp.

Wawancara ini diperkirakan 30 menit dan terdiri dari 17 pertanyaan. Jeda bisa Bapak/Ibu ambil kapanpun selama wawancara. Apabila Bapak/Ibu kurang berkenan menjawab pertanyaan-pertanyaan di wawancara, atau wawancara ingin dibatalkan kapanpun selama wawancara.

Saya akan mengambil catatan selama interview, dan mungkin akan ada jeda diantara pertanyaan-pertanyaan wawancara untuk mencatat. Bila Bapak/Ibu mengijinkan, saya ingin merekeman audio interview ini menangkap point-point penting dari wawancara. Bila diizinkan, saya meminta dokumentasi tentang cybersecurity organisasi. Saya juga berniat riset dan koleksi information dari website organisasi anda.

Mohon persetujuan partisipasi Bapak/Ibu dalam wawancara ini. Jika Bapak/Ibu ada pertanyaan, mohon kontak saya. Terima kasih atas perhatian Bapak/Ibu, dan semoga berkenan berpartisipasi dalam riset ini.

Terima kasih. Hormat saya.

Hari Roosman.–

Hari S. Roosman
Mahasiswa Calon S3
Nova Southeastern University
Ft. Lauderdale, Florida, U.S.A.

Appendix J: Interview Guide in Indonesian

Panduan Wawancara

Pertanyaan-pertanyaan wawancara ini adalag untuk sumber bahan penelitian riset ini.

Pegawai Senior akan di beri pertanyaan dari bagian 1 sampai 4. Pegawai Junior akan di beri pertanyaan dari bagian 1 sampai 5. Wawancara diperkirakan 30 sampai 40 menit.

1. <u>Organisasi</u>

IQ-1: Mohon memberikan deskripsi organisasi Bapak/Ibu (tipe organisasi, tujuan utama organisasi, jumlah pegawai, berapa usia organisasinya)

IQ-2: Berapa lama Bapak/Ibu berkerja untuk organisasi, dan apa jabatan, tugas, atau fungsi Bapak/Ibu di organisasi.

IQ-3: Bagaimana komposisi usia pegawai di organisasi anda? Apakah lebih banyak pegawai senior atau junior, atau kurang lebih sama?

2. <u>Pemahaman dengan IT, Information Security, and Cybersecurity</u>

IQ-4: Bagaimana Bapak/Ibu mengukur pengetahuan dan skill dalam IT dan cybersecurity?

IQ-5: Bagaimana kepahaman Bapak/Ibu tentang Information Security and Cybersecurity, dan berapa sering berurusuan di kerja?

3. <u>Praktek Cybersecurity dan Pencegahan Pelanggaran Cybersecurity Organization</u>

IQ-6: Apa sistim pencegahan cyberecurity di organisasi yang Bapak/Ibu ketahui.

IQ-7: Bagaimana Bapak/Ibu belajar atau mengetahui tentang pencegahan di organisasi tentang ancaman cyber-attack?

IQ-8: Bagaimana Bapak/Ibu menggunakan informasi ini untuk melindungi organisasi dari ancaman cybersecurity?

IQ-9: Bagaimana Bapak/Ibu sharing pengetahuan cybersecurity dengan rekan-rekan kerja untuk melindungi dari ancaman cybersecurity organisasi.

IQ-10: Apakah ada kendala untuk membagi pengetahuan cybersecurity dengan rekan-rekan lain di organisasi?
IQ-11: Apakah training atau pengetahuan cybersecurity diberi organisasi, dan dalam bentuk apa (video, e-mail, kelas, etc.) Apakah organisasi memberi training atau pengetahuan cybersecurity yang cukup, dan apakah training dan pengetahuan tersebut memadai?

4. Lain-Lain (peraturan organisasi and pemerintah tentang pensiun, etc.)

IQ-13: Dapatkah Bapak/Ibu memberikan rangkuman tentant pensiun di organisasi?

IQ-14: Dapatkah Bapak/Ibu memberikan rangkuman tentang peraturan pemerintah tentang sistim pensiun?

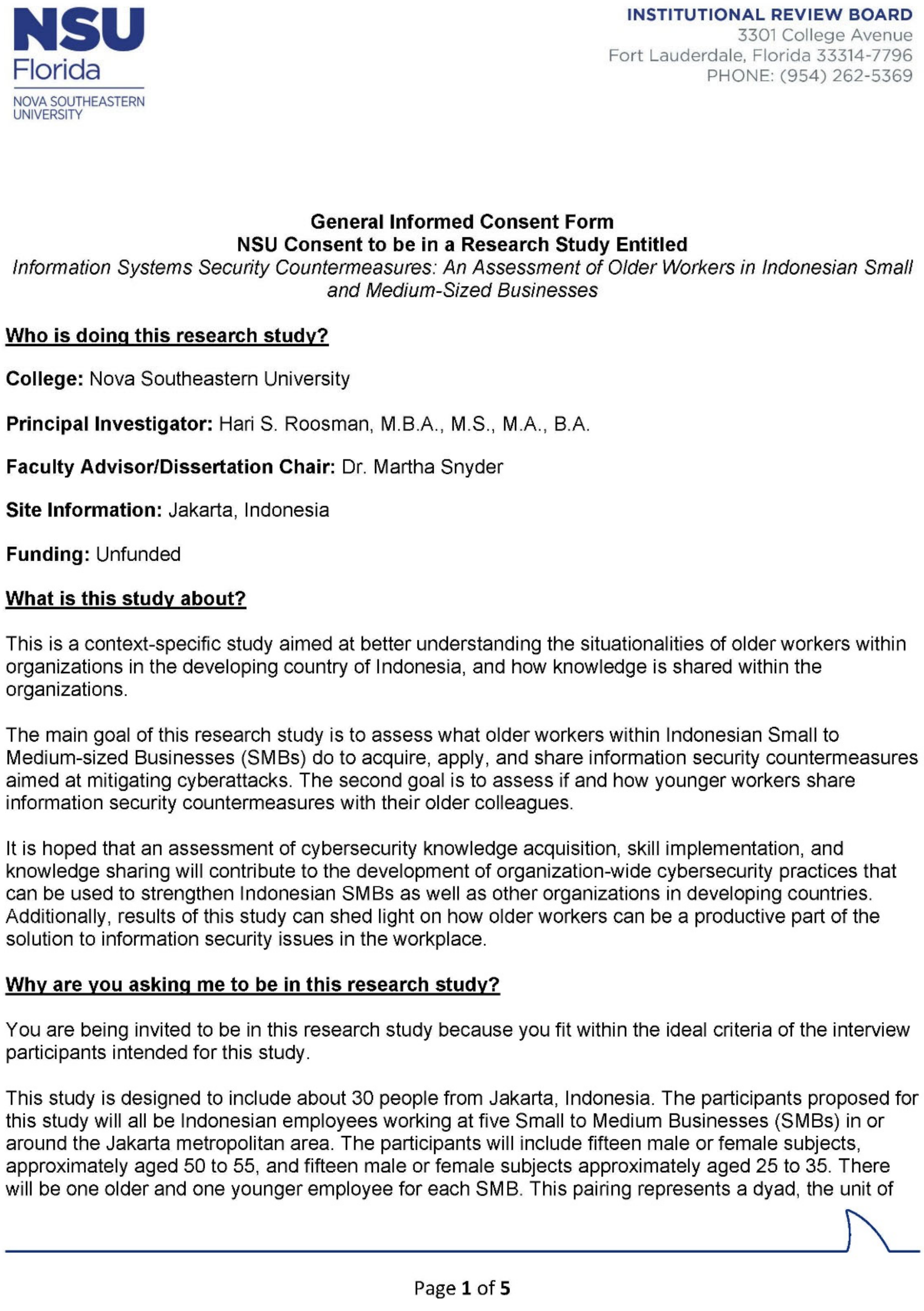
IQ-15: Apakah opini Bapak/Ibu tentang praktik cybersecurity di Indonesia?

5. Pembagian Pengetahuan di Organisasi

IQ-16: Berapa sering Bapak/Ibu diskusi tentang Information Security dan Cybersecurit dengan rekan-rekan kerja.

IQ-17: Apakah ada perbedaan dengan cara Bapal/Ibu membahasa informaso tentanh cybersecurity dengan rekan-rekan Senior di organisasi? Apakah ada perbedaan, dan kenapa?

Appendix K: General Informed Consent Form



NSU
Florida
NOVA SOUTHEASTERN
UNIVERSITY

INSTITUTIONAL REVIEW BOARD
3301 College Avenue
Fort Lauderdale, Florida 33314-7796
PHONE: (954) 262-5369

General Informed Consent Form
NSU Consent to be in a Research Study Entitled
Information Systems Security Countermeasures: An Assessment of Older Workers in Indonesian Small and Medium-Sized Businesses

Who is doing this research study?

College: Nova Southeastern University

Principal Investigator: Hari S. Roosman, M.B.A., M.S., M.A., B.A.

Faculty Advisor/Dissertation Chair: Dr. Martha Snyder

Site Information: Jakarta, Indonesia

Funding: Unfunded

What is this study about?

This is a context-specific study aimed at better understanding the situationalities of older workers within organizations in the developing country of Indonesia, and how knowledge is shared within the organizations.

The main goal of this research study is to assess what older workers within Indonesian Small to Medium-sized Businesses (SMBs) do to acquire, apply, and share information security countermeasures aimed at mitigating cyberattacks. The second goal is to assess if and how younger workers share information security countermeasures with their older colleagues.

It is hoped that an assessment of cybersecurity knowledge acquisition, skill implementation, and knowledge sharing will contribute to the development of organization-wide cybersecurity practices that can be used to strengthen Indonesian SMBs as well as other organizations in developing countries. Additionally, results of this study can shed light on how older workers can be a productive part of the solution to information security issues in the workplace.

Why are you asking me to be in this research study?

You are being invited to be in this research study because you fit within the ideal criteria of the interview participants intended for this study.

This study is designed to include about 30 people from Jakarta, Indonesia. The participants proposed for this study will all be Indonesian employees working at five Small to Medium Businesses (SMBs) in or around the Jakarta metropolitan area. The participants will include fifteen male or female subjects, approximately aged 50 to 55, and fifteen male or female subjects approximately aged 25 to 35. There will be one older and one younger employee for each SMB. This pairing represents a dyad, the unit of analysis for this study. The purpose of the dual age group categorization is part of this study's design to compare information and insights derived from subjects from differing age groups.

What will I be doing if I agree to be in this research study?

You will be invited to as a participant for an interview that will take approximately 30 to 60 minutes.

As a participant, you would be involved in the following process:

Prior to the interview:

- The researcher will brief you on the interview process, guidelines, and estimated duration of interview.
- The researcher will also provide you with a copy of the study's interview guide which contains a list of the questions that the researched will ask you during the interview.
- The researcher will request for your permission to record the interview with a digital audio recorder.
- The researcher will ask if you have any questions and are prepared or need extra time to begin interview.

During the interview:

- The researcher may ask if you need to pause or take a break during the interview.
- The researcher may ask if you have any questions during the interview.

After the interview:

- The researcher will inform you that the interview has concluded, and ask if you have any questions or requests.

Are there possible risks and discomforts to me?

This research study involves minimal to no risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life.

What happens if I do not want to be in this research study?

You have the right to leave this research study at any time or refuse to be in it. If you decide to leave or you do not want to be in the study anymore, you will not get any penalty or lose any services you have a right to get. If you choose to stop being in the study before it is over, any information about you that was collected before the date you leave the study will be kept in the research records for 36 months from the end of the study and may be used as a part of the research.

You have the right to leave this research study at any time, or not be in it. If you do decide to leave or you decide not to be in the study anymore, you will not get any penalty or lose any services you have a right to get. If you choose to stop being in the study, any information collected about you before the date you leave the study will be kept in the research records for 36 months from the end of the study but you may request that it not be used.

What if there is new information learned during the study that may affect my decision to remain in the study?

If significant new information relating to the study becomes available, which may relate to whether you want to remain in this study, this information will be given to you by the investigators. You may be asked to sign a new Informed Consent Form if the information is given to you after you have joined the study.

Are there any benefits for taking part in this research study

There is no guarantee or promise that you will receive any benefit from this study, but we hope the information learned from this research study will benefit other people with similar conditions in the future. We also hope findings from this research can add to the body of knowledge in this study discipline.

Will I be paid or be given compensation for being in the study?

You will not be provided payment or compensation for participating in this research study.

Will it cost me anything?

There are no costs to you for participating in this research study.

How will you keep my information private?

Information we learn about you in this research study will be strictly handled in a confidential manner, within the limits of the law and will be limited to people who only have a need-to-know to review this information. All confidential data will be stored securely in a password-protected USB 3.0 256-bit AES XTS Hardware Encrypted Portable External Hard Drive.

This data will be available to the researcher, the Institutional Review Board and other representatives of this institution, and any regulatory and granting agencies, if applicable. If we publish the results of the study in a scientific journal or book, we will not identify you. All confidential data will be stored securely in a password-protected USB 3.0 256-bit AES XTS Hardware Encrypted Portable External Hard Drive.

All data will be kept for 36 months from the end of the study and destroyed after that time by 31 December 2024.

Will there be any Audio or Video Recording?

This research study involves only audio recording. This recording will be available to the researcher, the Institutional Review Board and other representatives of this institution. The recording will be kept, stored, and destroyed as stated in the section above. Because what is in the recording could be used to find out that it is you, it is not possible to be sure that the recording will always be kept confidential. The researcher will try to keep anyone not working on the research from listening to or viewing the recording.

Whom can I contact if I have questions, concerns, comments, or complaints?

If you have any questions, concerns, and complaints, please contact us. If you have more questions about the research, your research rights, or have a research-related injury, please contact:

Primary contact:

Hari S. Roosman
Phone: +1-415-384-1140
E-mail: roosman@mynsu.nova.edu
E-mail: hari@roosman.com

Research Participants Rights

For questions/concerns regarding your research rights, please contact:

Institutional Review Board
Nova Southeastern University
(954) 262-5369 / Toll Free: 1-866-499-0790
IRB@nova.edu

You may also visit the NSU IRB website at www.nova.edu/irb/information-for-research-participants for further information regarding your rights as a research participant.

Research Consent & Authorization Signature Section

Voluntary Participation - You are not required to participate in this study. In the event you do participate, you may leave this research study at any time. If you leave this research study before it is completed, there will be no penalty to you, and you will not lose any benefits to which you are entitled.

If you agree to participate in this research study, sign this section. You will be given a signed copy of this form to keep. You do not waive any of your legal rights by signing this form.

SIGN THIS FORM ONLY IF THE STATEMENTS LISTED BELOW ARE TRUE:

- You have read the above information.
- Your questions have been answered to your satisfaction about the research

Adult Signature Section

I have voluntarily decided to take part in this research study.

____________________ Printed Name of Participant

____________________ Signature of Participant

__________ Date

____________________ Printed Name of Person Obtaining Consent and Authorization

____________________ Signature of Person Obtaining Consent & Authorization

__________ Date

References

Aaltio, I., & Heilmann, P. (2010). Case study as a methodological approach. In A.J. Mills, G. Durepos, & E. Wiebe (Eds.), *Encyclopedia of Case Study Research* (pp. 66–67). Sage Publishing. https://doi.org/dx.doi.org/10.4135/9781412957397

Abdillah, M. R., Wu, W., & Anita, R. (2020). Can altruistic leadership prevent knowledge-hiding behavior? Testing dual mediation mechanisms. *Knowledge Management Research and Practice*, 1-15. https://doi.org/10.1080/14778238.2020.1776171

Abed, J., & Weistroffer, H. R. (2016). Understanding deterrence theory in security compliance behavior: A quantitative meta-analysis approach. *Swedish Artificial Intelligence Society Proceedings, Sweden, 28.* https://aisel.aisnet.org/sais2016/28/

Abubakar, A. D., Bass, J. M., & Allison, I. (2014). Cloud computing: Adoption issues for sub-Saharan African SMEs. *The Electronic Journal of Information Systems in Developing Countries*, *62*(1), 1-17. https://doi.org/10.1002/j.1681-4835.2014.tb00439.x

Agrawal, V. (2017). A comparative study on information security risk analysis methods. *Journal of Computers*, *12*(1)*,* 57-67. https://doi.org/dx.doi.org/10.17706/jcp.12.1.57-67

Aguilar Solano, M. (2020). Triangulation and trustworthiness: Advancing research on public service interpreting through qualitative case study methodologies. *FITISPos International Journal*, *7*, 31-52. https://doi.org/10.37536/FITISPos-IJ.2020.7.1.249

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Ireland,* 1-5. https://doi.org/10.1109/cybersa49311.2020.9139638

Almeida, F., Carvalho, I., & Cruz, F. (2018). Structure and challenges of a security policy on small and medium enterprises. *KSII Transactions on Internet and Information Systems*, *12*(2), 747-763. https://doi.org/10.3837/tiis.2018.02.012

Alshboul, Y., & Streff, K. (2015). Analyzing information security model for small-medium sized businesses. *21st Americas Conference on Information Systems, USA.* https://aisel.aisnet.org/amcis2015/ISSecurity/GeneralPresentations/26/

Amrin, N. (2014). *The impact of cyber security on SMEs* [Master thesis, University Twente]. University Twente Student Digital Archive. https://essay.utwente.nl/65851/

Anand, P., & Hassan, Y. (2019). Knowledge hiding in organizations: Everything that managers need to know. *Development and Learning in Organizations: An International Journal*, *33*(6), 12-15. https://doi.org/10.1108/dlo-12-2018-0158

Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T., & Vasek, M. (2019). Measuring the changing cost of cybercrime. *The 18th Annual Workshop on the Economics of Information Security, USA.* https://doi.org/10.17863/CAM.41598

Arage, T., & Tesema, T. (2016). An integrated approach to information systems security policy violation: The case of Ethiopia. *Proceedings of the 10th International Conference on Informatics and Systems, Egypt*. 228-232. https://doi.org/10.1145/2908446.2908456

Arage, T., Belanger, F., & Tesema, T. (2016). Investigating the moderating impact of national culture in information systems security policy violation: The case of Italy and Ethiopia. *Proceedings of the 56th Mediterranean Conference on Information Systems*, *Cyprus*. https://aisel.aisnet.org/mcis2016/56/

Aviv, S., Levy, Y., Wang, L., & Geri, N. (2019). An expert assessment of corporate professional users to measure business email compromise detection skills and develop a knowledge and awareness training program, *19*. *Proceedings of the 14th Pre-ICIS Workshop on Information Security and Privacy, Germany.* https://www.albany.edu/wisp/includes/WISP2019_proceedings/WISP2019_paper_1.pdf

Bada, M., & Nurse, J. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises. *Information & Computer Security*, *27*(3), 393-410. https://doi.org/10.1108/ics-07-2018-0080

Badan Siber dan Sandi Negara. (2019). Computer security incident response team report: Calendar year 2020. https://govcsirt.bssn.go.id/laporan-tahunan-gov-csirt-2019/

Badan Siber dan Sandi Negara. (2020). *Cyber-attacks in Indonesia*. https://bssn.go.id/rekap-serangan-siber-januari-april-2020/

Badra, M., El-Sawda, S., & Hajjeh, I. (2007). Phishing attacks and solutions. *Association for Computing Machinery, 42*, 1-6. https://dl.acm.org/doi/10.5555/1385289.1385340

Balan, S., Otto, J., Minasian, E., & Aryal, A. (2017). Data analysis of cybercrimes in businesses. *Information Technology and Management Science*, *20*(1). https://doi.org/10.1515/itms-2017-0011

Bay, M. (2016). What is cybersecurity? In search of an encompassing definition for the post-Snowden era. *French Journal for Media Research*, *6,* 1–28. http://frenchjournalformediaresearch.com/lodel-1.0/main/index.php?id=988

Ben-David, Y., Hasan, S., Pal, J., Vallentin, M., Panjwani, S., Gutheim, P., Chen, J., & Brewer, E. A. (2011), 39-44. Computing security in the developing world. *Proceedings of the 5th ACM Workshop on Networked Systems for Developing Regions, USA.* https://doi.org/10.1145/1999927.1999939

Berry, A., Rodriguez, E., & Sandee, H. (2001). Small and medium enterprise dynamics in Indonesia. *Bulletin of Indonesian Economic Studies*, *37*(3), 363-384. https://doi.org/10.1080/00074910152669181

Berry, A., Rodriguez, E., & Sandee, H. (2002). Firm and group dynamics in the small and medium enterprise sector in Indonesia. *Small Business Economics*, *18*(1), 141-161. http://dx.doi.org/10.1023/A:1015186023309

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, *8*(1), 1–10. https://doi.org/10.1504/ijbcrm.2018.10011667

Boateng, R., Longe, O. B., Mbarika, V., Avevor, I., & Isabalija, S. R. (2010). Cybercrime and criminality in Ghana: Its forms and implications. *Proceedings of the 16th Americas Conference on Information Systems, Peru.* https://aisel.aisnet.org/amcis2010/507/

Bratthall, L., & Jørgensen, M. (2002). Can you trust a single data source exploratory software engineering case study? *Empirical Software Engineering*, *7*(1), 9-26. https://doi.org/10.1023/A:1014866909191

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brisola, E., & Cury, V. (2016). Researcher experience as an instrument of investigation of a phenomenon: An example of heuristic research. *Estudos De Psicologia (Campinas)*, *33*(1), 95-105. https://doi.org/10.1590/1982-02752016000100010

Bureau of Labor and Statistics. (2004). *Current labor statistics monthly labor review: December 2004*. https://www.bls.gov/opub/mlr/2004/12/cls0412.pdf

Burns, A., Davies, A., & Beynon Davies, P. (2006). A study of the uptake of information security policies by small and medium sized businesses in Wales. *ICEB 2006 Proceedings, Finland.* https://aisel.aisnet.org/iceb2006/71

Butt, A.S, & Ahmad, A.B. (2019). Are there any antecedents of top-down knowledge hiding in firms? Evidence from the United Arab Emirates. *Journal of Knowledge Management*, *23*(8), 1605-1627. https://doi.org/10.1108/jkm-04-2019-0204

Butt, A.S. (2020). Mitigating knowledge hiding in firms: An exploratory study. *Baltic Journal of Management*, *15*(4), 631-645. https://doi.org/10.1108/bjm-01-2020-0016

Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-middle attack to the https protocol. *IEEE Security & Privacy Magazine*, *7*(1), 78-81. https://doi.org/10.1109/msp.2009.12

Chawla, R., & Gupta, V. (2020). Examining role of individual and organization factors in knowledge hiding tendencies of IT sector employees. *Journal of Interdisciplinary Cycle Research,* 12(*10*), 1128-1141. http://www.jicrjournal.com/gallery/122-jicr-october-3357.pdf

Chelly, M. L. (2016). Employees' impact on cyber security human behavior consequences on security measures. *World Congress on Internet Security, UK.* https://doi.org/10.2053/WorldCIS.2016.0005

Chen, J. (2016). Cyber security: Bull's-eye on small businesses. *Journal of International Business and Law*, *16*(1). https://doi.org/https://scholarlycommons.law.hofstra.edu/jibl/vol16/iss1/10

Chen, Z., & Ji, C. (2009). An information-theoretic view of network-aware malware attacks. *IEEE Transactions on Information Forensics and Security*, *4*(3), 530–541. https://doi.org/10.48550/arXiv.0805.0802

Choi, Y. B., & Allison, G. D. (2017). Intrusion prevention and detection in small to medium-sized enterprises. *SAIS 2017 Proceedings, Sweden*, *11*. http://aisel.aisnet.org/sais2017/11

Ciutiene, R., & Railaite, R. (2015). Age management as a means of reducing the challenges of workforce aging. *Engineering Economics*, *26*(4), 391-397. https://doi.org/10.5755/j01.ee.26.4.7081

CK Chiu, W., Chan, A. W., Snape, E., & Redman, T. (2001). Age stereotypes and discriminatory attitudes towards older workers: An east-west comparison. *Human Relations*, 54(5), 629-661. https://doi.org/10.1177/0018726701545004

Connelly, C. E., & Zweig, D. (2015). How perpetrators and targets construe knowledge hiding in organizations. *European Journal of Work and Organizational Psychology*, *24*(3), 479-489. https://doi.org/10.1080/1359432X.2014.931325

Connelly, C. E., Zweig, D., Webster, J., & Trougakos, J. P. (2012). Knowledge hiding in organizations. *Journal of Organizational Behavior*, *33*(1), 64–88. https://doi.org/10.1002/job.737

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525–554. https://doi.org/10.25300/misq/2019/15117

Cross, C., & Gillett, R. (2020). Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. *Journal of Financial Crime*, *27*(3), 871–884. https://doi.org/10.1108/jfc-02-2020-0026

Cummings, A., Lewellen, T., McIntire, D., Moore, A. P., & Trzeciak, R. (2012). Insider threat study: Illicit cyber activity involving fraud in the U.S. financial services sector. *Journal of Financial Crime*, *27*(3), 871–884. https://doi.org/10.21236/ada610430

Curtin, M., & Fossey, E. (2007). Appraising the trustworthiness of qualitative studies: Guidelines for occupational therapists. *Australian Occupational Therapy Journal*, *54*(2), 88–94. https://doi.org/10.1111/j.1440-1630.2007.00661.x

Damayanthi, S. (2019). *Thematic analysis of interview data in the context of management controls research*. Sage Publications Ltd. https://dx.doi.org/10.4135/9781526474858

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences*, *43*(6), 1091–1124. https://doi.org/10.1111/j.1540-5915.2012.00383.x

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, *22*(5), 474-489. https://doi.org/10.1108/IMCS-08-2013-0057

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643–658. https://doi.org/10.1057/ejis.2011.23

D'Arcy, J., & Hovav, A. (2004). The role of individual characteristics on the effectiveness of information system security countermeasures, 176. *Proceedings from 10th Americas Conference on Information Systems, USA.* https://aisel.aisnet.org/amcis2004/176/

D'Arcy, J., & Hovav, A. (2005). Deterring information systems misuse: The impact of three security countermeasures. *The 4th Security Conference, USA*. https://www.researchgate.net/publication/318661207_Deterring_Information_Systems_Misuse_the_impact_of_three_security_countermeasures

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Denzin, N. K. (1970). Problems in analyzing elements of mass culture: Notes on the popular song and other artistic productions. *American Journal of Sociology, 75*(6), 1035-1038. https://doi.org/10.1086/224853

Department of Labor. (2008). *A chartbook of international labor comparisons: The Americas, Asia-Pacific, Europe.* https://www.bls.gov/fls/chartbook/chartbook2008.pdf

Dhillon, G., Talib, Y. Y., & Picoto, W. N. (2020). The mediating role of psychological empowerment in information security compliance intentions. *Journal of the Association for Information Systems*, *21*(1), 152–174. https://doi.org/10.17705/1jais.00595

Djuraskovic, I., & Arthur, N. (2014). Heuristic inquiry: A personal journey of acculturation and identity reconstruction. *The Qualitative Report*, *15*(6), 1569-1593. https://doi.org/10.46743/2160-3715/2010.1361

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2007). Fostering information security culture in small and medium size enterprises: An interpretive study in Australia, 120. *Proceedings from ECIS 2007, Switzerland.* http://aisel.aisnet.org/ecis2007/120

Dols, T. (2009). *Influencing factors towards non-compliance in information systems: Carelessness and shadow IT in the corporate workplace.* [Master's Thesis, University of Applied Sciences Faculty Utrecht]. HBO Kennisbank. https://hbo-kennisbank.nl/details/sharekit_hu:oai:surfsharekit.nl:54ba7f7d-3390-46c8-95d5-11aecca4404d

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity capacity: Does it matter? *Journal of Information Policy*, *9*, 280–306. https://doi.org/10.5325/jinfopoli.9.2019.0280

Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. (2019). Cybercrime business digital in Indonesia. *E3S Web of Conferences, Indonesia, 125*, 21001. https://doi.org/10.1051/e3sconf/201912521001

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23–40. https://doi.org/10.1080/00396338.2011.555586

Federal Bureau of Investigation Internet Crime Complaint Center. (2020). *Annual internet crime report*: *Calendar year 2019*. Federal Bureau of Investigation. https://pdf.ic3.gov/2019_IC3Report.pdf

Floder, K. (2020). *How a commitment-based HR system influences the relationship between self-monitoring and knowledge hiding behavior: A multilevel study* (Publication No. 8920166) [Master thesis, Tilburg University]. Tilburg University Library. https://tilburguniversity.on.worldcat.org/search?queryString=scr.uvt.nl:8920166

Furnell, S. M., Gennatou, M., & Dowland, P. S. (2002). A prototype tool for information security awareness and training. *Logistics Information Management*, *15*(5), 352–357. https://doi.org/10.1108/09576050210447037

Gafni, R., & Pavel, T. (2019). The invisible hole of information on SMB's cybersecurity. *Online Journal of Applied Knowledge Management*, *7*(1), 14-26. https://doi.org/10.36965/OJAKM.2019.7(1)14-26

Gagné, M., Tian, A. W., Soo, C., Zhang, B., Ho, K. S., & Hosszu, K. (2019). Different motivations for knowledge sharing and hiding: The role of motivating work design. *Journal of Organizational Behavior*, *40*(7), 783–799. https://doi.org/10.1002/job.2364

Gajimu. (n.d.). *Batas usia pensiun PNS menurut UU ASN*. https://gajimu.com/tips-karir/kiat-pekerja/batas-usia-pensiun-pns

Gartner. (n.d.). *Definition of small and midsize business (SMB)*. Gartner Information Technology. https://www.gartner.com/en/information-technology/glossary/smbs-small-and-midsize-businesses

Gibbs, J. P. (1968). Crime, punishment, and deterrence. *The Southwestern Social Science Quarterly*, *28*(4), 515-530. https://www.jstor.org/stable/42867909

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). 2004 CSI/FBI computer crime and security survey. *Computer Security Journal*, *21*(3), 1.

http://dls.virginia.gov/commission/pdf/2004%20CSI-FBI%20Computer%20Crime%20and%20Security%20Survey.pdf

Gringart, E., Helmes, E., & Speelman, C. P. (2005). Exploring attitudes toward older workers among Australian employers: An empirical study. *Journal of Aging and Social Policy, 17*(3), 85-103. https://doi.org/10.1300/J031v17n03_05

Gundu, T., & Flowerday, S. V. (2013). Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal*, *104*(2), 69–79. https://doi.org/10.23919/saiee.2013.8531867

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses. *Information Management and Computer Security*, *13*(4), 297–310. https://doi.org/10.1108/09685220510614425

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors, *Heliyon*, *3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Han, M. S., Masood, K., Cudjoe, D., & Wang, Y. (2020). Knowledge hiding as the dark side of competitive psychological climate. *Leadership and Organization Development Journal*, *42*(2), 195–207. https://doi.org/10.1108/lodj-03-2020-0090

Hayes, J., & Bodhani, A. (2013). Cyber security: Small firms under fire. *Engineering and Technology*, *8*(6), 80–83. https://doi.org/10.1049/et.2013.0614

Hight, S. D. (2015, August 14). The importance of a security, education, training, and awareness program. *Infosec Writers.* 1-5. http://www.infosecwriters.com/text_resources/pdf/SETA_SHight.pdf

Hill, H. (2001). Small and medium enterprises in Indonesia: Old policy challenges for a new administration. *Asian Survey*, *41*(2), 248–270. https://doi.org/10.1525/as.2001.41.2.248

Hovav, A., & D’Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information and Management*, *49*(2), 99–110. https://doi.org/10.1016/j.im.2011.12.005

Hughes, C., Robert, L., Frady, K., & Arroyos, A. (2019). *Managing technology and middle and low-skilled employees: advances for economic regeneration*. Emerald Publishing.

Ingersoll-Dayton, B., & Saengtienchai, C. (1999). Respect for the elderly in Asia: Stability and change. *The International Journal of Aging and Human Development*, *48*(2), 113-130. https://doi.org/10.2190/G1XR-QDCV-JRNM-585P

International Telecommunication Union. (n.d). *Definition of cybersecurity*. Retrieved June 24, 2021, from https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

International Telecommunication Union. ITU-Tx. 1205. Interfaces, *10*(20), 49. https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1205-200804-I!!PDF-E&type=items

Jiang, Z., Hu, X., Wang, Z., & Jiang, X. (2019). Knowledge hiding as a barrier to thriving: The mediating role of psychological safety and moderating role of organizational cynicism. *Journal of Organizational Behavior*, *40*(7), 800–818. https://doi.org/10.1002/job.2358

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

Kavisankar, L., & Chellappan, C. (2011). A mitigation model for TCP SYN flooding with IP spoofing. *2011 International Conference on Recent Trends in Information Technology, India,* 251-256. https://ieeexplore.ieee.org/document/5972435

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive, 9*(3), 2012-2052. https://ssrn.com/abstract=2058035

Kenny, G. (2012). An introduction to Moustakas's heuristic method. *Nurse Researcher*, *19*(3), 6–11. https://doi.org/10.7748/nr2012.04.19.3.6.c9052

Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., & Spector, P. E. (2019). Information security climate and the assessment of information security risk among healthcare employees. *Health Informatics Journal*, *26*(1), 461–473. https://doi.org/10.1177/1460458219832048

Kim, T. K., Lee, D. Y., & Chung, T. M. (2002). Mobile agent-based misuse intrusion detection rule propagation model for distributed system, 842-849. *EurAsia-ICT 2002: Information and Communication Technology, Iran.* https://doi.org/10.1007/3-540-36087-5_97

Kimwele, M., Mwangi, W., & Kimani, S. (2017). Adoption of information technology security policies: Case study of Kenyan small and medium enterprises (SMEs). *Journal of Theoretical and Applied Information Technology, 18*(2). http://www.jatit.org/volumes/eighteenth_volume_2_2010.php

Kissel, R. L. (2009) *Small business information security: The fundamentals* (Report No. NISTIR 7621). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.7621

Kissel, R. L., Quill, K., & Johnson, C. (2014) *Small and medium-size business information security outreach program* (ITL Bulletin). National Institute of Standards and Technology. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=916061

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: Factors of success. *Entrepreneurship and Sustainability Issues*, *6*(4), 2081-2094. https://doi.org/10.9770/jesi.2019.6.4(37)

Krefting, L. (1991). Rigor in qualitative research: The assessment of trustworthiness. *American journal of occupational therapy*, *45*(3), 214-222. https://doi.org/10.5014/ajot.45.3.214

Lanke, P. (2018). Knowledge hiding: Impact of interpersonal behavior and expertise. *Human Resource Management International Digest*, *26*(2), 30–32. https://doi.org/10.1108/hrmid-01-2018-0010

Lau, F., Rubin, S. H., & Trajkovic, L. (2000). Cybernetics evolving to systems, humans, organizations, and their complex interactions, 2-3. *SMC 2000 Conference Proceedings, USA.* https://doi.org/10.1109/ICSMC.2000.884337

Law, M. C., & MacDermid, J. C. (2014). *Evidence-based rehabilitation: A guide to practice* (3rd ed.). Slack, Inc.

Levy, Y. and Gafni, R. (2021). Introducing the concept of cybersecurity footprint. *Information and Computer Security, 29*(5), 724-736. https://doi.org/10.1108/ICS-04-2020-0054

Li, J. Y., & Hoffman, E. (2018). Information security policy compliance. *Social Science Research Network*. https://dx.doi.org/10.2139/ssrn.3252742

Lichtenstein, J. (2014). *Demographic characteristics of business owners* (Business Owner Demographics, Issue Brief 2). Small Business Administration Office of Advocacy. https://cdn.advocacy.sba.gov/wp-content/uploads/2014/01/07145947/Issue-Brief-2-Business-Owner-Demographics.pdf

Liu, Y., Zhu, J. N. Y., & Lam, L. W. (2020). Obligations and feeling envied: A study of workplace status and knowledge hiding. *Journal of Managerial Psychology*, *35*(5), 347–359. https://doi.org/10.1108/jmp-05-2019-0276

Maurer, T.J., Barbeite, F.G., Weiss, E.M. & Lippstreu, M. (2008), New measures of stereotypical beliefs about older workers' ability and desire for development: Exploration among employees aged 40 and over. *Journal of Managerial Psychology*, *23*(4), 395-418. https://doi.org/10.1108/02683940810869024

McCann, R. M., & Keaton, S. A. (2013). A cross cultural investigation of age stereotypes and communication perceptions of older and younger workers in the USA and Thailand. *Educational Gerontology*, *39*(5), 326-341. https://doi.org/10.1080/03601277.2012.700822

McGregor, J., & Gray, L. (2002). Stereotypes and older workers: The New Zealand experience. *Social Policy Journal of New Zealand*, 163-177. https://www.msd.govt.nz/documents/about-msd-and-our-work/publications-resources/journals-and-magazines/social-policy-journal/spj18/18-pages163-177.pdf

McKee, D. (2006). *A dynamic model of retirement in Indonesia*. UCLA: California Center for Population Research. https://escholarship.org/uc/item/2hd6t64v

Mercuri, R. T. (2003). Analyzing security costs. *Communications of the ACM*, *46*(6), 15-18. https://doi.org/10.1145/777313.777327

Moustakas, C. E. (1990). *Heuristic research: Design, methodology, and applications* (1st ed.). Sage Publications, Inc.

Moustakas, C.E. (1994). *Phenomenological research methods* (1st ed.). Sage Publications, Inc.

Muller, L. P. (2015). Cyber security capacity building in developing countries: Challenges and opportunities. *Norwegian Institute of International Affairs (NUPI)*. https://www.jstor.org/stable/resrep07959

Mutchler, L. A. (2019). Response awareness and instructional self-efficacy: Influences on intent. *Information & Computer Security*, *27*(4), 489–507. https://doi.org/10.1108/ics-05-2018-0061

National Institute of Standards and Technology (2011). *Glossary of key information security terms.* https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7298r1.pdf

Nugraha, L. K., & Putri, D. A. (2016). Mapping the cyber policy landscape: Indonesia. *Global Partners Digital.* https://www.gp-digital.org/wp-content/uploads/2017/04/mappingcyberpolicy_landscape_indonesia.pdf

Onwubiko, C., & Lenaghan, A. P. (2007). Managing security threats and vulnerabilities for small to medium enterprises. *2007 IEEE Intelligence and Security Informatics*, 244–249. https://doi.org/10.1109/isi.2007.379479

Ortman, J. M., & Guarneri, C. E. (2009). *United States population projections: 2000 to 2050.* United States Census Bureau. https://www.census.gov/content/dam/Census/library/working-papers/2009/demo/us-pop-proj-2000-2050/analytical-document09.pdf

Osborn, E. (2015). *Business versus technology: Sources of the perceived lack of cyber security in SMEs.* University of Oxford. https://ora.ox.ac.uk/objects/uuid:4363144b-5667-4fdd-8cd3-b8e35436107e/datastreams/ATTACHMENT01

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards information systems security policy compliance. *2007 40th Annual Hawaii International Conference on System Sciences, USA,* 156b-156b. https://doi.org/10.1109/HICSS.2007.206

Paoli, L., Visschers, J., Verstraete, C. & Van Hellemont, E. (2018). The impact of cybercrime on Belgian businesses (KU Leuven Centre for IT & IP Law Series, Volume 5). *Intersentia.* https://doi.org/10.1017/9781780687742

Park, J. Y., Robles, R. J., Hong, C. H., Yeo, S. S., & Kim, T. H. (2008). IT security strategies for SME’s. *International Journal of Software Engineering and its Applications*, *2*(3), 91-98. https://www.researchgate.net/publication/255591542_IT_Security_Strategies_for_SME's

Pattinson, M., Butavicius, M., Lillie, M., Ciccarello, B., Parsons, K., Calic, D., & McCormac, A. (2019). Matching training to individual learning styles improves information security awareness. *Information and Computer Security*, *28*(1), 1–14. https://doi.org/10.1108/ics-01-2019-0022

Paulsen, C., & Toth, P. (2016). *Small business information security: The fundamentals (Report No.7621 Revision 1).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.7621r1

Peterson, S. J., & Spiker, B. K. (2005). Establishing the positive contributory value of older workers: A positive psychology perspective. *Organizational Dynamics,* 34(2), 153-167. https://doi.org/10.1016/j.orgdyn.2005.03.002

Rahayu, D. (2018). Indonesia national cybersecurity review: Before and after establishment national cyber and crypto agency (BSSN). *2018 6th International Conference on Cyber and IT Service Management (CITSM), Indonesia.* https://doi.org/10.1109/CITSM.2018.8674265

Rout, D. (2015). Developing a common understanding of cybersecurity. *ISACA Journal*, *6*, 1–4. https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/developing-a-common-understanding-of-cybersecurity

Safa, N. & Von Solms, R. (2016). An information systems knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442-451. http://dx.doi.org/10.1016/j.chb.2015.12.037

Saleem, J., Adebisi, B., Ande, R., & Hammoudeh, M. (2017). A state of the art survey - Impact of cyber attacks on SME's. *Proceedings of the International Conference on Future Networks and Distributed Systems, UK, 52.* https://doi.org/10.1145/3102304.3109812

Šalhūb Zainab Karāk, & Qāsimī Lubna al. (2010). *Cyber law and cyber security in developing and emerging economies*. Edward Elgar Publishing, Inc.

Samorodov, A. (1999). *Ageing and labour markets for older workers*. Employment and Training Department, International Labour Office, Geneva. https://www.ilo.org/wcmsp5/groups/public/---ed_emp/documents/publication/wcms_120333.pdf

Saputra, P., Sudirman, A., Sinaga, O., Wardhana, W., & Hayana, N. (2019). Addressing Indonesia's cyber security through public-private partnership (PPP). *Central European Journal of International & Security Studies*, *13*(4), 104-120. https://search.proquest.com/docview/2394981291/fulltextPDF/3259574E7F5044F5PQ/1

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *The Journal of Digital Forensics, Security and Law*, *12*(2), 53–74. https://doi.org/10.15394/jdfsl.2017.1476

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers and Security*, *21*(6), 526–531. https://doi.org/10.1016/s0167-4048(02)01009-x

Serenko, A., & Bontis, N. (2016). Understanding counterproductive knowledge behavior: Antecedents and consequences of intra-organizational knowledge hiding. *Journal of Knowledge Management*, *20*(6), 1199–1224. https://doi.org/10.1108/jkm-05-2016-0203

Setiyawan, A. (2019). National cybersecurity policy in the U.S. and Indonesia. *UNTAG Law Review*, *3*(1), 71-87. http://dx.doi.org/10.36356/ulrev.v3i1.1071

Shalhoub, Z. K., & Lubna, A. Q. S. (2010). *Cyber law and cyber security in developing and emerging economies*. Edward Elgar Publishing.

Shivhare, P., & Savaridassan, P. (2015). Addressing Security Issues of Small and Medium Enterprises through Enhanced SIEM Technology. *SSRN*. https://doi.org/10.2139/ssrn.2592463

Silva de Garcia, P., Oliveira, M., & Brohman, K. (2020). Knowledge sharing, hiding, and hoarding: How are they related? *Knowledge Management Research and Practice*, 1-13. https://doi.org/10.1080/14778238.2020.1774434

Singh, S. K. (2019). Territoriality, task performance, and workplace deviance: Empirical evidence on role of knowledge hiding. *Journal of Business Research*, *97*, 10–19. https://doi.org/10.1016/j.jbusres.2018.12.034

Sinkovics, R. R., Penz, E., & Ghauri, P. N. (2008). Enhancing the trustworthiness of qualitative research in international business. *Management International Review*, *48*(6), 689–714. https://doi.org/10.1007/s11575-008-0103-z

Smith, K. T., Smith, M., & Smith, J. L. (2010). Case studies of cybercrime and its impact on marketing activity and shareholder value. *Academy of Marketing Studies Journal, 15*(2), 67-81. http://ssrn.com/abstract=1724815

Sofyan, Y., De Clercq, D., & Shang, Y. (2021). Detrimental effects of work overload on knowledge hiding in competitive organizational climates. *Asia Pacific Journal of Human Resources*. https://doi.org/10.1111/1744-7941.12317

Soja, E., & Soja, P. (2020). Fostering ICT use by older workers. *Journal of Enterprise Information Management*, *33*(2), 407–434. https://doi.org/10.1108/jeim-12-2018-0282

Stefanidis, K., & Serpanos, D. (2005). Countermeasures against distributed denial of service attacks. *Proceedings of the 2005 IEEE Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Bulgaria.* https://doi.org/10.1109/IDAACS.2005.283019

Strand, K. L. (2018). *Influencing factors and effectiveness of a security awareness campaign* [Master's thesis, Norwegian University of Science and Technology]. NTNU Open. http://hdl.handle.net/11250/2565108

Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255-276. https://doi.org/10.1287/isre.1.3.255

Suhartanto, D., & Leo, G. (2018). Small business entrepreneur resistance of ICT adoption: a lesson from Indonesia. *International Journal of Business and Globalisation*, *21*(1), 5-18. https://ideas.repec.org/a/ids/ijbglo/v21y2018i1p5-18.html

Sultan, N. (2019). *Heuristic inquiry: Researching human experience holistically* (1st ed.). Sage.

Sumner, A., & Yuan, X. (2019). Mitigating phishing attacks: An overview. *Proceedings of the 2019 ACM Southeast Conference, USA,* 72-77. https://doi.org/10.1145/3299815.3314437

Tambunan, T. (2005). Promoting small and medium enterprises with a clustering approach: A policy experience from Indonesia. *Journal of Small Business Management*, *43*(2), 138-154. https://doi.org/10.1111/j.1540-627X.2005.00130.x

Tambunan, T. (2019). Recent evidence of the development of micro, small and medium enterprises in Indonesia. *Journal of Global Entrepreneurship Research*, *9*(1), 1-15. https://doi.org/10.1186/s40497-018-0140-4

Tambunan, T., & Busnetti, I. (2018). Small business use of the internet: Findings from Indonesia. *Asian Journal of Agricultural Extension, Economics & Sociology*, *28*(1), 1–15. https://doi.org/10.9734/ajaees/2018/44545

Thong, J. Y., & Yap, C. S. (1995). CEO characteristics, organizational characteristics and information technology adoption in small businesses. *Omega*, *23*(4), 429-442. https://doi.org/10.1016/0305-0483(95)00017-I

Udofot, M., & Topchyan, R. (2020). Factors related to small business cyber-attack protection in the United States. *International Journal of Cyber-Security and Digital Forensics*, *9*(1), 12–25. https://doi.org/10.17781/p002644

Umar, A., Sasongko, A. H., & Aguzman, G. (2018). Business model canvas as a solution for competing strategy of small business in Indonesia. *International Journal of Entrepreneurship*, *22*(1), 1-9. https://www.abacademies.org/articles/business-model-canvas-as-a-solution-for-competing-strategy-of-small-business-in-indonesia-7024.html

United Nations Conference on Trade and Development. (2005). Information Economy Report 2005.*United Nations Conference on Trade and Development (UNCTAD) Information Economy Report (IER)*. https://doi.org/10.18356/e2626460-en

United Nations Conference on Trade and Development. (2017). Information Economy Report 2017: Digitalization, Trade and Development. *United Nations Conference on Trade and Development (UNCTAD) Information Economy Report (IER).* https://doi.org/10.18356/3321e706-en

Van den Hooff, B., de Ridder, J., & Aukema, E. (2004). Exploring the eagerness to share knowledge: The role of social capital and ICT in knowledge sharing. *Social Capital and Information Technology*, *7*, 163-186. https://doi.org/10.7551/mitpress/6289.003.0010

Vinosa, D., Nastiti, T. (2020). Personal competitive and knowledge hiding: Moderating role of perceived task interdependence. [Doctoral dissertation, Universitas Gadjah Mada]. UGM Campus Repository. http://etd.repository.ugm.ac.id/penelitian/detail/193530

Viswanatha, A., Volz, D., & O'Keeffe, K. (2020, February 11*). Four members of China's military indicted over massive Equifax breach*. The Wall Street Journal. https://www.wsj.com/articles/four-members-of-china-s-military-indicted-for-massive-equifax-breach-11581346824.

Von Solms, B., & Kritzinger, E. (2011). Critical information infrastructure protection (CIIP) and cyber security in Africa: Has the CIIP and cyber security Rubicon been crossed? *Third International ICST Conference, AFRICOMM 2011, Tanzania.* https://doi.org/10.1007/978-3-642-29093-0_11

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security: What goes where? *Information and Computer Security*, *26*(1), 2-9. https://doi.org/10.1108/ICS-04-2017-0025

Wallen, E. S., & Mulloy, K. B. (2006). Computer-based training for safety: Comparing methods with older and younger workers. *Journal of Safety Research*, *37*(5), 461–467. https://doi.org/10.1016/j.jsr.2006.08.003

Weiss, J., Perkins, E., & Walls, A. (June 7, 2013). *Definition: Cybersecurity*. Gartner. https://www.gartner.com/en/documents/2510116/definition-cybersecurity

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and information security awareness. *Computers and Security*, *88*, 101640. https://doi.org/10.1016/j.cose.2019.101640

Yang, K., & Ribiere, V. (2020). Drivers of knowledge hiding in the university context. *Online Journal of Applied Knowledge Management*, *8*(1), 99–116. https://doi.org/10.36965/ojakm.2020.8(1)99-116

Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *The Qualitative Report*, *20*(2), 134–152. https://doi.org/10.46743/2160-3715/2015.2102

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, *19*(3), 321-332. https://doi.org/10.1177/1356389013497081

Yin, R. K. (2015). *Qualitative research from start to finish* (2nd ed.). Guilford.

Yin, R. K. (2017). *Case study research and applications: Design and methods* (6th ed.). Sage Publishing.

Zareen, M.S., Akhlaq, M., Tariq, M. & Khalid, U. (2013). Cyber security challenges and way forward for developing countries. *Proceedings from 2nd National Conference on Information Assurance, Pakistan.* https://doi.org/10.1109/NCIA.2013.6725318

Zhioua, S. (2013). The Middle East under malware attack dissecting cyber weapons. *Proceedings from IEEE 33rd International Conference on Distributed Computing Systems Workshops, USA,* 11-16. https://doi.org/10.1109/ICDCSW.2013.30

Zukowski, T., & Brown, I. (2007). Examining the influence of demographic factors on internet users' information privacy concerns. *SAICSIT '07: 2007 Annual Conference of the South African Institute of Computer Scientists and Information Technologists, South Africa.* https://doi.org/10.1145/1292491.1292514