Indiana State University
Sycamore Scholars

Electronic Theses and Dissertations

Fall 12-1-2023

In-person And Remote Employees And Information Security Policy Compliance

Joyce Mui

Follow this and additional works at: https://scholars.indianastate.edu/etds

Recommended Citation
Mui, Joyce, "In-person And Remote Employees And Information Security Policy Compliance" (2023). *Electronic Theses and Dissertations*. 7.
https://scholars.indianastate.edu/etds/7

This Dissertation is brought to you for free and open access by Sycamore Scholars. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of Sycamore Scholars. For more information, please contact dana.swinford@indstate.edu.

Joyce Y. Mui

Indiana State University (ISU)
Doctor of Philosophy (PhD), Technology Management, expected December 2023

Colorado State University (CSU), Global
Master of Project Management (MPM), specializing in Information Technology, June 2019

University of California, Los Angeles (UCLA)
Bachelor of Science (BS), Mathematics/Applied Science, specializing in Computing, June 2000

IN-PERSON AND REMOTE EMPLOYEES AND INFORMATION SECURITY POLICY COMPLIANCE

A Dissertation

Presented to

Graduate Studies

Bailey College of Engineering and Technology

Indiana State University

Terre Haute, Indiana

In Partial Fulfillment

of the Requirements for the Degree

PhD in Technology Management

---

by

Joyce Yin Mui

December 2023

© Joyce Yin Mui 2023

Keywords: technology management, data breach, employee behavior, security, compliance

COMMITTEE MEMBERS

Committee Chair: Barbara A. W. Eversole, PhD

Professor, Human Resource Development

Indiana State University

Committee Member: Cindy L. Crowder, PhD

Professor, Human Resource Development

Indiana State University

Committee Member: Philip J. Lunsford II, PhD, PE

Associate Professor Emeritus, Technology Systems

East Carolina University

ABSTRACT

Many workers have changed their working status from in-person to remote, in the past several years, with a large increase in the number of employees working remotely during and after the COVID-19 pandemic. In parallel, the increasing costs of data breaches and number of security incidents continue to be a concern to organizations seeking to protect their organization, systems, and data. This study's research questions were formed using a theoretical framework of the Theory of Planned Behavior (TPB) to discover influences on employee behavior and the Social Bonds Theory (SBT) to address strength of relationships and impact to compliance. This study investigated in-person and remote employees and their lived experiences with information security policies (ISP), seeking to gain understanding of employee lived experiences, relationships within organizations, and ISP compliance.

This qualitative study used the phenomenology research method to interview study participants, that worked in-person and remotely, to gather data. Lived experiences of both in-person and remote study participants covered their experiences such as with their organization's implementation and enforcement of ISP, organizational culture and leadership attitudes shaping ISP compliance, and clarity and training of ISP for employee audiences. Top factors that influenced employee compliance of ISPs of both in-person and remote study participants included the automation, hectic/busy times, efficiency, availability, training, and enforcement of the ISPs. Overall, study participants reported positive relationships within their organization, regardless of whether they were in-person or remote, however, nearly all study participants also

noted that building relationships was easier to do in-person than remote, even as technology has bridged some of the gap between in-person and remote working relationships.

PREFACE

Before, during, and just after the COVID-19 pandemic, I managed a HIPAA compliant environment, including the information security policies (ISP). As a practitioner and later-in-career researcher, I sought to blend my practitioner experiences with this dissertation study, combining my research interests with securing organizational systems and assets via cybersecurity frameworks and ISPs. As I saw daily, technology management is as much about the technology as it is about the people who interact with the system. The human resources and their behavior either increase or decrease the risks to the organization and its systems and data. This dissertation study was a personal and professional interest of mine and results in practical practitioner suggestions and proposed future research.

ACKNOWLEDGMENTS

I thank my amazing and hilarious immediate family, Britton and Declan Wright, for their support, love, and laughter, throughout this journey. To my extended family, thanks for tolerating us: Sally, Sherman, Lindsay, Azalea, Otis, Delilah, William, Clara (and the kids), Bao Bao, Yin Yin, Boo Boo, and last, but not least, Chuck. To my wonderful friends, professional network, and all the study participants (who I cannot identify!), my dissertation would not have been possible without you; thank you for your time, candidness, and willingness to participate! Finally, I would like to thank my advisor, Dr. Barbara Eversole, and my committee members, Drs. Crowder and Lunsford, for their feedback and support throughout my doctorate program.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Security and compliance are essential for consideration and implementation in organizations, regardless of industry, though of heightened importance for organizations in regulated industries. Employees must consider, comply with, and contribute to security and compliance to help organizations manage risk to organizational data, systems, and assets. Failure to manage threats and risks to organizational assets and comply to information security policies (ISP) increases risks to the organization, including potential fines (Gatzlaff & McCullough, 2010), bad press, and loss of customer trust (S. Ali et al., 2021). Data breaches may be the result of security and compliance failures and gaps, causing increases in organizational spending after data breach events to repair damage and upgrade information technology as a part of corrective actions (Choi et al., 2020; Kapoor & Nazareth, 2013).

Security and compliance are adjacent concepts and work together in organizations. Information security is how security is implemented to prevent risks or threats from becoming intrusions, incidents, or issues in an organization (R. Ali et al., 2021). Compliance is the paperwork and adherence to regulations, laws, and organizational policies and procedures (Kim & Kim, 2017). Employee compliance to ISP has become a focus to reduce risk and increase security of organizational assets as employees make decisions daily on compliance (Nasirpouri Shadbad & Biros, 2021). ISP refers to a variety of documentation in organizations, some of

which are highly technical policies and some that are more general. SANS Institute (2023) provided examples of ISP, including Acceptable Encryption Policy or Router and Switch Security Policy that were more technical policies for technical employees, as well as ISP that non-technical employees may be aware of, such as a Password Protection Policy or Email Policy. In this study, ISP referred to technical and non-technical ISPs, though with the broad sample population, many potential participants were only aware of non-technical ISPs.

In March 2020, the COVID-19 pandemic shut down many traditional office spaces across the United States (U.S.) and the world. As a result, remote work increased by 33% amongst U.S. organizations, with the information industry having over 50% of employees working remotely full-time (BLS, 2022). In the U.S., remote workers tripled between 2019 and 2021, from 5.7%, or 9 million people, to 17.9%, or 27.6 million people (Census Bureau, 2022). Employee technostress, or technology stress on individuals, increased because of COVID-19 as so many employees began working remotely (Singh et al., 2022). Meanwhile, increased stress has been found to lower ISP compliance (Trang & Nastjuk, 2021). This study explored today's post COVID-19 pandemic environment amongst the greater number of employees distributed across in-person and remote work environments, as well as employees' attitudes, behavioral factors, and potential relationships associated with ISP compliance. The cohort of study participants was employed individuals that worked either full-time remotely or in-person, at organizations that had at least one ISP that employees had to follow.

Background of the Study

Organizations use security and compliance measures to prevent risks from becoming security issues impacting the organization's data or systems. Organizations use ISP to provide guidance for standards and how to actively safeguard against threats, such as hacking or

employee mistakes (Alqahtani, 2017). Risks to an organization were not appropriately managed if employees do not comply with ISP, resulting in possible fines and lawsuits (San Nicolas-Rocca et al., 2014). With the increase of remote workers since the COVID-19 pandemic, much is unknown about in-person and remote employee attitudes, their intention to comply to ISP, and factors that influence ISP compliance.

IT Security

Information technology (IT) security within organizations, including information security and cybersecurity, were used to reference ways to secure organizational assets. Information security refers to the preservation of the information or data, which includes the confidentiality, integrity, and availability of the data, while cybersecurity protects computer systems in organizations where the data is hosted (Taherdoost, 2022). Security components include policies and procedures, standards, and implemented security tools to protect organizational assets from employee mishaps or abuse, as well as from environmental dangers and bad actors, such as hackers (Reid & Van Niekerk, 2014).

Organizations use IT security to ensure where their assets, which may be made up of data, computer systems, networks, and physical spaces where data, systems, or people, were located. Security standards, such as International Organization for Standardization (ISO), include considerations of the likelihood of risks or threats to the confidentiality, integrity, and availability of organizational systems (Taherdoost, 2022). Frequently, news stories report data breaches from organizations. Data breaches are the unintentional release of confidential data (PRC, 2019), whereas healthcare data breaches identify patients and must also contend with Health Insurance Portability and Accountability Act (HIPAA) guidelines (De Simone, 2019). Data breaches typically happen when some sort of failure in security occurs, whether that be a

misconfiguration, poor policy, or human error (Dolezel & McLeod, 2019).

For security to be effective, it must be considered from all angles of an organization, including internally, externally, and from ideas to products and services. Some organizations will have more formal security documentation, while others may document information security (IS) within their configurations and code, where the appropriateness of level of documentation is determined by the organization's risk tolerance and industry. For organizations that choose or are required to use formal cybersecurity documentation, best practices include cybersecurity frameworks and standards, such as National Institute of Standards and Technology (NIST) 800-171 and International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001, ISO/IEC 27002 (NIST, n.d.; ISO, n.d.; Kalaiprasath et al., 2017). The effectiveness of cybersecurity frameworks varies by implementation, which includes employee compliance and employee skill set to implement and comply, continuous improvement, and maintenance. Organizations may develop cybersecurity plans and security and compliance polices to protect organizational systems and to follow law and regulations for their industry.

Organizational Compliance

Some organizations may rarely consider compliance, depending on their industry and business needs, while others must follow regulations in most countries, such as the U.S. or countries in Europe and the European Union (EU). In the U.S., healthcare organizations must follow HIPAA guidelines, specifically the Privacy and Security Rule to protect individual electronic personal health information (PHI) via administrative, physical, and technical means (HHS, 2022). In the EU, the General Data Protection Regulation (GDPR) sets standards organizations must follow for privacy and security of data within the EU (GDPR, 2023). Thus, organizational compliance also varies from organization to organization, though most

organizations have some form of ISP with which they wish to comply.

ISP should be written practically and be relevant to organizations with continuous review and improvement to keep the documentation current and usable (Alqahtani, 2017). ISPs document organizational policies and general commitments, such as annual reviews of system interconnections, and work alongside procedures that detail processes, such as the role and manual steps required to complete the review of system interconnections. Both policies and procedures are intended to provide guidelines and instructions on how to secure organizational assets, or information systems (Angraini et al., 2019). ISP compliance typically refers to both compliance of the policies and procedures. Many scholars within the literature review use ISP interchangeably for information security policies and procedures, though they are slightly different. Other examples of ISP may include implementation guidelines within systems, password management, specifications of system automation and auditing, or manual procedures for employees to follow. For organizations whose industry is regulated, like banks or hospitals, ISP compliance is of higher importance and higher fines may be levied in the case of data breaches, when regulators audit the organization.

Employee Behavior and Human Factors in Security and Compliance

Organizational policies, including information security policy and compliance policy works alongside cybersecurity frameworks and standards to maintain guidelines for implementation of systems and maintenance, as well as employee actions and behaviors on behalf of an organization. Employee behavior is influenced by many factors including but not limited to family-work conflicts (Galanti et al., 2021), organizational leadership style (Guhr et al., 2019), inclusion in developing organizational procedures (Balozian et al., 2019), technostress (Nasirpouri Shadbad & Biros, 2022; Hwang et al., 2022), security awareness (Carmi & Bouhnik,

2020), and organizational culture (Alshaikh, 2020). Employees are potential insider threats to organizations, whether they intend to be malicious or not, by having access to and intimate knowledge of the organization (Balozian et al., 2019).

Statement of the Problem

Data breaches and other security incidents impact organization reputation, productivity, financials, and customer or patient privacy. Data breaches, especially in regulated industries, are expensive in terms of cost, time, and resources. The Ponemon Institute (2017), an independent research and education organization specializing in IT security and privacy practices, reported that $7.35 million is the average total cost of a data breach in the U.S., which is the highest average total cost in the past 12 years. Symantec (2014), an infrastructure and security company owned by Broadcom, reported that from October 2013 to September 2014 there were a total of 255 data breaches and 656 million identities exposed within the 157 countries that they monitor. Identity Theft Resource Center (ITRC) (2023) reported that in 2022, 87-92% of all U.S. data breaches were the result of cyberattacks, with phishing and related exploits being the cause, followed by ransomware. Edwards et al. (2016) used a public data set from the Privacy Rights Clearinghouse (PRC), a non-profit organization for data privacy, to predict that data breaches may cumulatively cost up to $179 billion over the next three years. Data breaches, and resulting fines from data breaches, may be mitigated, and managed by security and compliance measures. Employee behavior and actions impact the effectiveness of security and compliance in organizations, such that improving employee compliance to ISP increases security in organizations (Renaud et al., 2021).

The phone and internet company Verizon (2022) reported that 82% of data breaches involved human elements, such as stolen credentials, errors, phishing, or misuse. Humans

interact with organizational systems and are thus the users of systems. Users of a system may intentionally or unintentionally cause security incidents that result in such data breaches. One study conducted in 2020 showed that because of the COVID-19 pandemic, at least half of the employees sampled worked at home at least some of the time in July 2020, and one third worked at home all the time (Eurofound, 2020). In the U.S. during the pandemic, 71% of employees worked remotely (Pew Research Center, 2020), and after the pandemic in February 2022, 59% of employees, who can work remotely, were working remotely (Pew Research Center, 2022).

With the increased trend of remote work, organizations were also reporting that remote work has a strong correlation with data breaches. IBM Security (2022) stated that past data shows that when organizations have 81% to 100% of employees working remotely, the cost of a data breach averaged $5.10 million USD versus when organizations had 20% of employees working remotely, then the cost of a data breach averaged $3.99 million USD. BLS (2022) reported that in the U.S., large organizations with over 500 employees were more than twice as likely to have remote workers. In addition, the "educational services, finance and insurance, information, and management of companies" industries were more likely to have remote workers (BLS, 2022, para. 4). WEF (2023) reported that the top five industries in the U.S. that were offering hybrid or fully remote work were computer or mathematical, business and financial operations, legal, management, and architectural and engineering.

Malwarebytes (2020) conducted an opinion survey of over 200 IT managers, directors, and C-suite executives in the U.S. and found 20% of participants said that a security breach occurred in their organization due to a remote worker; in addition, only 16.2% of managers surveyed felt that their employees, either remote or in-person, were acutely aware of cybersecurity procedures. Checkpoint (2022) conducted a survey of 1200 security professionals

and found that 57% of the workforce works remotely, at least two days a week. The same study reported that 11% of respondents whose organizations allowed remote access did not require the use of common security tools for remote access, such as virtual private network (VPN), multi-factor authentication (MFA), device risk posture check, or zero trust network access.

Purpose of the Study

The purpose of this study was to describe and explain how the social bonds that leadership and management build with employees, and vice versa, influence employee attitudes and resulting behavior, specifically for ISP compliance. Hirschi's Social Bond Theory (SBT), also called Social Control Theory, claims that individuals who have social bonds or attachments to other persons within a community or society are less likely to have deviant behavior (Hirschi, 2017). The Theory of Planned Behavior (TPB) suggests that attitudes, norms, and perceived behavioral control contribute to individual intention and behavior (Ajzen, 1991). Thus, this study examined attitudes, intention, and factors contributing to employee compliance behavior. Applying SBT allowed insights into whether remote employees possess or lack social bonds to others in their organization that may lead to less compliant or deviant behavior, e.g., non-compliance with ISP. Further, the relationship between in-person and remote employees and managers may influence attitudes and intention and be a factor in resulting employee compliance behavior. Then through application of the TPB, along with SBT, insights were gained into the lived experiences of in-person and remote workers, including ISP compliance and behavior in the workplace.

As it was difficult to gain access to an organization's employee data for compliance, this study used self-reported data, using video conference tools to interview, from employees whose organizations require them to comply with ISP. While the interviewees were anonymized in this

study, employee demographics were gathered for industry, role, ISP awareness, and work status being in-person or remote. Then, the interviews explored employee bonds and attachment to their co-workers, leadership, and managers. Finally, the interviews gathered data on the phenomena of in-person and remote employees and ISP compliance, seeking to understand factors, attitudes, and intention to comply with ISP.

These research questions addressed gaps in the literature review and continue the conversation to understand the phenomena around today's in-person and remote working experiences and ISP compliance, as they impact overall organizational security and compliance posture.

1. What are in-person employee experiences with ISP compliance? (RQ1)
2. What are remote employee experiences with ISP compliance? (RQ2)
3. What factors influence in-person employees to comply with ISP compliance? (RQ3)
4. What factors influence remote employees to comply with ISP compliance? (RQ4)
5. What impact does a relationship between a manager and employee influence ISP compliance? (RQ5)

Significance of the Study

The recent COVID-19 pandemic which started approximately in March 2020 pushed many organizations to allow employees to work remotely (Pew Research Center, 2020). Many employees remained remote after the height of the pandemic, if their organization allowed remote work and they were physically able to work remotely (Pew Research Center, 2022). At the same time, the prevalence of internet crime complaints, such as hacking and social engineering or bad actors tricking employees into providing information or credentials, skyrocketed from approximately 350K in 2018 to 800K in 2022; losses from internet crimes

were at an all-time high at $10.3B in 2022 in the U.S., compared to losses of $2.7B in 2018 (FBI, 2022). Successful cyberattacks result in reputational damage and customer loss, along with significant costs, that threaten businesses and organizations (Meisner, 2018).

Organizations, especially regulated industries, should be concerned about the increasing costs of cyberattacks. As employees are the first and last line to implement and comply with best practices included in ISP, this study seeks to understand ISP compliance of employees. The understanding of lived experiences of in-person and remote employees and ISP compliance begins to address these phenomena.

Research is limited around in-person and remote employees' attitudes and intention to comply to ISP and factors that influence attitudes and intention to comply. Limited research exists on remote work, though much research exists surrounding ISP compliance and security and compliance in organizations. Previous research has been conducted on remote work, and separately, ISP compliance, though none has studied both critical areas in tandem. This study was significant as it started the conversation on discovering in-person and remote experiences and intentions to comply to ISP, and factors that influence in-person and remote behavior towards ISP compliance.

Assumptions

The selection criteria for participating in this study required participants be employed and familiar with their organization's ISP. This study assumed that participants were employed and familiar with their organization's ISP, where the concept of ISP was clearly understood by the participants. Since this study used self-reported data from participants, data gathered in this human behavior study relied on participants being accurate, honest, and truthful in their responses. ISP compliance varies widely between organizations, with employees in regulated

industries likely having the most strict or well-defined ISP, though this study did not exclude individuals from non-regulated industries. IBM (2022) reported that in 2021, only 5% of cyber-attacks were attributed to malicious insiders or employees with criminal intent; thus, in this study, employees were assumed to not have malicious intent.

Limitations

Limitations to this qualitative study existed and certain decisions were made which considered limited scope, time, cost, and resources. This study interviewed individuals that were employees at any organization, and the selection criteria for participation was employment with an organization either full-time in-person or full-time remote work (omitting employees who were hybrid workers). Another selection criterion was that the employee was aware of the presence of ISP within their organization that they were required to comply with. While the data collection attempted to create a remote natural setting, interviewing using a video collaboration tool may create awkwardness and stifle free flowing conversation for data collection. Interviews were based off a semi-structured interview guide. Follow up questions were asked as needed, probing on participants' responses, as is common when conducting research interviews (Creswell & Creswell, 2020).

While study participants will not be identified in study results, it was possible that participants were unwilling to be completely honest during the interview process to protect themselves or their organizations. As study participants were anonymous in the study, specific examples within organizations may have information redacted to protect the study participants and their organizations. The study's interviews were completed in the U.S., utilizing video capabilities, which may impact the ability of the researcher and study participant to communicate effectively. Despite outreach efforts, limitations of this study included recruitment of individuals

who heard about this study and self-selected to complete the interviews. This study was not intended to be generalizable and sought only to gather information from which to adequately answer the proposed research questions and meet the study objectives. This study provided insight into these topics leading to appropriate future research opportunities.

Definitions of Terms

Industry and academic journals vary on the terminology and definition of terms that were used within this study. This section clarifies the terminology and definitions that this study uses to clarify any definition variations. In addition, this section lists abbreviations used within this study.

Attitudes towards ISP: An individual's attitude is a part of their behavioral disposition and their feelings towards a behavior (Ajzen, 1991); in this study, the attitudes towards ISP were the employee's attitude and experiences towards their organization's ISP compliance.

Compliance to ISP: An individual, group, or organization's adherence to ISP, also may be thought of as to what extent were written ISP followed (Kim & Kim, 2017).

CSR: Corporate social responsibility

Deviant behavior: Behavior that is generally, by society or community standards, illegal or morally wrong (Hirschi, 2017). This study uses SBT as a theory for explaining deviant behavior where non-compliance is an ISP deviant behavior.

HIPAA: Health Insurance Portability and Accountability Act of 1966 (HHS, 2022).

Hybrid employees: Pullan (2022) described hybrid working as a mixed mode of working where some employees were in-person while others were remote. Hassan et al. (2022) agreed and defined hybrid work as employees that work one to four (out of five) working days, working remotely, and in the office the other days.

In-person employees: Individuals who work full-time in an office, provided by the employee's organization.

Intention to comply to ISP: An individual's intention is their motivation to behave in a certain way (Ajzen, 1991); the definition of intention to comply to ISP in this study is the employee's intention or motivation to comply with documented ISP in their organizations.

IS: Information security are the technical and administrative methods and implementation to protect organizational assets against threats and harm (Carmi & Bouhnik, 2020). Information security includes protection of confidentiality, integrity, and availability (CIA), though also appropriate access of systems and data (Lundgren & Möller, 2019).

ISP: Information security policy/policies (ISP) are organizational guidelines to protect assets including data and systems (Gwebu et al., 2020), whereas information security procedures (ISP) are the process and procedures of how to implement the security requirement (Carmi & Bouhnik, 2020). In this study, ISP compliance refers to either information security policy or procedure compliance that were meant for non-technical employees (e.g., Ethics Policy) and technical employees (e.g., Virtual Private Network Policy), though due to the inclusion criteria of this study, the focus of ISP questions will surround ISP understood by all employees, non-technical and technical (SANS Institute, 2023).

IT: Information technology

Non-compliance to ISP: Opposite of "compliance" where an individual, group, or organization's non-adherence to ISP or to what extent ISP is not followed (Kim & Kim, 2017). This study considers non-compliance to ISP a deviant behavior.

Phenomena: Phenomena, in phenomenology, are the experiences of humans in the world where humans live and meanings of those experiences; phenomenology is the study of phenomena (Vagle, 2018).

Remote employees: Individuals that work from home, telework or mobile work, where an employee works from their home and not the organization's office space (Shimura et al., 2021).

U.S.: United States of America

CHAPTER 2

LITERATURE REVIEW

The literature review assessed current literature around remote employees and employee behavior regarding security and compliance. Ayyagari (2012) analyzed public data breach trends and found that data breaches due to hacking were decreasing though data breaches due to the human element were increasing, leading to increasing focus on how organizations can minimize the human element contributing to data breaches such as enforcement of security policies. Since the COVID-19 pandemic, many office workers moved to remote working and continue to work remotely (Census Bureau, 2022). As employee work settings have changed recently and historically, this literature review is timely to discover research that exists around the new normal of remote work and ISP compliance. This literature review provides insight on the state of research in the primary areas of employee behavior and compliance and is agnostic to industry or job type of employees for the greatest volume of literature. Noticeably, a gap in literature exists for remote employees, specifically, around ISP compliance.

Security and Compliance

Even before the COVID-19 pandemic, security of systems was challenging for organizations and gaining employee ISP compliance was difficult. This part of the literature review will contain security and compliance literature not specific to COVID-19. The literature

covers existing studies for employee compliance to ISP, best practices, and ideas to increase security and compliance in organizations. Security and compliance are required together to protect organizations and reduce organizational risks. Here both topics were explored, though the focus of this study surrounded employee behavior and ISP compliance.

Employee Behavior and Compliance

Human behavior is influenced by many internal and external factors, and human behavior within a workplace context is even more complicated to study and explain. R. Ali et al. (2021) conducted a systematic review of literature of ISP compliance and found that compliant behaviors were influenced by factors such as national culture, intrinsic/extrinsic motivations, protection motivation behaviors, culture/aware behaviors, management behaviors, social behaviors, and actual compliance behaviors. Conversely, the study also found that security-related stress/neutralization, value conflicts, and deterrence were the primary factors in noncompliant behaviors. Kim & Han (2019) showed that corporate social responsibility (CSR) mediates ISP compliance positively and will influence employees to be compliant, despite costs of compliance. Human behavior is influenced by many factors making it difficult to pinpoint given knowledge and documented processes, why employees may choose to behave non-compliantly.

Employees bring their life personal norms into their attitudes towards security and compliance and social norms, all of which that factor into employee behavior and employee compliance (Bauer & Bernroider, 2017). Information security awareness (ISA), employee attitude, normative beliefs, and personal capabilities have a positive influence on ISP compliance (Carmi & Bouhnik, 2020), whereas higher employee workload is positively related to employee noncompliant behavior of clicking a phishing link in an email (Jalali et al., 2020). Non-

technology employees were influenced to comply with policies and procedures by self-efficacy and their perceived impact of the threat event (Hooper & Blunt, 2020). Culture, norms, leadership, personal motivations, and stress were common themes of influences of employee behavior regarding compliance behaviors, including ones that impact security within an organization.

Information Security Awareness

Information security awareness (ISA) programs intend to share information and knowledge with employees to reduce security risk and encourage compliant behavior. San Nicolas-Rocca et al. (2014) suggested that users need to participate in security initiatives to gain knowledge and promote collaboration and compliance with ISP. ISA may be designed for specific organizations, use various communication formats (e.g., videos, email, etc.), showcase real-world examples, and encourage feedback and interaction with ISA programs, to be more effective (Bauer et al., 2017). ISA best practices include relating security to employee personal lives, reinforcing security procedures and guidelines, creating a relaxed state of alert, and minimizing security fatigue (He & Zhang, 2019). Jaeger & Eckhardt (2021) proposed that ISA is situational, with experienced users more aware of security, phishing emails that were aligned with the employee's work reduce their notice of security cues, salient designed phishing emails draw users away from security cues than plain text, and security messages increase ISA. ISA increases knowledge of why certain protocols should be followed and markets security and compliance concepts to keep the topic fresh in the minds of employees to increase compliance.

Compliance Intention and Costs of Compliance

Employee intention to comply with policies and procedures is possibly the first step in compliance. Increasing employee knowledge of importance of security and compliance, the

consequences of security breaches, and employee awareness of their ISP compliance contribute to increasing ISP compliance (Ryutov et al., 2017). Compliance intention is also influenced by organizational commitment, social influence, and resource availability via self-efficacy (Herath & Rao, 2009). Jalali et al. (2020) indicated that collective felt trust and trust in information security technology contributed to compliance intention, but that compliance intention is not significantly related to compliance behavior. Even if employees intend on complying with organizational policies and procedures, knowledge, time, and other factors may disrupt the exchange from compliance intention to employee compliant behavior.

Many employees have a large workload and may already feel overextended to the point that the cost of being compliant may outweigh other responsibilities. Employees justify the decisions they make, whether to follow policies and rules in an organization or not, based on the cost of compliance, or if rules enable work or were disruptive (Hannah & Robertson, 2015; Herath & Rao, 2009; Hofeditz et al., 2017). Employees were more likely to be compliant with ISP when they realize the benefits of ISP compliance and the costs of ISP noncompliance (Kim & Han, 2019). Li et al. (2022) found that regular information security training is necessary to increase employee awareness of potential security risk severity and vulnerability to protect organizational assets. The same study recommends reducing perceived rewards for noncompliance and increasing employee perceived severity and self-efficacy will increase employee intention to comply with ISP. Organizations should ensure that employees understand the value of compliance and compliance processes so that they are not skipped, despite other job stresses.

Social Bonds

Social bonds in organizations create norms and contribute to culture. Feng et al. (2019)

used the SBT, where relationships between people and society prevent deviant behavior, to discover that the social bond partially mediates the impact of benevolent and moral leadership on ISP compliance. A different SBT-based study, Dong et al. (2021), found that top management control and IS security concerns contributed positively to nurse commitment and personal norms, resulting in increased social bonding in healthcare employees, like nurses, and ISP compliance.

Cheng et al. (2013) found that social control, using deterrence and SBT, influenced ISP compliance intentions based on employee bonds with other employees. Ali et al. (2020) agreed with the findings from Cheng et al. (2013) in that social bonds of employees improve ISP compliance. When social bonds in organizations were strong, employees were more likely to comply to ISP, as their peers and friends were also doing so.

Leadership

The focus of leadership draws attention of employees to specific areas. Hu et al. (2012) found that perceived top management participation in information security directly and indirectly influences employee attitudes, subjective norm, and perceived behavioral control, based on TPB, towards ISP compliance. In addition, this study indicated that top management plays an influential role in shaping organizational culture which also directly and indirectly influences employee attitudes, subjective norms, and perceived behavior control towards ISP compliance. Employees also appear to be motivated to behave compliantly when they believe that compliance is mandatory and that management is actively watching (Boss et al., 2009). With leadership focus on security and compliance, employee behavior may increase towards ISP compliance.

Influential leaders were often sought by organizations to implement change or motivate employees. In the case of ISP compliance, leadership styles impact organizations in different ways. In a Chinese study, Feng et al. (2019) researched the impact of paternalistic leadership, or

leadership that requires loyalty and obedience from employees in exchange for taking care of employees in a parental manner, and found that the factors of benevolence, morality, and authoritarianism within paternalistic leadership all positively influence ISP compliance. National culture may play a role in acceptable leadership styles, as Western cultures may not be as open to welcoming a paternalistic leadership style.

Other studies investigated different leadership styles and had similar findings of a type of leadership style that increased compliance via employee behavior. Guhr et al. (2019) investigated full-range leadership styles (transformational, transactional, and passive/avoidant) and found that transformational leadership is the most effective at achieving preferred employee information security behaviors, such as compliance to ISP. Balozian et al. (2019 p. 198) investigated "different levels of users (managers and employees) are affected by the same approaches (coercive vs. empowering) to ISP compliance" and found that the empowering approach is more effective for both managers and employees. However, the same study showed that managers required the justification of why to comply to increase their compliance, while employees were more likely to comply if they participated in developing the ISP. Another study suggested that the trust and friendliness of Irish managers were interpreted by employees as permission to behave in a noncompliant manner (Connolly et al., 2019). Leadership styles influence behavior, inspire employees, and possibly unintentionally condone poor compliance behavior.

Organizational Culture

Organizational culture supports the norms, general habits, and trends of an organization; work climates were like the feel and attitude of a work environment. Employee behavior is influenced by cybersecurity culture, which is a sub-culture within organizational culture, that may be developed with security education, training, and awareness initiatives that assist in

transforming behaviors into compliance (Alshaikh, 2020). Similarly, security culture drives employee compliance in organizations (D'Arcy & Greene, 2014). Gwebu et al. (2020) conducted a study that supports ethical work climates and neutralization as factors that explain ISP noncompliance, where work climates most likely to be compliant were principled, followed by benevolent, and then least likely egoistic. Organizational culture and work climates set expectations of employee behavior that carries through to employee behavior towards security and compliance processes.

National Culture

Every nation has a unique culture that is made up of historical influences and more modern influences which impact human behavior, attitudes, and norms. National culture influences the work environment and personal values, which may or may not align with ISP compliance (Karjalainen et al. (2020). Connolly et al. (2019) discovered that national culture played a role in compliance attitudes and behavior, where U.S. employees were more likely to behave compliantly and less likely to behave non-compliantly than their Irish counterparts. A suggestion from the study is that Ireland's national culture is a collectivist society that values personal relationships over tasks and organizations, whereas the U.S. individualistic society places tasks and organizations over personal relationships. Karjalainen et al. (2020) suggested that organizations must tailor learning of information security to national cultures who learn differently and that Western nations see ISP monitoring and sanctions as lack of trust from an organization, while Eastern nations accept these practices as "effective behavioral change strategies" (p. 20).

Safety Compliance

Safety compliance is a subset of compliance to organizational policies and procedures,

though geared at safety while performing a job function. Clark et al. (2014) confirmed the relationship between safety climate and safety compliance among nurses in a hospital setting, where the safety climate is determined by organizational leadership emphasis on safety and that organizational citizenship behavior (OCB), defined "as going above and beyond one's job description," has impact on overall work performance (p. 101). The same study found that leadership attitudes towards safety positively influenced safety compliance and behavior, as well as overall work performance, such as improved patient outcomes. Similarly, a study by Clarke (2013) used meta-analytic path analysis and found that for safety leadership, both active transactional and transformational leadership styles, contribute to effective safety leadership and safety climate, including safety compliance and participation, influencing employee behavior in these areas. Here, safety compliance is influenced by leadership and safety climate, with increased patient outcomes as a result.

Kark et al. (2015) conducted an experiment using leadership theory and self-regulatory focus theory with scenarios and surveys and found that transformational leadership is positively associated with situational promotion focus and in turn, safety initiative behaviors, while active transactional leadership positively influences employee prevention focus though a significant link was not found with active transactional leadership and safety behaviors. Approached from the negative leadership behavior angle, Yuan et al. (2020) found a link between abusive leadership to negative safety behaviors and compliance due to the emotional toll on employees.

Safety compliance will have challenges, including employee stress, financial insecurity, and perhaps personality type, despite encouragement of safety compliance with leadership and safety climate. Probst et al. (2020) found that employees with job and financial insecurity to have a negative relationship with compliance to Center for Disease Control and Prevention (CDC)'s

guidelines for COVID-19 prevention, whereas financially secure employees were more likely to be compliant to the CDC COVID guidelines. Ucho & Gbande (2012) concluded that type B personalities (defined as opposite of type A) and women were more compliant with their safety behaviors than type A personalities (defined as ambitious, aggressive, competitive, impatient, having muscle tension, rapid speech, irritation, hostility, and anger) and men; for gender, previous research suggested that women were more compliant to safety protocols. Safety compliance has direct impact on organizations, employees, or customers/patients, increasing its importance, though the act of compliance through employee behavior is still grouped with overall compliance to organizational policies and procedures.

Employee Behavior and Noncompliance

A lot of literature reflects studies' methods to increase employee compliance, and this section focuses on employee noncompliance which is when employees decide not to comply. Some employees may not want to be bothered or be too stressed to comply while others may have criminal intent in their noncompliance. While employee noncompliance is like employee compliance, the viewpoint to noncompliance peers into noncompliance side of employee behavior.

Technostress

Technostress is a concept that is becoming more popular in literature, though some were still unfamiliar with this concept. Technostress is the stress that technologies add to individuals; for example, employees may feel stress to comply with security polices and the use of security technologies (Hwang et al., 2022). Nasirpouri Shadbad & Biros (2022) investigated the impact of technostress, the negative stress of information technology (IT), on ISP compliance and found that employees justify their ISP noncompliant behavior based on the factors that cause

technostress. Technostress results in greater negative impacts on employee behavior of organizational commitment and compliance intention (Hwang et al., 2022; Hwang, & Cha, 2018), where promotion-focused personalities find stress with complying to security technology and policies and prevention-focused personalities did not (Hwang et al., 2022). Similarly, employees with high promotion focus experienced less technostress (Hwang, & Cha, 2018). Humans handle stress differently, including technostress, and stress can impact resulting human behavior to comply with ISP.

Noncompliance Deterrence

Employee compliance may be encouraged with rewards for compliance, though some organizations also put in place deterrence mechanisms to encourage employees to comply. Deterrence mechanisms include employee sanctions, and sanction certainty, severity, and celerity (or quickness of sanction response from the organization) were positivity associated with ISP compliance (Chen et al., 2020). Raddatz et al. (2020) found perceived sanction severity and perceived sanction certainty positively influence compliance intention to computer usage policies (a subset of ISP), though perceived sanction celerity was not found to influence compliance intention, where perceived sanction certainty had the strongest influence of employee compliance intention. The same study also found that employee awareness of being monitored positively and significantly influenced perceived sanction severity, perceived sanction certainty, and perceived sanction celerity, though the awareness of monitoring did not directly influence employee intention to comply with the policies.

Employees respond to ISP compliance with both the carrot and stick method, or with rewards and punishments respectively, where only employees with a high promotion focus were motivated by rewards (Liang et al., 2013). Trang & Brendel (2019) found that employee

sanctions influence employee deviant behavior and ISP compliance and that sanctions impact positive security behavior rather than negative, perhaps explained by risk-adverse employees exhibiting positive compliance behavior. Deterrence mechanisms appear to work mostly when they were consistently applied, though much research also may convince organizations that positive encouragement, such as influential and involved leaders, may work more effectively to entice employees to comply to ISP, rather than punishment.

Deliberate Acts of Noncompliance

Xin et al. (2020) focused their study on employees that maliciously commit acts upon organizational computers or assets, also called insider threats. The study used factors of self-control, hacking self-efficacy, moral beliefs, and organizational crime deterrence efforts, and collected data for the study using "scenario-based cross-sectional survey strategy" since the subject matter involved reporting or committing illegal activity (p. 1561). The study found that motivation was the primary driver and target suitability followed, for malicious computer abuse, and an individual's low self-control is a major driver for motivation to commit malicious computer abuse, where moral beliefs have a small moderating effect in a financial scenario only. In addition, the study found that deterrence nor guardianship influenced employees from committing malicious computer abuse.

Remote Work

Prior to COVID-19, remote work was not as prevalent, though did exist. Literature around remote work increased because of the pandemic and is included, though limited literature exists regarding remote workers and ISP compliance. Hatashima & Sakamoto (2017) provided the only remote worker and ISP compliance study found, prior to and after the COVID-19 pandemic. This study found that employees working with sensitive data were more careful to

follow organizational rules and regulations for ISP compliance, than those who did not.

Pandemic Remote Work

Remote work, or working from home (WFH), gained popularity for many organizations around March of 2020 when the pandemic made its way around the globe, increasing the numbers of employees working remotely temporarily and permanently (Pew Research Center, 2020). As a result of the COVID-19 pandemic, employees who began to work remotely had increased challenges to balance home and work life. Many employees struggled to balance work and home life, where self- leadership and autonomy were positively related to remote productivity and engagement, though family-work conflict and social isolation was negatively related to remote working stress (Galanti et al., 2021).

Pandemic Remote Work Stress

Employees globally experienced stress from global events, work, and home. Shimura et al. (2021) conducted a study in Japan and found that remote work reduces psychological and physical stress, though increased presenteeism or work productivity loss via sickness. A study from Latin America, conversely, found that remote work increased perceived stress, productivity, and engagement, but decreased work-life balance and work satisfaction, with perceived stress impacting men's productivity more than women's (Sandoval-Reyes et al., 2021). Another study in Germany also found increased perceived work-related stress and negative impact to mental and general health, possibly due to the lack of separation from work and home life, though self-efficacy mediates stress and health outcomes (Lange & Kayser, 2022). These studies from Japan, Latin America, and Germany did not specify industry of participants.

Stress presents in different ways and may vary based on the industry or country that a study was completed in. As a result, another study by Chudzicka-Czupała et al. (2023) found

conflicting results, where remote employees had lower stress severity than in-person employees. The same study found if in-person employees have a continuance commitment to their organizations and see no other alternatives at work will feel more stress. This study was completed with Polish employees in the education industry.

Other pandemic stress findings included that women experience more stress with remote work due to work life balance and women's home duties (Toscano et al., 2022). In addition, work and personal technostress impacts wellbeing where technology is used for both pleasure, such as watching television and using social media, as well as for work, blurring work and personal lives (Singh et al., 2022). The stress of the pandemic and push towards remote work impacted many, though the impact on work is not completely understood, though stress has been noted in previous studies as a factor in lower ISP compliance (Trang & Nastjuk, 2021; Nasirpouri Shadbad & Biros, 2021). The direct relationship of ISP compliance and increased remote workers and remote work has not yet been studied or found in the literature review; thus, this study may contribute to this literature.

Pandemic Remote Work Manager Relationship

Remote work during the pandemic impacted communication for many employees who were previously used to seeing their peers and managers in-person. Müller et al. (2022) suggested that not all jobs were suitable for remote work, even as organizations were pressured to allow remote work after the pandemic; to combat the challenges of remote work, training, communication and collaboration technology, and developing a good relationship with one's manager will assist remote workers in being successful. The leader-member exchange is a significant predictor, with strong trust and quality of the employee and manager relationship, in predicting job performance (Toscano et al., 2022). The quality of remote employee and manager

relationships may require further research, especially considering on-going remote work or for employees who were hired remotely and need to build a relationship with their manager remotely.

Pandemic Security Recommendations

While literature is lacking from the pandemic regarding ISP compliance and remote employee, literature exists providing recommendations for remote workers and security. Employee behavior is a risk of remote work and organizations should consider tools such as anti-virus, network security, and a security operations center (SOC) to combat cyberattacks (Kolomoets, 2022). Securing the remote workforce includes ensuring only the appropriate access to data is granted to the appropriate individuals, maintaining compliance with ISP and regulations like GDPR, securing computer systems, and supporting the remote employees (Fielding, 2020). With the increase of remote work, risks to organizations were also increasing including phishing attacks, conference bombing, and ransomware, though employees must follow organization ISP to mitigate some of these risks, including required automated configurations to limit the risk, rather than allowing employees to make bad decisions (Curran, 2020). The security recommendations provided for pandemic remote work are also found in best practices pre-COVID, however, the point is taken that these security best practices were more important with a distributed remote workforce.

Remote employees may not be as familiar with the organization as they may be with in-person work, reducing security emphasis and knowledge. Sidor-Rządkowska (2022) suggested that organizational culture that emphasizes security is the key to combat risks to cybersecurity, since processes may not be followed by employees. This finding is interesting and should be considered, however, other studies have found that having strong organizational culture increases

ISP compliance or following of processes (Sarkar et al. 2020; Nasir et al., 2019). Remote workers ISA is influenced by knowledge, behavior towards following security guidelines, and learning inertia, though not by attitude or experience inertia (Zhen et al., 2022). Remote employees may pose some risk with less exposure to organizational security measures, than those who were in-person, however, organizational culture and knowledge sharing were methods that all employees in-person and remote, may benefit from to increase security knowledge.

Theoretical Framework

Employee behavior is human behavior, in the context of a work environment. From the literature reviewed for employee behavior and security and compliance, employee behavior is often delivered in the context of human behavior theories such as deterrence theory (Hooper & Blunt, 2020; Raddatz et al., 2020; Trang & Brendel, 2019; Herath & Rao, 2009), the theory of planned behavior (Carmi & Bouhnik, 2020; Jalali et al., 2020; Hu et al., 2012), protection motivation theory (Li et al., 2022; Hooper & Blunt, 2020; Herath & Rao, 2009), conservation of resources theory (Hammer et al., 2016), rational choice theory (Kim & Han, 2019), social bond theory (Dong et al., 2021; Feng et al., 2019), self-regulatory focus (SRF) theory (Kark et al., 2015), theory of reasoned action (Hooper & Blunt, 2020; Bauer & Bernroider, 2017), and routine activity theory (RAT) (Xin et al., 2020). Human behavior theories may be applied to humans inside and outside of the work environment. For this study, human behavior theories were examined from the perspective of in-person and remote employees and work environments pertaining to ISP compliance.

To gain data and knowledge from the lived experiences of in-person and remote employees around ISP compliance, the theoretical framework for this study will use the TPB and SBT as a foundational basis. The TPB has been used in past studies to explain human security

and compliance behavior by using factors that influence the resulting behavior, such as the culture, peer behavior, or awareness (Hina et al., 2019). SBT has been used in past studies to explain crimes and delinquency behavior through social bonds, where the ongoing and changing of social bonds between individual relationships contribute to resulting delinquent behavior. (Mears & Stafford, 2022). With TPB to explain behavior and SBT to explain delinquent behavior towards ISP compliance, the two theories make up the theoretical framework for this study as a basis of explaining behaviors of in-person and remote employees.

Theory of Planned Behavior (TPB)

The TPB is a seminal social science theory used over several decades as well as in more recent research, such as research by Carmi & Bouhnik (2020), Hu et al. (2012), and Jalali et al. (2020), to predict and explain employee behavior. Cheng (2019) also reported that, in his study of intention and behavior with using technology, that TPB may be a stronger theory to use, if including factors such as social influence, versus other theories such as the technology acceptance model (TAM). Ajzen (1991) explained that human self-regulation plays an important role in behavior, rather than a human's attitude by itself. TPB extended the Theory of Reasoned Action by adding attitude and perceived behavioral control as influences on subjective norms and on an individual's intention, and these were both factors which can explain and predict employee behavior (Ajzen, 1991).

Steinmetz et al. (2016) found that behavior change interventions with TPB is more effective with public and group changes versus private or individual changes. The TPB focuses on an individual's intention to behave, by way of factors that influence the intention (Gross, 2017). Thus, when seeking to understand the lived experiences of employees and their intention to comply and compliance behavior to ISP, TPB aligns as a part of the theoretical framework.

TPB may be utilized flexibly based on the behavior topic being studied, though a free-response format to collect self-reported data from individuals is recommended to investigate attitudes, norms, and perceived behavior control towards the behavioral intention and behavior (Ajzen, 2020).

Social Bond Theory (SBT)

Past studies by Cheng et al. (2013), Feng et al. (2019) and Dong et al. (2021) used SBT as a basis of studying ISP compliance. Hirschi (2017) described SBT as studying the bonds that individuals have with society, where the less bonded an individual is, the more likely delinquent behavior is exhibited. Often, SBT is used when studying criminal thought and intent, though the elements of SBT may be applied to any behavior. Positive deviance may also be explained by SBT with positive deviance being the abstainers of poor behavior, in delinquent-forward environments (Wolfzorn et al., 2006). Bonds are formed with attachments, or affection for others in society, commitment to conformity, involvement in activities in the community, and beliefs in norms of the community (Hirschi, 2017). This study uses SBT to form questions in the interview guide to later explain social bonds between employees and managers and query the lived experiences of employees within ISP compliance and their work.

Cultures exist in many forms that impact social bonds, such as national or religious culture or culture in online communities. Zaidi et al. (2016) used SBT to study cultural impact to deviancy in adolescents and found that the three components, attachment, belief system, and commitment and involvement, of the SBT explain deviant behavior. This study found that strong attachment between adolescents and their parents, strong belief system, and commitment to and involvement in culturally acceptable activities, explains non-deviant behavior, and the opposite led to more deviant behaviors. Online communities typically have a weaker culture and social

links via members, though individuals with higher perceived internalization and identification bonds, or sense of belonging, and perceived communication and control will impact the quality of the online discussion (Shih & Huang, 2014). The proposed study uses TPB as a basis for explaining and predicting employee behavior together with SBT, where SBT may explain an employee's attitudes that contributes to TPB.

Summary

Many studies have covered ISP compliance and the factors that contribute to increasing ISP compliance. ISP compliance is complicated as the compliance is influenced by factors that align to the TPB intention and resulting behavior. Some factors that influence ISP compliance include management/leadership (Hu et al., 2012; R. Ali et al., 2021; Boss et al., 2009; Feng et al., 2019; Guhr et al., 2019), culture (R. Ali et al., 2021; Alshaikh, 2020; D'Arcy & Greene, 2014; Gwebu et al., 2020), motivations, and employee behaviors (R. Ali et al., 2021). Some factors that increase ISP compliance may include CSR (Kim & Han, 2019), norms (Bauer & Bernroider, 2017), ISA, attitudes, beliefs, individual capability (Carmi & Bouhnik, 2020), and employee social bonds (Feng et al., 2019; Dong et al., 2021; Cheng et al., 2013; Ali et al., 2020). Conversely, ISP non-compliance may include factors such as technostress (Hwang et al., 2022; Nasirpouri Shadbad & Biros, 2022; Hwang, & Cha, 2018) and deterrence mechanisms (Chen et al., 2020; Raddatz et al., 2020; Liang et al., 2013; Trang & Brendel, 2019).

Remote work has been studied a bit less than ISP compliance, though a flurry of recent studies has been conducted since the start of the COVID-19 pandemic. Pandemic remote work studies include challenges of balancing work and home life, as well as social isolation (Galanti et al., 2021), and stress (Shimura et al., 2021; Sandoval-Reyes et al., 2021; Lange & Kayser, 2022; Chudzicka-Czupała et al., 2023; Toscano et al., 2022; Singh et al., 2022). SBT was selected as

part of the theoretical framework for this study to further build on and explore remote employees' and managers' relationship (Müller et al., 2022; Toscano et al., 2022). Best practices for remote work include having an organizational culture that supports security (Sidor-Rządkowska, 2022) and ISA (Zhen et al., 2022).

From the literature review, the TPB and SBT were found to support this study of lived experiences of in-person and remote employees. TPB takes the perspective of explaining or predicting employee behavior via intention towards a behavior (Ajzen, 1991) that may be applied to this study as the intention of in-person and remote employees to comply with ISP. SBT uses the basis of attachments affection, commitment to conformity, and involvement in community to form social bonds to explain human behavior in terms of delinquency (Hirschi, 2017). Together, TPB is used to explain behavior and SBT to explain deviant behavior of employees, as the foundational theoretical framework behind the lived experienced study of in-person and remote employees and ISP compliance.

Since the COVID-19 pandemic, more studies have been conducted because of the increase of remote workers. However, a gap in literature exists with regards to ISP compliance and remote employees distinctly. IBM Security (2022) noted that the cost of data breaches was higher for organizations that had most of their employees working remotely. More research is needed to evaluate in-person versus remote employees and their ISP compliance. Literature, such as Ayyagari (2012), has shown that employee ISP compliance or employee behavior within their organizations is a cause of increasing data breaches. Combined, a gap in research exists and this study intends to begin exploration of employee lived experiences as in-person and remote employees and their ISP behavior.

CHAPTER 3

RESEARCH METHODOLOGY

Research Design and Methodology

This study utilized qualitative research, specifically the phenomenological design method, as an approach to interview participants and gather data. Qualitative research is popular in social science and health research and allows participants to hear from non-researchers in their voice, while gaining in-depth data on a topic area (Thelwall & Nevill, 2021). Qualitative studies are useful to discover the understanding of human experiences by interpreting data collected through the qualitative lens (Creswell & Creswell, 2020). Qualitative research and understanding experiences with technology may be understood using the phenomenological method for research (Cilesiz, 2011), where phenomenological research uncovers and describes the lived experiences of individuals to understand the phenomena (van Manen, 2016). This study applied the phenomenological design of qualitative methods to obtain rich data that captures the essence of the lived experience (Husserl & Moran, 2001) of employees on their attitudes and intentions toward complying to ISP.

Human behavior—and more specifically decisions employees make—were the primary factors affecting ISP compliance. Thus, studying employee attitudes, intention, and factors

towards ISP compliance, through application of the SBT and TPB, answered this study's research questions. Articles cited within the literature review used various methodologies based on the respective studies' research aims and research questions. Frequently, studies around ISP compliance and employee intention have used surveys to collect data regarding employee attitudes, intention, and behavior. The advantage of the qualitative approach taken in this study was the ability to gather in-depth, rich data that will contribute back to the research knowledge base (Elo et al., 2014). Semi-structured interviews allowed study participants to fully elaborate on the questions asked without being restricted to a survey research design.

Creswell & Creswell (2020) noted that using a phenomenological research design invites interview participants to detail their experiences of a phenomena where phenomena include "attitudes, beliefs, opinion, feeling, and the like" (Percy et al., 2015, p. 77). For example, human science is a lived experience whereas phenomenology is the study of individual experiences, as human behavior is a phenomenon of experience, not an objective reality (Sloan & Bowe, 2014). Phenomenology research is personal and considers two concepts, epoché, withholding judgment, and bracketing, removing preconceived notions, to genuinely consider the participants and their contributions to get to the meaning and understanding of the information (Larsen & Adu, 2021). In this study, the phenomena were the experiences of those working in-person and remote and the attitudes, intention, and factors of employee behavior to ISP compliance, as well as the influences of relationships within organizations.

In qualitative designs, researchers shape the direction and interpretation of the research which is called reflexivity (Creswell & Creswell, 2020). Reflexivity in qualitative studies is important to the study and should include the researcher's point of view and standpoint to evaluate potential impact on the research and findings (Anderson, 2017). For this study, the

researcher's industry background was securing and managing HIPAA complaint technology systems, including logging and identifying violations committed against ISP. The researcher's interest was to understand the phenomena, especially within the context of many organizations or departments working remotely due to the pandemic. The researcher has attempted to avoid preconceived notions when gathering, analyzing, and interpreting data from the participants.

Study Population

This study's population was voluntary participants who were able to spend approximately one hour on a video call with the study researcher. The pre-screening requirements were that participants affirmed that they were employed by an organization (not self-employed), work either 100% remote or in-person (or close to 100%) and were aware that there were ISP that their organization required them to follow. The selection of the sample population was a convenience sample (Creswell & Creswell, 2020), based on the selection criteria and the convenience and availability of the participant for the interview. A summary of participant inclusion criteria was as follows:

- Participant agreed to spend approximately one hour in a video call with researcher.
- Participant confirmed that they were employed by an organization, not self-employed.
- Participant confirmed that they work full-time 100% remote or 100% in-person.
- Participant was aware that their organization required them to follow at least one ISP.

Sample Size

Qualitative research does not require large numbers of participants and random sampling like in quantitative research, instead, qualitative research should "purposefully select participants" "that will best help the researcher understand the problem and the research question" (Creswell & Creswell, 2020, p. 262). Hennink & Kaiser (2022) found that saturation,

where no additional data was discovered, was achieved after 9-17 interviews, though Saunders & Townsend (2016) recommended an interview population of 15-60 participants for workplace and organization research studies. For phenomenological studies, Creswell & Creswell (2020) recommend a sample size of 3-10. Due to the varied recommendations, this study aimed to recruit and gather no more than 20 participants with approximately half of the population 100% remote and the other half of the population 100% in-person. Saturation in qualitative research should be flexible based on the research, as it is a "statement about the unobserved based on the observed" (Saunders et al., 2018, p. 1904). The final sample size of this study was reached when saturation occurred, and the researcher felt that they would not hear any new information from continuing to interview additional participants.

Study Recruitment

The study sample population was recruited from the researcher's personal and professional networks within the U.S., though the participants were not known to the researcher personally. The researcher requested volunteers verbally, via email, and via a social media contact, through direct messages in LinkedIn. Recruitment used approved Institutional Review Board (IRB) script language that explained the study, purpose, and criteria for participants. A recruitment email and verbal recruitment script was developed and reviewed by the university IRB prior to sending to target participants for recruitment. Participants did not have a personal relationship with the researcher and were not first-degree contacts in LinkedIn during the study research period (though participants may become first degree LinkedIn contacts with the researcher after the study was completed). The recruitment email and verbal recruitment script contained content including the request for their time, purpose of the research, requested method of contact (e.g., video interview), any known risks to the research, and contact information for

participation or questions. A written verbal consent document was also delivered, via email, for review and verbal consent to each participant, prior to including the participant in the study.

Instruments and Data Collection

For qualitative research via interview, the researcher is the instrument, though a technical instrument may be used to record the conversation (Creswell & Creswell, 2020). This study recorded and transcribed interview conversations for clarity, though the primary data collection method was notes from the researcher-participant interview. An interview guide was used, containing approximately ten questions to prompt the participant, though the semi-structured interview also allowed for discovery and a free flowing of conversation and information. The researcher typed notes live and after the interview directly into a word processor. The phenomenological approach interview questions were based on SBT and TPB, where SBT considers attachments, commitment, involvement, and beliefs (Hirschi, 2017) and TPB is based on attitude, perceived behavioral control, subjective norm, and intention, as factors to predict behavior (Ajzen, 1991).

In the post-COVID-19 era, video interviews and online chats are now acceptable to use for research interviews, though a notable downside of chatting is the lack of intonation and emotional tone (Gunawan et al., 2022). This study primarily used video interviews to reduce boundaries of location and increase the participant pool. The participant may have elected to use the online interview technology without turning on their video, though the researcher preferred having video capabilities enabled to have a more in-person interview experience. Email was only used for quick follow-ups after the primary interviews were completed, as necessary.

This study's interviews were semi-structured and allowed the interviewer to weave though the participant's thought process. Demographic data was gathered at the end of each

interview. Semi-structured interviews gather similar data around specific areas, allowing for follow up and divergent threads of thought (Gill et al., 2008). The phenomenological method suggests that interview questions be broad in nature and gather experiences from individuals (Creswell & Creswell, 2020). To gather deep and natural feedback of participants and their experience, phenomenological interviews should be conversational and allow the participant to talk (Vagle, 2018). The qualitative interview method was used to collect data for research on "views, experiences, beliefs and/or motivations of individuals on specific matters" (Gill et al., 2008, p. 292). The interviews extracted rich data from the participants, based on the semi-structured interview questions, leaving room for the participant to add their experiences to the topic area.

Interview Guide

The interview began with a brief introduction from the researcher that provided insight to the researcher and their background, so that the participant felt comfortable and gained understanding of the line of interview questions. Guiding the interview, the researcher built a rapport with the participant, expanded into the semi-structured interview with the interview questions, and closed the interview with demographic questions. The researcher set the tone for the interview to allow for free-flowing conversation, targeted for no longer than 60 minutes. The interview guide is found in Appendix A.

Data Collection Procedure

The researcher utilized an inductive interview process with an interview protocol as a basis of the data collection, writing notes directly into the interview word processing file. Each of these interview protocol files was also the participant information form and was kept separately in a folder for each participant. At the same time, interviews were recorded and stored

as a media file, using a video chat tool, whether the video capability was turned on or if the interview was voice only.

Data collected was identifiable back to the participant, though kept confidential to the researcher and the researcher's advisor who completed an audit of the research process, including the data collected. The anonymization of individuals happened when transitioning from the interview transcripts into the output of the data for analysis by replacing names with pseudonyms and removing sensitive identifying data. Data was stored locally on the researcher's device and backed up on the researcher's Google Drive private instance. The researcher used the principle of least privilege to secure access to the participant's data within Google Drive, as well as using a default deny all external connections firewall on their device.

Field Notes and Memos

Field notes and memos provided additional context to the research process, along with the data collected from participants. Field notes were another layer to qualitative research that were also used for secondary analysis and meta-synthesis and to construct "thick, rich descriptions of the study context, encounter, interview, focus group, and document's valuable contextual data" (Phillippi & Lauderdale, 2018, p. 381). Memos were notes taken during the research process by the researcher and were valuable in qualitative research in which the researcher immersed themselves in the research (Birks et al., 2008). Both field notes and memos were useful for additional data analysis from the research process and were tools to assist the researcher with writing of the narrative of the study's findings.

Data Analysis

The data analysis of qualitative research data used thematic analysis applied to interview notes and interview transcripts, where each participant's data was coded to identify concepts and

themes (Nowell et al., 2017). The interviews were transcribed with the assistance of an automated transcribing tool and validated by the researcher. Coding transcripts is a process to identify patterns from large amounts of data and begins the process of sorting through what data may be important for a study and what may not be (Auerbach & Silverstein, 2003). With all data coded, the data was organized and integrated for analysis. Data analysis in phenomenology studies should "bracket assumptions, identify nonrepetitive and nonoverlapping statements in interview transcripts (horizontalization), and create textural and structural descriptions of the experience" (Hays & Wood, 2011, p. 289).

Interview transcripts were coded and analyzed with ATLAS.ti, qualitative research software. Although an automated transcription tool was used, transcripts were validated manually by the researcher. Transcript data was imported into ATLAS.ti and a first level analysis using the word cloud feature was used to gather popular and relevant concepts within the interviews. ATLAS.ti was used manually to code inductively and deductively and was documented in a codebook which served as the code system for this study. Finally, analysis and visualizations were completed, as appropriate, to establish relationships in the data, find patterns, and suggest further areas of research.

First Cycle Coding

The coding began with deductive codes, based on the interview guide, that started the initial codebook. With coding line-by-line, inductive codes emerged which further categorized qualitative data and increased rigor of data analysis (Oliveira, 2022). The first level of coding used the data collected from the interviews to analyze the text within the data to identify relevant data excerpts through "speech acts" (Larsen & Adu, 2021). Labels or codes were applied to pieces of data, which included phrases or sentences, and may be "descriptive, theoretical,

emotional, reflective" (Bhattacharya, 2017, p. 150). This initial line-by-line coding was both deductive—codes were created based on interview guide questions—and inductive or in vivo coding, where codes emerge from the participant's exact words (Rogers, 2018). This study uploaded transcripts into ATLAS.ti to manually check results of the automated ATLAS.ti tool for initial coding. The purpose of the first cycle coding was to find phrases and concepts that were common, match demographic data to parsed excerpt data, and create categories of concepts (Larsen & Adu, 2021).

Second Cycle Coding

This study's next level of coding was focused on creating categories and themes of concepts that were used to answer the study's research questions. The second cycle coding identified emerging themes based on commonalities and relationships (Deterding & Waters, 2021), and used focused coding in the second cycle to search for the frequent or significant codes (Rogers, 2018). "Themes, or categories, are the classification of more discrete concepts," whereas expressions were symbolic of a theme (Ryan & Bernard, 2003, p. 87). Then, the emerging themes were transformed into meaningful themes (Larsen & Adu, 2021). Themes were identified using various techniques including repetitions, metaphors and analogies, transitions, similarities and differences, linguistic connectors, or missing data (Ryan & Bernard, 2003).

Validity, Reliability, and Generalizability

Qualitative research has been criticized for lacking validity and reliability (Anderson, 2017). This study addressed validity and reliability, while focusing on gathering data from the point of view of people and their self-reported behavior. The quality of qualitative studies is found in the research design, researcher credibility, plausibility of findings, and research method applicability (Rose & Johnson, 2020). Qualitative research assumes that "multiple realities" exist

and seeks to interpret the data from values, beliefs, and experiences (Anderson, 2017, p. 126). Qualitative research must consider validity, reliability, and generalizability just as quantitative research does, however the implementation of each should be adjusted to the qualitative method (Leung, 2015). This study considered both validity and reliability, though was not intended to be generalizable as generalizability was not an expected outcome.

Validity

For qualitative research, validity addresses the appropriateness of the tools, process, and data used within a study, including if the research question was answered using this method with the study's sample population (Leung, 2015). Alternatively, validity for qualitative research may be labeled "truth value" indicating that the qualitative method for validation is that multiple interpretations may exist, though participant perspectives were accurately reflected in the study (Noble & Smith, 2015, p. 34). Many tools capture validity including member checking, triangulation, crystallization, rich descriptions, peer debriefing, and an audit trail (Rose & Johnson, 2020). Epoché and brackets are also tools to validate that data collected and interpreted is the essence of the experience using common sense and previous knowledge about the phenomena (Cilesiz, 2011). This study achieved validity by maintaining and ensuring accuracy of documents and recordings of the interviews and inviting participants to comment on transcripts and research findings. The researcher's advisor also audited records from the research process for this study.

Reliability

For qualitative research, reliability is the "exact replicability of the process and results" (Leung, 2015, p. 326). Consistency and neutrality are terms that may be used in qualitative research along with or instead of reliability to indicate that other researchers using the same

methods should find similar findings and separating the truth value of the researcher bias and participant contributions, respectively (Noble & Smith, 2015). Rose & Johnson (2020) added that reliability means that a reasonable researcher should be able to use the research design and have similar results and analysis. This study maintained a clear interview process, including documentation on any issues that arose during the research of this study to provide adequate information that allowed a reasonable researcher to replicate the study.

Ethical Considerations

While the interviewing process is very personal, this research anonymized the identity of participants and their organizations in the study findings. The results and findings from this study may be considered sensitive to participants and their organizations, especially if participants were admitting that they do not necessarily follow organizational ISP. Participants in phenomenological interviews shared personal and intimate details about their lives, thus, ensuring participant privacy and data security was a priority (Cilesiz, 2011). The research notes contained the identity of the participants to ensure validity by sending participants transcripts to validate transcripts and summary findings, though the findings within the study obscured participants and organization identity.

The research process took steps to ensure ethical research was conducted. First, the researcher obtained verbal consent from each participant prior to collecting data from participants. Informed consent is an ethical research standard to ensure that participants that take part in voluntary research understand the proposed research and their participation in it (Xu et al., 2020). Also, the researcher and participant well-being and interests were important to consider from an ethical perspective, throughout the research process, as in some cases, the guidelines were not clear for every decision in the research process, including in the reporting

and interpretation of the data (Mitchell & Irvine, 2008). Here, the researcher was transparent and self-respective to hold themselves accountable for the research and process. The study proposal was also taken to the IRB for human subjects' research review to ensure proper process and approvals were gained, prior to executing the study design.

Summary

The summary of the research methodology detailed the process of this study design. Target population and recruitment was discussed, along with the sample size of the target population. Sample demographics and interview questions were presented in the proposal design to provide context to the study's aim of data collection. The data collection process via interviews and data analysis using ATLAS.ti was also included. The research methodology also addressed validity and reliability concerns within this qualitative research. Using this research methodology, data was collected and analyzed for in-person and remote employees and their attitudes, intention, and factors of ISP compliance.

CHAPTER 4

RESULTS

This qualitative research study conducted N=20 semi-structured interviews, with twelve mostly remote participants and eight mostly in-person participants. Initially, the researcher intended on having a completely even split of in-person and remote participants, however, as recruitment moved forward for both in-person and remote participants, the researcher found that there were more remote participants identified and willing to complete the interview. The researcher completed the interviews in order of convenience to the participants, from June to August 2023. As the researcher completed the first 16 interviews, there were 12 remote participant interviews and only four in-person participants. Upon reaching 12 remote participants, the researcher culled recruitment of all participants to focus solely on in-person participants to ensure that the balance of participants between remote and in-person interviews were not completely unbalanced.

Field Notes and Memos

The researcher took field notes and memos throughout the data collection and data analysis process and collected anecdotal data to the study to provide context and potential areas that may be improved on for similar studies in the future. Field notes data collected include impressions and notes from electronic and verbal conversations had, feelings, thoughts or ideas about tactic changes, observations, possible explanations of the data, and reflections from the

researcher. For this study, field notes topics focus mainly on the data collection process, rather than the data analysis.

Most of the in-person study participants commented that they chose to be in-person, rather than being mandated to return to the office by their organization. Some of the in-person participants who chose to be in the office claimed that they worked better in an office due to their life situations, liked to socialize, or that their work was more easily done in an office. One of the in-person participants thought that the in-person requirement was not reasonable as the organization proved that during the pandemic that the efficiency and effectiveness of the organization remained strong. Another in-person participant was a school librarian and had to work in-person to work in the library with the students.

Demographics

After the data collection (interview and Zoom automated transcription), the participants' identities were stripped from their transcripts and the data for data analysis. The demographics of the participants are shown in Table 1. Age was calculated based on birth year and the current year, 2023. The generation of study participants was identified using birth year and CGK (2023) approximate generation guide of the following:

- Gen Z: 1996-2015
- Millennials/Gen Y: 1977-1995
- Generation X: 1965-1976
- Baby Boomers: 1946-1964
- Traditionalists/Silent Generation: Born before 1945

Table 1

Study Participant Demographics Generation and Age

Generation	Age	Number of Study Participants	Percentage
Gen Z	8-27	0	0%
Millennials	28-46	8	40%
Generation X	47-58	11	55%
Baby Boomers	59-77	1	5%
Traditionalists	78+	0	0%
Total	N/A	20	100%

Note. The median age of the participants was approximately 44.

Most study participants were from Generation X at 55% with 11 study participants in this age range, followed closely by Millennials at 40% or eight participants. There was only one Baby Boomer in this study which comprised of only 5% of the study population. In Table 2, the study participant's gender demographics are displayed. Study participants were overwhelmingly male; females recruited to participate in the interview cited lack of knowledge and comfortability as reasons they did not wish to participate. Overall, 85% of participants were male and 15% female, with Generation X having two female participants or 18% of the Generation X study participant population and Millennials having one female participant or 12.5% of the Millennial study population.

Table 2

Study Participant Demographics Gender

Generation	Male	Percentage Male	Female	Percentage Female	Total
Millennials	7	87.5%	1	12.5%	8
Generation X	9	82%	2	18%	11
Baby Boomers	1	100%	0	0%	1
Total	17	85%	3	15%	20

Note. One of the Generation X female participants worked in-person. The other two female participants, one Millennial and one Generation X, worked remotely.

Location

Study participants were all located in the U.S. with most of the organizations for which the participants worked also located in the U.S. In Table 3, the distribution of the location of study participants ranged from the majority in Colorado with 10 participants or 50% of the study population to three participants in Florida, or 15% of the study population. Finally, California hosted two study participants or 10% of the study population, while Alabama, Georgia, Indiana, North Carolina, and South Carolina all had a single participant or 5% each of the study population. The organizations that the participants worked for were headquartered around the U.S. from California, Colorado, Connecticut, Florida, Illinois, Minnesota, New Jersey, New York, North Carolina, and Texas. Only one of the study participant's organizations was headquartered outside the U.S., in Ireland.

Table 3

Study Participant Demographics Location

Participant Location	Number of participants	Percentage
CO	10	50%
FL	3	15%
CA	2	10%
AL	1	5%
GA	1	5%
IN	1	5%
NC	1	5%
SC	1	5%
Total	20	100%

Note. Most of the participants were in Colorado as the researcher is also located in Colorado.

Titles

As expected, the study participants had a wide range of titles, with none of the titles matching other participant's titles. As such, the researcher grouped engineers and technologists, security operations and security managers, senior/lead engineer and systems analyst type titles, and any director or director of engineering title together. In Table 4, a summary of the study participant's titles is shown, where senior engineers/analysts, considered technology experts, top the charts with seven participants, making up 35% of the participants in the study. Closely following, director of engineering and security operations/manager titles were represented by four participants each and 20% of the participants each. Finally, the engineer/technologist category had two participants or 10% of study participants and Claim Team Manager, VP of

Origination, and School Librarian all had one participant each and represented 5% of the study population each.

Table 4

Study Participant Job Title Demographics

Title	Number of participants	Percentage
Senior/Lead Engineer or Analyst	7	35%
Director of Engineering	4	20%
Security Ops/Manager	4	20%
Engineer/Technologist	2	10%
Claim Team Manager	1	5%
VP of Origination	1	5%
School Librarian	1	5%
Total	20	100%

Note. The lead systems analyst participant acted in an engineering-similar role, thus was grouped with the senior/lead engineers.

Industry

Similarly, to the study participant titles, few of the participants cited working in the same industry. The researcher also grouped like categories such as insurance and finance into financial services and software security and information security into security services. In Table 5, financial services led the most study participant's industry at four or 20% of the population, followed by healthcare at three participants or 15%, security services at two participants or 10%, and supply chain at two participants or 10%. Adverting, automotive, cloud services, contract and compliance, education, engineering, government, and management technology consulting each

had one study participant or 5% of the study population.

Table 5

Study Participant Industry Demographics

Title	Number of participants	Percentage
Financial Services	4	20%
Healthcare	3	15%
Security Services	2	10%
Supply Chain	2	10%
Advertising	1	5%
Automotive	1	5%
Cloud Services	1	5%
Contract and Compliance	1	5%
Education	1	5%
Electronics	1	5%
Engineering	1	5%
Government	1	5%
Management Technology Consulting	1	5%
Total	20	100%

Note. The lead systems analyst participant acted in an engineering-similar role, thus was grouped with the senior/lead engineers.

Self-Rated ISP Familiarity

As a part of the demographics section in the interview guide, a question requested that study participants rate their familiarity with ISPs on a scale of 1 to 5, with 5 being extremely

familiar with ISPs. Many participant responses included halves or between two numbers. For simplicity, the researcher rounded up; for instance, if a participant ranked themselves a 4.5, the ISP familiarity rating was rounded up to a 5. Similarly, if a participant ranked themselves a 2 or a 3, the researcher used the higher number. In Table 6, seven participants or 35% gave themselves a 5 for ISP familiarity, followed by six participants or 30% ranking themselves a 3. Twenty-five percent or five participants rated themselves a 4, and two participants or 10% gave themselves a 2. None of the participants ranked themselves a 1 for ISP familiarity.

Table 6

Study Participant ISP Familiarity Self-Rating

Self-Rating	Number of participants	Percentage
5	7	35%
4	5	25%
3	6	30%
2	2	10%
1	0	0%
Total	20	100%

Note. The average ISP familiarity self-rating was 3.85 out of 5.

Qualitative Data Analysis

Interviews were transcribed by Zoom after the cloud recording, however, the interviews transcribed did not completely capture each word spoken and required a few manual tweaks to correct words or add missing words. The researcher manually read and redacted any identifiable data from the transcripts, including names, organization name, or any organization proprietary data such as the name of a software that is developed by or for the organization that might

inadvertently identify the organization. With the interview data gathered reviewed, corrected, and redacted, the transcript text files were then uploaded into ATLAS.TI as documents.

First Cycle Codes

First cycle coding was completed using deductive codes derived from the interview guide and research questions. Several reviews of the transcripts were used as a method to identify passages and words within the transcripts for the coding. As the interview was semi-structured, the interviews took various threads with each participant, and interviews were coded with inductive codes as well during the first cycle coding. The emerging codes in the first cycle coding analysis presented the basis for the second cycle coding analysis. Relationships within and between the codes were noticed anecdotally during this manual transcript review. 63 first cycle codes were documented in a codebook and within ATLAS.TI, which per Linneberg & Korsgaard (2019) is within the guidelines for number of initial codes, 50 to 70. During first cycle coding, the researcher first coded generally, but realized that more detailed coding was required to complete second cycle coding for themes to emerge. Most codes from first cycle coding were inductive codes, rather than deductive codes.

Figure 1

Word Code Cloud from ATLAS.TI

Note. The more frequently used codes are in the center and in larger text, while the less frequently used codes are smaller and on the edges.

Second Cycle Coding

The first cycle codes were used to begin second cycle coding. Table 7 displays the hierarchical grouping of codes and themes that emerged from second cycle coding. The themes were identified in Table 7, from the transcript interview data. The eight themes were factors that influence following ISP, increase ISP compliance, ISP intention, organization ISP stance, organizational relationships, remote versus in-person, result of non-compliance to ISP, and types of ISPs.

Table 7

Second Cycle Coding Themes

Theme	Number of Codes
Factors that influence following ISP	15
Increase ISP compliance	14
ISP intention	5
Organization ISP stance	2
Organizational relationships	4
Remote vs in-person	5
Result of non-compliance to ISP	11
Types of ISPs	15

Note. Six codes were reused in the "factors that influence following ISP" and "increase ISP compliance" themes.

Themes

The eight themes that emerged from the data analysis were factors that influence following ISP, increase ISP compliance, ISP intention, organization ISP stance, organizational relationships, remote versus in-person, result of non-compliance to ISP, and types of ISPs. The intention of ISPs in organizations, the organization's ISP stance, results of non-compliance, and types of ISPs contribute to the lived experiences of ISP compliance, or RQ1 and RQ2. Factors that influence whether an individual will follow ISPs and ways to increase ISP compliance directly related to the research questions RQ3 and RQ4 in this study. Organizational relationships, as a theme, targets RQ5 though also provides context to RQ1 and RQ2.

Study participants have been de-identified, though for readability, each study participant

was assigned a pseudonym. The pseudonym names begin with “R” for the remote study participants, and “I” names for the in-person study participants. See Appendix D for a full list of the pseudonyms, matched with their generation.

The lived experiences of study participants were categorized into themes of ISP intention, organization ISP stance, results of non-compliance to ISP, and types of ISPs. The theme of remote or in-person also contributes to RQ1 and RQ2 and RQ3 and RQ4, though overall there were not clear and definitive lines between in-person and remote experiences. Thus, the remote versus in-person theme is discussed separately at the end of the results chapter. Organizational relationships also contribute to the lived experiences of study participants, though analysis of organizational relationship data is found with the RQ5 results.

RQ1: What are in-person employee experiences with ISP compliance?

In-person lived experiences with ISP compliance contains the themes of ISP intention, organization ISP stance, result of non-compliance to ISP, and types of ISPs. The in-person lived experiences vary between the individuals, with some in-person lived experiences being technical in nature and more heavily integrated with ISP compliance, while other in-person study participants knew of fewer ISPs and were more aligned with high level ISP compliance such as phishing policies.

ISP Intention

The intention of ISPs in organizations is the purpose of why the documents exist. Table 8 illustrates the in-person study participants’ interview responses to ISP intention.

Table 8

ISP Intention from In-Person Participants

Intention	In-Person	% In-Person
Protect data	7	88%
Protect the organization & system	7	88%
Protect customers	3	38%
Meet regulations	1	13%
Communicate intent	0	0%

Note. One intention was counted per study participant, for each category, even if the participant mentioned the intention multiple times in their interview. Percentage in-person was calculated with eight in-person study participants.

Protect Data/Customers/Organization & System

Although separate codes, the codes of protect data, protect customers, and protect organization & system were combined in this write-up as the concepts overlap and were very similar. Irvin remarked that ISPs "protect the company from cyber-attacks, breaches, ransomware" and "protect patients, identifying information, and patient health information." Isaac said that ISP were to ensure "data security' and that "person's information is protected." Ike remarked that ISPs were to "protect the clients" and "some type of data." Ira similarly added that ISPs were to "protect private information," "our data," and "ourselves as a company." Iver said that ISP were to protect data and reduce risk of "being compromised," while Isadora contributed that ISP intention was to protect confidentiality and privacy. Ilya also cited protecting the company, confidentiality, and protecting information as reasons ISPs exist.

Meet Regulations

One in-person participant, Ivan, related that meeting regulations was the intention of ISPs and cited HIPAA, GCPR, and the California Consumer Privacy Act (CCPA).

Communicate Intent

None of the in-person study participants mentioned communicates intent as an ISP intention.

Organizational ISP Stance

Table 9 shows the stance of in-person study participants' lived experiences in their organization and their determination of if the ISP stance was mandatory or nice to have. ISP stance was determined by the participant's answer to the interview question of if ISP compliance was mandatory or nice to have in their organization. Not all participants answered the question of their organization's stance and some participants responded that ISP were both mandatory and nice to have.

Table 9

Organization's ISP Stance According to In-Person Participants

Stance	In-Person	% In-Person
Mandatory	4	50%
Nice to have	5	63%

Note. One stance was counted per study participant, for each category, even if the participant mentioned the stance multiple times in their interview. Percentage in-person was calculated with eight in-person study participants.

Mandatory

50% of in-person study participants responded that ISPs were considered mandatory in

their organization. Iver provided a caveat on data type, “mandatory compliance depending on the classification level.” Irvin said that ISP compliance was “mandatory, but it’s because it’s enforced.”

Nice to Have

Isaac commented, “smaller ma and pa type organizations don't always do that [mandatory ISPs].” Ike noted that they have “never had anything be enforced” leading them to believe that ISP compliance is a nice to have. Ilya commented “both my companies [that I’ve worked for] were very, very lax on this whole ISP thing.”

Both

Ira responded that ISP compliance is a “mix of both” mandatory and nice to have in their organization.

Result of Non-Compliance to ISPs

In-person study participants noted their organization’s response or potential response to non-compliance to ISPs. In Table 10, the responses were tallied.

Table 10

Results of Non-Compliance to ISPs for In-Person Participants

Results	In-Person	% In-Person
Security incident	7	88%
Termination	4	50%
Additional coaching/training	3	38%
Written warning	3	38%
Severity dependent	2	25%
Check clarity of policy	1	13%
Fines and lawsuits	1	13%
No consequences	1	13%
Verbal discussion	1	13%
Loss of reputation	0	0%
Removal of access	0	0%

Note. One result was counted per study participant, for each category, even if the participant mentioned the result multiple times in their interview. Percentage in-person was calculated with eight in-person study participants.

Security Incident

Seven out of eight in-person study participants had experiences with security incidents because of ISP non-compliance. In this study, a security incident is any incident, including an actual data breach, that breaks ISPs. Ira described a vendor breach:

> It freaks a lot of people out. And then we have to start from scratch with whatever process is related to it and see how we can continue to do what we need to do. While

> working around the vendor, while they're figuring out their stuff and getting their stuff back online or back in order from the breach, our legal department will get involved. Our compliance department will get involved. So, [will] the business unit itself that's affected by it. So, there's usually a lot of different higher ups from a lot of different areas of the company that will get on one giant Zoom call and start hashing things out.

Ivan recalled how a simple mistake could break ISP and be a security incident:

> One of the things that is common in ISPs in a call center environment is personal cell phones [not] being allowed on the call center floor… As we all know, cell phones can do a lot and one of the reasons that those policies exist is because there are many times where credit card number needs to be taken on the [call center] phone or sensitive information needs to be passed or personally identifiable information (PII) is passed over the phone… Usually their [ISP] policies say no pens, no paper [either]… because a call center agent [may be] being nefarious and could write it [PII] down, but it could be an example where a person may not truly understand [the why], somebody that maybe wasn't properly trained, and they have their cell phone on out and playing or taking notes.

One in-person study participant described near misses of security incidents related to phishing and another one described an actual security incident resulting from the phishing. Irvin contributed:

> Our CFO clicked on a phishing email and entered his information one time. The only reason that we were able to catch it as quick as we did is because we had previously put the fear of God in him. [We previously told him] if you don't do what we're telling you to do and your account gets breached, you are going to f--- our company. And he panicked when he realized what he'd done and reached out to us literally within two minutes. And

> we're able to deactivate his account, revoke all sign in sessions, change his password, and do all that stuff. Then, [we] monitored his account in the upcoming weeks to see if people were trying to get into it. But the only reason that happened was because we had literally told him, you are one of the least compliant people in the company. You consistently do it [are non-compliant] and if you are one of the people who gets breached, our company is going to be in serious trouble because of you and it will be your fault. And so, when he did mess up, he got scared, and so it worked out nicely for us, but it like could have not been great.

Ilya described an actual security incident and data breach:

> I worked at a previous company who had just basically one [IT] guy. It's kind of limited, and it's very difficult for him because you can only do so much when everyone has the power to click on a malicious email. So, we were actually breached, and they held our information up for ransom, for Bitcoin. So, it was some guy overseas, I think, in like Saudi Arabia or something, and we were able to track the IP back and say, hey, you guys have our information. So, we [the organization] had to negotiate a deal, but they [the blackmailer] said our company had to pay... so yeah, our company had to pay.

Termination

Results of non-compliance to ISPs may result in termination, possibly depending on the severity or intent of the incident. 50% of in-person study participants mentioned termination or loss of employment as a potential result of non-compliance to ISP. Isaac said a potential result might be “employment loss,” and Irvin agreed, providing an example, “One person was terminated when they refused to do their information security training.”

Additional Coaching/Training

38% of in-person study participants noted additional coaching/training as a result of non-compliance to ISP in their organization and experience. Ivan mentioned “coaching or training,” while Iver agreed that their organization provides a counseling session in the event of non-compliance. Irvin said, “We will basically sit them down and get them remedial training.”

Written Warning

If the situation warrants a written warning in response to a security incident as a result of non-compliance, some organizations will provide a written warning, according to three in-person study participants. Irvin stated, “if you do not follow our information security program, you will get a warning and an attempt at remediation.”

Severity Dependent

Results of non-compliance in organizations depend heavily on what the incident was. Two in-person study participants mentioned that in their organization, the resulting “what happens” after an ISP is not complied to, depends on how severe the incident was. Iver said each incident was “handled with a degree of concern that they were shown in the disregard for the ISP.” Ivan also noted the severity of the incident is handled on a “case to case basis” and dependent on if the “breaking of the policy” was “intentional and done through ill will.”

Check Clarity of Policy

When employees were non-compliant, the issue may be in the clarity of the ISP itself, one in-person study participant pointed out. Ivan commented, “if a person truly didn't understand what he or she was doing was wrong, then… the policy should be reviewed to make sure that it was clear. That what they were doing was wrong.”

Fines and Lawsuits

If non-compliance to ISPs results in data breaches or compromise of laws, fines and lawsuits may be a result. One in-person study participant mentioned fines or lawsuits that may result from ISP non-compliance. Isaac noted “monetary fines” as a possible issue.

No Consequences

Non-compliance to ISPs may result in no consequences, an adjacent code to the ISP organizational stance of nice to have. Only one in-person participant, Ilya, mentioned that “no one really gets reprimanded” for non-compliance to ISPs.

Verbal Discussion

One in-person study participant mentioned verbal discussions as a potential result of non-compliance to ISPs. Ilya presented an example in their organization,

> There was a guy who actually clicked on to malicious emails like two weeks in a row. I'm like, Oh, my, gosh! This guy's a fool. And he did get a speaking to by like one of our guys in the place to say hey, you should watch out about where you're clicking.

Loss of Reputation

None of the in-person study participants mentioned loss of reputation.

Removal of Access

None of the in-person study participants mentioned removal of access as a result of non-compliance to ISP.

Types of ISPs

A total of 15 policies were mentioned by study participants during the interviews as shown in Table 11. Study participants did not necessarily know the names of policies and many simply provided examples of a policy that they knew about in their organization that impacted

them. The researcher grouped together examples and like-policies; for example, logging into a computer with a username and password and two factor authentication (2FA) or multi-factor authentication (MFA) was grouped into the authentication/authorization policy group. Types of ISPs were a part of the lived experiences of study participants, contributing to answering the research questions RQ1 and RQ2 of the experiences of in-person and remote study participants with ISP compliance. Types of ISPs may contribute to as factors that influence in-person and remote study participants with ISP compliance, in RQ3 and RQ4, as many participants could not name many polices that they had to comply to, so lack of awareness or knowledge of ISPs may contribute as a factor of compliance.

Table 11

Types of ISPs Mentioned by In-Person Study Participants

ISPs	In-Person	% In-Person
Authentication	7	88%
Data Security	6	75%
Training	5	63%
Network	4	50%
Vulnerability Management	4	50%
Acceptable Use	2	25%
Access Control	2	25%
Mobile Device	2	25%
Personnel Security	2	25%
Contracts	1	13%
Disaster Recovery	1	13%
Incident Response	1	13%
Information Security Program	1	13%
Logging, Monitoring, and Alerting	1	13%
Change Management	0	0%

Note. One ISP was counted per study participant, for each category, even if the participant mentioned the policy multiple times in their interview. Percentage in-person was calculated with eight in-person study participants.

Authentication

A frequently mentioned policy, seven out of eight in-person study participants mentioned

authentication in their interviews. 88% of in-person study participants mentioned authentication as a policy, which is the highest percentage of all the policies mentioned for in-person participants. A few participants mentioned session limits or timeouts with authentication. The overwhelming majority of the participants cited passwords and MFA as their example, which included using a vendor application or phone to obtain a code. Ira spoke about passwords and having a "different password for each application."

Data Security

Data security policies including encryption, handling, and classification, topped the number of non-repeat and unique mentions by the study participants. Six or 75% of in-person study participants cited examples of data security in the interviews. Notably, methods of data security varied from participants, which included encryption of data in transit, via email, mobile devices and on servers, as well as data masking, access, classification, scrubbing identifiable information, and data loss prevention tools. Isadora contributed that the security training included "what information is okay to share. And what information isn't okay to share."

Training

Six in-person participants reported annual training requirements from their organization. Methods of training included classes and videos.

Network

Network polices were mentioned by four or 50% of in-person study participants. The comments about the network include physical access restrictions to the network, remote access, VPN, network encryption, and firewalls blocking access to external websites. Irvin stated, "If you are not in America, you cannot access any of our information, no matter what."

Vulnerability Management

Four or 50% of in-person study participants mentioned vulnerability management examples in their interviews, with stopping or reacting to phishing attempts at the top of the examples. Tools and methods that participants mentioned that assist with vulnerability management include endpoint protection, antivirus, software management tools, or patches.

Acceptable Use

This study defined acceptable use as what employees can and cannot do on organization time or with organization equipment. Two in-person study participants mentioned acceptable use or examples of acceptable use policies, including use of social media, representing the organization, behavior, and unauthorized use of unapproved software. Ivan explained, “Things like acceptable use, social media. Things like don't take an email from my client, drop it into chatGPT, and let it go out on the inter-webs for everyone to then mine it.”

Access Control

This study defined access control as both access management and access control for organizational systems. Two in-person study participants commented on access control in their organizations or provided examples given in the interview for access control include Active Directory groups, the organization’s network or virtual private network (VPN), user access versus elevated or administrator access, email, applications, folders or drive access, and local access to servers. Isaac explained, “administrator personnel have a higher level of privileges than a basic user,” and Irvin agreed that there were “levels of access based on the role the person has.”

Mobile Device

Mobile devices may include workstations, laptops, tablets, or mobile phones. Two in-person study participants, Isaac and Irvin, provided examples that included use of USB or thumb

drives, encryption, and system hardening.

Personnel Security

Examples grouped in the personnel security policies were clean desk, clean screen, screen protector, locking laptops and devices, locking paper with sensitive information, shredding paper with sensitive information, and badge access. Two in-person participants reported personnel security examples in their interviews. Isadora said that they "shut down my computer when I leave" but their computer is "not always in a locked area." Irvin stated that policy requires that employees, "Put the notes into a cabinet at their desk that has a lock on it" and to be careful, "Don't allow anyone to store passwords or anything like that on post-it notes."

Contracts

Only one in-person study participant referred to contracts policies. Irvin mentioned the procurement process with a vendor, including completing a risk assessment on the vendor and purchase.

Disaster Recovery

Only one participant, Irvin, provided examples of disaster recovery type policies in their interview. The examples of disaster recovery policies included how to handle fires in a server room and backups to systems and data.

Incident Response

This study defines incident response as what the organizational policy is if there is an incident to investigate, stop or report on. Incidents may include anything from malicious malware infecting the organization's system or accidents that involve unauthorized release of identifiable data. One in-person study participant mentioned incident response.

Information Security Program

Irvin was the only study participant to mention an overarching information security program document that governs the organization and subsequent policies.

Logging, Monitoring, and Alerting

Only one in-person participant mentioned logging, monitoring, and alerting in their interviews. Ilya provided an example of their organization logging screenshots of their desktop to be able to investigate what each employee in the organization is doing at any time, "someone can actually remotely log in and basically look at screenshots of every second that I am clicking through or seeing on my screen."

Change Management

None of the in-person participants mentioned change management policies.

Summary of In-Person Lived Experiences with ISP Compliance

The themes of ISP intention, organization ISP stance, result of non-compliance to ISP, and types of ISPs were used to answer RQ1: What are in-person employee experiences with ISP compliance? One in-person participant mentioned that ISPs were present to meet regulations, while the majority mentioned that the intention of ISPs were to protect customers, data, and the organization or system. One in-person participant said that ISPs were both mandatory and nice to have in their organization, depending on what the subject was, while half of the participants said that ISP compliance was mandatory, according to their organization. Seven or 88% of in-person participants reported that security incidents were the result of non-compliance to ISPs, followed by termination, additional coaching/training, and written warning as the next most popular. Finally, the in-person study participants mentioned authentication policies as the most popular or well-known policy, followed by data security, training, network, and vulnerability management

as the next frequently mentioned ISPs.

The results show the varied answers and experiences from the in-person study participants' interviews. The information technologists with engineering, systems, web, or security in their titles or industry, such as Isaac, Ira, Ivan, Irvin, Ira, and Ike, had a greater depth and breadth of understanding of ISPs. These in-person technologists were able to explain how some ISPs were implemented and how some of the ISPs fit into their organization's IT strategy. The security and compliance in-person participant knew ISPs extremely well, as they were the person in their organization who wrote the majority of the ISPs and enforced their implementation. The in-person non-technical librarian and finance participants, Isadora and Ilya, were aware of ISPs, though their knowledge of ISPs in their organizations were more limited to what ISP was required for them to login and complete their job functions. For the in-person participants, it is possible that the organization did not have many written ISPs or because their position did not require them to be more closely involved with a greater number of ISPs. The lived experiences of in-person participants appeared to differ based on the participant's job function and organization.

RQ2: What are remote employee experiences with ISP compliance?

As with RQ1, the remote lived experiences with ISP compliance contains the themes of ISP intention, organization ISP stance, result of non-compliance to ISP, and types of ISPs. Most of the remote study participants worked jobs that were technical in nature, e.g., software or systems engineers or security or compliance. As a result, the lived experiences of remote employees showed a more technical side of ISP compliance.

ISP Intention

The intention of ISPs in organizations is the purpose of why the documents exist. Table

12 illustrates remote study participants' interview responses to a question about ISP intention. Roman said the intention of ISPs was to "CYA," while Rhett said specific data may be "considered classified as security information. And we don't obviously want that information to be leaked out. It's private."

Table 12

ISP Intention from Remote Participants

Intention	Remote	% Remote
Meet regulations	8	67%
Protect the organization & system	6	50%
Protect data	5	42%
Protect customers	4	33%
Communicate intent	1	8%

Note. One intention was counted per study participant, for each category, even if the participant mentioned the intention multiple times in their interview. Percentage of remote participants was calculated with 12 remote study participants.

Meet Regulations

Eight or 67% of remote study participants said that the intention of ISPs was to meet regulations or demonstrate compliance. Rupert commented, "NIST 800-53 is just a good general place to start for us. We have HIPAA as well that we have to comply with. We have state-based regulations that we have to deal with. We have international compliance and regulatory requirements." Remote study participants also mentioned the following frameworks, standards, and regulations: GDPR, CCPA, SOC 2, ISO 27001, and PCI, DSS.

Protect Data/Customers/Organization & System

Although separate codes, the codes of protect data, protect customers, and protect organization & system were combined in this write-up as the concepts overlap and were very similar. Remington said "[ISPs] are protective to the organization. It's to protect proprietary data. It's to protect personal information." Rupert agreed that ISPs intend to prevent "IP (intellectual property) leaking." Rhys responded, "it's up to us… as a security professional, to try and give them some guardrails [through ISPs] and some controls that help them manage risky situations because data breaches sensitive information." Rex commented:

> Any time you work with customer data, customer information, especially in the medical field, you've got data bursts. You've got address, social. The potential for fraud is very great, so we all have to be very vigilant. What we [try to] do each day is to make sure that we keep our customers information safe, so they don't get hacked and just abused by other third parties.

Communicates Intent

One remote study participant, Rhys stated, "ISPs should communicate executive management leadership and company intent."

Organizational ISP Stance

One of the questions in the interview guide requested the study participants' opinion on if their organization considered ISP compliance mandatory or nice to have. Table 13 shows the stance of remote study participants' lived experiences in their organization and their determination of if the ISP stance was mandatory or nice to have. Not all participants answered the question of their organization's stance and some participants responded that ISP were both mandatory and nice to have.

Table 13

Organization's ISP Stance According to Remote Participants

Stance	Remote	% Remote
Mandatory	6	50%
Nice to have	3	25%

Note. One stance was counted per study participant, for each category, even if the participant mentioned the stance multiple times in their interview. Percentage of remote participants was calculated with 12 remote study participants.

Mandatory

50% of remote study participants responded that ISPs were considered mandatory in their organization. Rex proclaimed that ISP compliance was "10 out of 10 mandatory," and Raven agreed that "ISPs are applicable to every employee in our organization." Rhett also provided a caveat to mandatory ISP compliance, depending on the leader, "it all depends on the commander, how bad do they want to drop the hammer?"

Nice to Have

Three remote study participants responded that ISP compliance was nice to have. Rufus elaborated, "in small companies, they don't even have the bandwidth to even state a policy in most cases."

Both

Raven commented that ISP compliance is mandatory or nice to have in their organization, depending on the manager.

Result of Non-Compliance to ISPs

Study participants noted their organization's response or potential response to non-

compliance to ISPs. In Table 14, the responses were tallied.

Table 14

Results of Non-Compliance to ISPs for Remote Participants

Results	Remote	% Remote
Security incident	9	75%
Termination	9	75%
Severity dependent	5	42%
Verbal discussion	5	42%
Written warning	4	33%
Fines and lawsuits	4	33%
Additional coaching/training	3	25%
No consequences	3	25%
Removal of access	2	17%
Loss of reputation	1	8%
Check clarity of policy	0	0%

Note. One result was counted per study participant, for each category, even if the participant mentioned the result multiple times in their interview. Percentage of remote participants was calculated with 12 remote study participants.

Security Incident

Many remote study participants, nine or 75%, had experiences with security incidents as a result of ISP non-compliance. In this study, a security incident is any incident, including an actual data breach, that breaks ISPs. Raven offered, “We've seen people breach an ISP, and then we end up with a security incident.” Rusty described a data breach at their organization, caused

by a customer, and said in the aftermath of the breach, the organization and employees learned a lot and “really tightened up.” Rhett provided an example of a security incident of a secret mission posted online,

> They [military personnel] usually go out on drug intervention. The members are told that [they] are personnel on these boats that you're not supposed to tell your family or friends or anything where you're going… then a [military branch member], [on] a whole social media craze [posts online], “Heading out. Can't wait to get the Puerto Rico!” Well, now we know you're leaving [your base in] [redacted] and you're going to Puerto Rico. Your pathway is pretty much defined, and it was completely by accident, obviously.

Raven described a phishing incident in their organization,

> She [an employee] clicked on something to update her printer driver through a number of other clicks. She ended up on a scam website where she was talking to somebody from "HP" to help her with her printer. They remoted into her computer, which was breach of ISP. and we worked with her to fix it because once she realized what she had done, she immediately came to us and said, here's this thing that happened. And we [reacted with] you're now network quarantined and we're wiping your machine. Thankfully, I don't think that there was anything on it, and there was nothing that spread. So, it was not a big breach incident… We were like just please be very careful. Don't do things like that again. Here's where you went wrong but thank you for coming to us so that we could help you fix the issue.

Termination

Results of non-compliance to ISPs may result in termination, possibly depending on the

severity or intent of the incident. Nine or 75% of remote study participants mentioned termination or loss of employment as a potential result of non-compliance to ISP. Roman shared that, “People have been fired for tripping DLP (data loss prevention)” in their organization, and Rex said if the incident was at a “criminal level where you're going in clicking on these things and then using that information to open up credit cards or something that would be instant termination.”

Similarly, Raven revealed,

> There was somebody [an employee] who was sharing data routinely, not following the ISP controls, having an issue. And I think he was very recently hired, and my manager is actually moving to have him terminated because he is such a huge security issue.

Remington recalled incidents in previous organizations where:

> People have been fired for exposing parts of pre-production cars, which I think is really harsh. It's really difficult to exist in the wild with a pre-production car and not have people follow you around for photo. Photograph you… for having basically a paparazzo like follow you around.

Severity Dependent

Results of non-compliance in organizations depend heavily on what the incident was. Five remote study participants mentioned that in their organization, the resulting “what happens” after an ISP is not complied with, depends on how severe the incident was. Rusty commented that the severity of an incident determines if it goes beyond the direct manager to human resources (HR) or the Chief Information Security Officer (CISO). Rex agreed that incidents were reviewed with the leader and HR, if needed. As Rupert said, “there's cases where something is so

egregious that that you just can't let it slide." If the incident was "something small and it causes no real harm," Rhett said the result could "be as simple as a verbal warning."

Verbal Discussion

Five or 42% of remote study participants mentioned verbal discussions as a potential result of non-compliance to ISPs. Rex explained, "If you didn't [follow ISP], then that was a discussion, and we'd have continued performance management." Rusty said, the process included, "sitting down with the person and going through the process and make sure it doesn't happen again."

Written Warning

If the situation warrants a written warning in response to a security incident as a result of non-compliance, some organizations will provide a written warning, according to four or 33% of remote study participants. Rhett elaborated in their organization,

> If the command really takes it seriously or takes it medium serious then, in the code, in the Military or the [military branch]. It's called a bad page 7, and it goes in your record. For someone like me as an officer, a bad page 7 can affect promotion.

Fines and Lawsuits

If non-compliance to ISPs results in data breaches or compromise of laws, fines and lawsuits may be a result. Four remote study participants mentioned fines or lawsuits that may result from ISP non-compliance. Rufus commented on potential "penalties," as a possible issue. Rachel indicated that being "fined for having been a part of a data breach as a consulting company are astronomical." From a military perspective, Rhett communicated that military folks must deal with both the regular public courts and the UCMJ (The Uniform Code of Military Justice), they add "They will serve literally 2 different prison terms. They will serve their public

prison term and as soon as they get out the military will grab them and make them serve their military prison term."

Additional Coaching/Training

Three or 25% of remote study participants noted additional coaching/training as a result of non-compliance to ISP in their organization and experience. Rupert said their organization seeks to "educate and improve as opposed to, to punish… and turn a situation to something that's a learning opportunity." Rex's organization has employees review training in the event of non-compliance.

No Consequences

Non-compliance to ISPs may result in no consequences, an adjacent code to the ISP organizational stance of nice to have. Three or 25% of remote participants noted no consequences as a result of ISP non-compliance. Reid confirmed, "I've been doing like security since 2009, and I've never heard of anybody facing any consequences for and not abiding by it." Ray agreed and said, "I don't think anyone is actually looking over your shoulder."

Removal of Access

Sometimes non-compliance to ISPs results in removal of access to organizational systems, according to two remote study participants. Rhett confirmed if "you lapse in your in your mandated training, then you will lose your access." Remington shared, "I've worked in companies where people decide to watch YouTube all day every day. And all of a sudden, you know, their Internet privileges are revoked."

Loss of Reputation

As a result of non-compliance to ISPs, one remote participant, Rex, explained "when you lose that trust [from the customers], and then it's hard to re- regain that goodwill with the

customers, once you lose it."

Check Clarity of Policy

None of the remote participants mentioned checking clarity of a policy.

Types of ISPs

A total of 15 policies were mentioned by study participants during the interviews as shown in Table 15. Many study participants did not know the names of policies and instead provided examples of the policy as they understood it. The researcher grouped together examples and like-policies; for example, logging into a computer with a username and password and two factor authentication (2FA) or multi-factor authentication (MFA) was grouped into the authentication/authorization policy group. Types of ISPs were a part of the lived experiences of study participants, contributing to answering the research questions RQ1 and RQ2 of the experiences of in-person and remote study participants with ISP compliance. Types of ISPs may contribute to as factors that influence in-person and remote study participants with ISP compliance, in RQ3 and RQ4, as many participants could not name many polices that they had to comply to, so lack of awareness or knowledge of ISPs may contribute as a factor of compliance.

Table 15

Types of ISPs Mentioned by Remote Study Participants

ISPs	Remote	% Remote
Training	12	100%
Authentication	9	75%
Mobile Device	8	67%
Vulnerability Management	8	67%
Data Security	7	58%
Acceptable Use	5	42%
Access Control	5	42%
Network	4	33%
Personnel Security	4	33%
Change Management	2	17%
Contracts	1	8%
Incident Response	1	8%
Logging, Monitoring, and Alerting	1	8%
Disaster Recovery	0	0%
Information Security Program	0	0%

Note. One ISP was counted per study participant, for each category, even if the participant mentioned the policy multiple times in their interview. Percentage of remote participants was calculated with 12 remote study participants.

Training

Most participants reported annual training requirements from their organization, though

one participant in a security organization said the training was bi-weekly. Methods of training included classes, videos, gamification, and quizzes. Some of the participants said that security training was included in the onboarding with their organizations. Training policies topped the ISP policies that remote study participants commented on; 100% of remote study participants noted training as an ISP in their interview, which is the highest ranked ISP for remote participants. Rhys explained with a phishing example,

> Phishing is when someone clicks on a link in an email. And that link takes them to something with malicious intent instead of to where they thought they were going. And so, we educate through security awareness the general populace of an organization on phishing what it is and how to look at the URL and [how to] determine if it is what they think they is. But everybody has links that they click on a regular basis. And so, you have to know how to handle that well, most organizations as part of security awareness, train on phishing, and try and teach them. The secondary step there is to validate, you know are people doing it. And so, there are security companies that will help you by creating mock phishing exercises. Those mock phishing exercises allow an organization to determine. Do people click on stuff? They shouldn't and so that is trust but validate. And that's a key concept in information security and information security policies. Once you find somebody clicks on it, then, more mature organizations will enhance the training. So yeah, you got trained. You did click on something still, so make the person aware immediately. Hey, this was a phishing attempt. It was not an actual phishing thing. This is what you should have done, etc.

Authentication

A frequently mentioned policy, nine or 75% of remote study participants mentioned

authentication in their interviews. A few participants mentioned session limits or timeouts with authentication. The overwhelming majority of the participants cited passwords and MFA as their example, which included using a vendor application or phone to obtain a code. Rhett mentioned using a Common Access Card (CAC) "there's no access to anything without a CAC card. There is no passwords anymore. if you lose your CAC card, you have to call IT, and they might give you a temporary user and password to log in that way." Remington mentioned that in their organization if you "sit idle for too long, it logs you out." Rachel described their organization's authentication is "passwordless. So, everything is facial recognition. Fingerprints." Ray expressed annoyance with changing passwords in their previous organization:

> Back when I was working in the office, they required me to change my Windows login every month, I wrote it down and stuck it to my monitor. Every time, just like nope. You're making me do this. This password policy is dumb. I'm going to do exactly what the policy encourages, and I wrote it down on a sticky note and stuck in my monitor. Anyone who want to log in my computer absolutely could.

Mobile Device

Examples of mobile devices, such as workstations, laptops, tablets, or mobile phones, policies were noted by eight or 67% of remote study participants. Policy examples included use of USB or thumb drives, how or what is possible to download, restrictions of administrator access, network restrictions, and hardening on a mobile device. Rachel stated, "You can't download software that's going to put our company at risk of having some type of data breach." Rhett contributed, "some [military branch] members are allowed to use a USB Drive, but it has to be an encrypted hard drive, and it's been approved by the [military branch] in advance."

Vulnerability Management

Eight or 67% of remote study participants mentioned vulnerability management examples in their interviews, with stopping or reacting to phishing attempts at the top of the examples. Tools and methods that participants mentioned that assist with vulnerability management include endpoint protection, antivirus, software management tools, or patches.

Data Security

Seven or 58% of study participants cited examples of data security in the interviews, including encryption, handling, and classification. Notably, methods of data security varied from participants, which included encryption of data in transit, via email, mobile devices and on servers, as well as data masking, access, classification, scrubbing identifiable information, and data loss prevention tools. Rex said, “any kind of banking, information, credit, or information, any of that cannot be sent electronically.” Rachel contributed that their organization takes data security seriously and “masks even our own employees.”

Acceptable Use

This study defined acceptable use as what employees can and cannot do on organization time or with organization equipment. Five or 42% of study participants mentioned acceptable use or examples of acceptable use policies, including use of social media, representing the organization, behavior, and unauthorized use of unapproved software. Rachel said, “At all times, each employee represents the company, and we cannot divulge any information that’s related to our clients.”

Access Control

This study defined access control as both access management and access control for organizational systems. Five or 42% of remote study participants commented on access control

in their organizations or provided examples given in the interview for access control include Active Directory groups, the organization's network or virtual private network (VPN), user access versus elevated or administrator access, email, applications, folders or drive access, and local access to servers. Rhett elaborated, "Only certain people have the ability to upload and download to their own OneDrive account on DOD 365 from home" and that the organization was "controlling who has access and what has access and controlling how the files can leave."

Network

Network polices were mentioned by four or 33% of remote study participants. The comments about the network include physical access restrictions to the network, remote access, VPN, network encryption, and firewalls blocking access to external assets. Roman commented that they can't take their work laptop on trips because "I won't be able to access social media sites, because corporate is blocking access." Rhett provided an example,

> Every workstation is assigned to a particular Ethernet port, and it can only connect that one port. If you move it to a different one, it'll automatically lock up. It'll lock that line up and that laptop up immediately. And it obviously, if I take my laptop and plug it in, it'll have no Internet access. And to the point that if that happens enough, they'll actually shut down the Internet of that floor until they resolve that issue, if they detect a non [military branch] workstation attached to the to the network.

Personnel Security

Examples grouped in the personnel security policies were clean desk, clean screen, screen protector, locking laptops and devices, locking paper with sensitive information, shredding paper with sensitive information, and badge access. Four or 33% of remote study participants reported personnel security examples in their interviews. Rex said:

> At home you're supposed to do it [too]. Just the windows key L, lock your computer, and definitely in office. Those were huge things that when I have worked in office before, and that was part of my team all the time. [When] you got up and walked away, you had to lock that computer.

Change Management

Change management examples were provided by two remote study participants who work in an information technology development capacity. Rhett described the change management promotion process from development, test, and production environments, “I do stuff in three levels. One is I develop in my local box. And then, whatever code I upload goes straight to a testing environment and then into the actual production server.” Roman mentioned change management as an example when describing their organization’s approval process and one-time password required for production changes.

Contracts

Only one remote study participant referred to contracts policies. Rachel spoke about their legal agreements and contracts with their organization’s customers, including the agreed upon hosting or exchange of data, “We need to be able to test all the software and things that we're building. So that's normally agreed to with the client through our legal process.”

Incident Response

This study defines incident response as what the organizational policy is if there is an incident to investigate, stop or report on. Incidents may include anything from malicious malware infecting the organization’s system or accidents that involve unauthorized release of identifiable data. One remote participant, Rex, detailed the process of self-reporting when accidents were discovered with unintentional data release.

Logging, Monitoring, and Alerting

One remote study participant mentioned logging, monitoring, and alerting in their interview. Raven mentioned that actions on their organizational system made by users were logged and correlated within a service used by the organization.

Disaster Recovery

None of the remote participants cited disaster recovery as an example.

Information Security Program

None of the remote participants mentioned an information security program specifically.

Summary of Remote Lived Experiences with ISP Compliance

The themes of ISP intention, organization ISP stance, result of non-compliance to ISP, and types of ISPs were used to answer RQ2: What are remote employee experiences with ISP compliance. Showing familiarly with ISPs, many remote study participants dove deep into ISP intentions in their organizations, including communicating management intent, meeting various regulations, and protecting customers, data, and the organization and system. Half of the remote participants said their organization's ISP stance was mandatory. Further, remote study participants noted security incidents, termination, severity dependency, and verbal discussions as results of non-compliance with ISPs. All remote study participants mentioned training as an ISP, followed by the next three most popular ISPs: authentication, mobile device, and vulnerability management. Many remote study participants emphasized processes of ISP compliance, along with in-depth knowledge of implementation of ISPs.

Out of the 12 remote study participants, only one did not have an information technology or security or compliance job function. The results from the remote study participants was thus skewed towards technical knowledge of ISPs, including implementing ISPs or in some cases,

technically working around ISPs. The one non-technical remote participant, Rex who was a Claim Team Manager, was very aware of ISPs and some of the technical implementation of ISPs, possibly due to the senior level experience that they had, their manager position, and their interest in security of the organization.

RQ3: What factors influence in-person employees to comply with ISP compliance?

In-person participants discussed factors that influenced them to comply with ISPs. Top factors that were cited by in-person study participants included: availability, proper training, clarity and being hectic/busy. Further, in-person study participants contributed suggestions that might increase ISP compliance in organizations.

Factors with ISP Compliance

In-person study participants stated examples that influenced their decisions around ISPs. These in-person participants contributed their narratives about their lived experiences, in their current and past organizations, regarding decisions and actions influencing ISP compliance. Table 16 shows the 15 codes, and the breakdown of the amount and percentages in-person participant mentions and examples. Availability of ISPs were most noted by in-person study participants as a factor influencing if they would follow an ISP. The theme of factors that influence in-person ISP compliance directly applied to RQ3: What factors influence in-person employees to comply with ISP compliance?

Table 16

In-Person Factors That Influence Following ISP

Factors	In-Person	% In-Person
Availability	8	100%
Proper training	7	88%
Clarity	6	75%
Efficiency	6	75%
Hectic/busy	6	75%
Integrity	5	63%
Automated	4	50%
Enforcement	3	38%
Cost	2	25%
Leadership	2	25%
Compliance	1	13%
Intentional	1	13%
Organizational culture	1	13%
Social Media	0	0%

Note. One factor was counted per study participant, for each category, even if the participant mentioned the factor multiple times in their interview. Percentage in-person was calculated with eight in-person study participants.

Availability

All in-person participants mentioned ISP availability as a factor that influences their or their peers' ISP compliance. Ivan said, "the fact that an ISP exists is obviously helpful," though

acknowledged sometimes a “policy just wasn’t written.” Irvin commented that “all of our employees have access to our ISP documents,” but added, “I doubt [the employees] have read the actual text of the policies.” Some participants noted that they had full access and availability to their organization’s documented ISPs, though Ike noted, “looking at the whole library, searching the internet for policies, I haven't found that it was super easy to navigate so there are some challenges there” in finding ISPs. Other study participants noted that ISP access is restricted to those with access in layers of need-to-know basis or that they didn’t know where the ISPs were located in their organization. Isaac said, “certain layers of the ISP that are totally hidden,” and Ivan agreed, “our entire ISP is not something we disclose, and it should not be disclosed to every associate.” Ilya said, “I don’t know where to go” to find ISPs in their organization and added:

> They [the organization] had us sign a consent form, basically agreeing to a bunch of terms of what we can and cannot do on our laptops. And how they're able to track that information and see at any point in time, access our computers to see what we've been doing. So, I thought it [ISP documents] was going to be in there, [but] the only thing that they listed with no pornography, which is very obvious. But they didn't talk anything about gambling or [other] video sites or anything like that. It was just one thing that they listed. So, I'm surprised.

Proper Training

Training is mentioned by most study participants as an ISP, however, if the training is applicable, understood by the audience, covers the right material, or is helpful is another subject. Proper training where employees understand the why behind the training and how to handle different scenarios is cited by 88% of in-person participants, as a factor in ISP compliance. To

support proper security training, Ivan commented that you need, “to understand a policy in order to truly buy into the policy.” Isadora reported that in their organization, “Training is really not equitable across the board. You know some people are being taught and some aren't depending on the employee type.”

Clarity

75% of in-person study participants mentioned clarity of ISPs as a factor in ISP compliance. If employees do not understand ISPs and they were not clear, study participants generally found that it was difficult to comply with these types of ISPs. Ira said, “a little bit difficult to kind of track down the right person quickly” to ask questions about ISPs or their availability. Ivan suggested, “if there is a scenario that is gray and somebody truly doesn't understand the aspect of the policy, that should be brought to the IT Security Group, or whoever is in charge of owning that policy.” Organizations may need to customize and target the audience of ISPs to ensure that all levels of the organization may understand them and comply to them. In Irvin’s organization, they explained that the ISPs “had not been customized to our specific circumstances,” making it more difficult to comply because the ISPs were not customized to the organization.

Efficiency

Six or 75% of in-person participants remarked on the efficiency of ISPs as a factor in ISP compliance. A few study participants commented that if the ISP were inconvenient, in the way or they felt put out, that they may work around an ISP to make their life easier. Ira said, “It usually comes down to time. If it’s going to cost me time to follow a particular policy… I focus more on trying to meet the goal of the project or try to get the task done.” Ivan agreed and offered,

There are very few aspects of an ISP that makes your day to day job easier... There’s a

> human nature element that may make people not want to follow it… but I know the policy is in place for a reason and that you're going to have to do it either way.

Irvin contributed, "If an ISP is extremely inefficient and forces people to really go out of their way to follow it, most employees probably were not going to follow it, given the opportunity to skirt it without repercussions."

Hectic/Busy

Six or 75% of in-person study participants noted that being busy at work made them less likely to comply to ISPs. Project timelines, urgency in completing tasks, or production fixes were reasons that participants may opt to work around ISPs. For timelines, Irvin said, "If you are overloaded, you're going to focus on the things that are most important and to a lot of people the ISP is not the most important." Ike provided real-world examples of how easy it is to get caught up:

> In those, times where you're more distracted, more exhausted, it'd be easier to [say], "Oh, shoot! Let me check this really quick while I'm thinking about it. I'm online. Let me do this." [But] you might be breaking the rules… [When] your guard could be down, you would allow yourself to do something that was if you were, 8'clock in the morning or 10'clock in the morning you wouldn't… If you're on vacation, you'd be more willing to [say] "Hey, I'm gonna pull over here to McDonald's and jump on this Wi-fi because I really need to look at this stuff, this budget report or something and approve it." And you can accidentally get hacked. Or if somebody sent you email, and it just so happens the coincidence where you have phishing email… and click on it and then [realize] this is not what I meant to click… So definitely, if you're under the gun or if you're away or you're

> just trying to do something really quick, it could lead to steps that you would never make [otherwise].

Ira described a work scenario that pushed them to work around ISPs:

> We had an FTP that wasn't working… so in order to troubleshoot, I had to go into our test environment and find [the password], since we refresh production to test, and the record was there. Then, I had to track down a developer who was able to decrypt the password for me. We can do that [find the password] on test probably frowned upon. But I needed to get into that FTP. To get to, to get things back up and running, and that was my only way to do it [at the time it was needed].

Integrity

Personal integrity or doing the right thing was mentioned by five or 63% of in-person study participants, as a reason to comply to ISPs. Ivan said, “you know what they say about integrity, integrity is best when nobody’s looking. Do the right thing.” Ike described themselves as a “rule follower” who tries to “stick to the policy.”

Automated

Automated ISPs are technically enforced by the organization (e.g., remote employees were not allowed onto the organization’s network unless the employee logs in to the VPN) or require minimal interaction with the employee to comply with the ISP. Four or 50% of in-person study participants referenced automated tooling or methods in their interviews as a factor that positively influences or increases ISP compliance. None of the study participants indicated that automated ISPs would lower or make ISP compliance neutral. Ira described that in their organization, technically automated ISPs force compliance, “if you don't follow the ISP, you can't log on, or the system just won't work.” Ivan commented, “If a company has a lot of money

and can automate things, then certainly tasks to comply with an ISP might be easier, more easily accomplished." In Irvin's organization, they said:

> we made them [ISPs] technical automated so that people didn't have a choice. Then they just couldn't do anything about it. So, all of our endpoint protection stuff like using smart screen and Defender and blocking websites and stuff like users don't have any say in that, and so there's no choice to them. They just have to do whatever it is. And so that's nice in some ways.

Enforcement

Enforcement of ISPs is defined differently than consequences or results of ISP non-compliance, even though it is similar. In this study, ISP enforcement is the following up from an organizational level to enforce and check-in on employees and their ISP compliance. Only three in-person participants mentioned this type of enforcement as an influence in ISP compliance in their organizations. Ira contributed, "There's no real ISP police running around making sure that you're not letting anyone follow you into the door. You're not leaving anything on your desk like that." Irvin's organization does enforce ISPs to an extent, but they commented that to increase manual ISP compliance would include "staffing up more and increasing manual oversight" which may be "past the point of diminishing returns."

Cost

Only two in-person participants remarked on the cost in dollars of compliance to ISPs as a factor. Isaac stated about ISPs, "There's always the inherent cost of it as well."

Leadership

Leadership attitude towards ISPs and their own compliance with ISPs were reasons study participants may decide to comply with ISPs. Two in-person participants noted that leadership is

a factor in ISP compliance, while a couple of participants also commented that leadership was the largest offenders of ISP non-compliance. Irvin suggested, “the biggest mess ups almost invariably come from people higher up in the company” and “lot of the managers and the directors like they're in those positions because they've been in the industry for a long time, and they remember the good old days. We didn't have to worry about information security, or compliance.”

Ilya agreed, “my manager would be more like, ‘Hey, up to your discretion [ISP compliance]. It's just based off of how well you're doing.’ Like as in how many sales you've sold.”

Compliance

Only one in-person participant cited compliance as a factor in ISP compliance in their organization, though many participants cited meeting regulations as an intention of ISPs in their organization. Irvin provided their thoughts around how some employees were motivated to comply with compliance, “salespeople have seen how much it helps us having these compliance certifications when we go to try to acquire new customers.”

Intentional

Regarding intentionally breaking ISPs, only Ivan, an in-person study participant, commented, “I've never seen somebody do it [break ISPs] truly of having the nefarious reasons.”

Organizational Culture

An organizational culture of whether actions and behaviors were acceptable to the organization and its stakeholders is a factor in ISP compliance according to one in-person study participant. Ira advised, “if everybody is not on board for how we're gonna fix this, then it does me no good to go rogue, because they won't follow along.”

Social Media

None of the in-person study participants mentioned social media as a factor in influencing ISP compliance.

Increase ISP Compliance

In Table 17, study participants suggested ways to increase ISP compliance. Six factors that influence whether individuals comply to ISPs also overlap as suggestions from study participants as things that may increase ISP compliance in their organization. The theme of increasing ISP compliance aligns with additional factors that influence ISP or RQ3: What factors influence in-person (RQ3) employees to comply with ISP compliance?

Table 17

Suggestions to Increase ISP Compliance from In-Person Participants

Suggestions	In-Person	% In-Person
Availability*	8	100%
Proper training*	7	88%
Automated*	4	50%
Enforcement*	3	38%
Security updates	3	38%
Leadership*	2	25%
Rewards system	2	25%
Get help	1	13%
Most important upfront	1	13%
Organizational culture*	1	13%
Reinforcement	1	13%
Viable solutions	1	13%

Note. One suggestion was counted per study participant, for each category, even if the participant mentioned the suggestion multiple times in their interview. Percentage in-person was calculated with eight in-person study participants.

*Six codes overlapped between the themes of factors that influence following ISP and increasing ISP compliance. The six codes were ISP automation, availability, enforcement, leadership, organizational culture, and proper training.

Security Updates

Three in-person participants recommended sharing more knowledge about security

updates as ways to increase ISP compliance. Isaac said that ISP information should be more "disseminated."

Rewards System

Two in person study participants suggested rewards systems, games, or competitions that may increase ISP compliance. Ira said:

> The reality is that when there's a team lunch on the line or department a happy hour or something, people will hopefully make a point to comply more than if it's a no reward. I mean [it] shouldn't have to be that way but that seems to be the best way to get people to do things. You bribe them.

Similarly, Irvin suggested increasing ISP compliance with a "reward focused thing of like, if you report a phishing email, everybody who reports to phishing email correctly in a month gets enter to win a $50 Amazon gift card or something like that."

Get Help

One in-person study participant, Ilya, suggested that increasing ISP compliance would be possible "if we have somebody who is actually more hands on and more on site would help out a little bit."

Most Important Upfront

One in-person study participant emphasized the need to filter the most important ISP ideas to the top, to increase ISP compliance. Ike said, "there's a lot of information out there" and questioned, "what is the stuff that I really focus on?" Ike proposed "maybe like a quick setup, these three or four or five, modules would be something that you need to do to get up and going and understand."

Reinforcement

Iver, an in-person participant, suggested that ISP compliance may increase if there was more "following up on compliance to ensure the personnel are utilizing the tools they have in front of them and that the policy that they are given is being held to the standard."

Viable Solutions

Only one in-person study participant suggested ensuring that ISPs were written so that the solutions were viable. Isaac suggested "using several sources together and seeing where they overlap. That's where an ISP should target rather than going to one source and saying, That's the only option."

Summary of Factors that Influence In-Person Employees to Comply with ISP

Factors that influence in-person employees to comply with ISPs include the themes factors with ISP compliance and ways to increase ISP compliance. First, in-person participants emphasized, with all in-person participants commenting, that ISPs must be available for employees for ISP compliance. Some in-person participants did not know where to find ISPs in their organization or noted that their organization hid parts of the ISPs. Proper training was suggested so that employees understand the why behind the ISPs and the ISPs themselves followed next in popularity of mentions by in-person study participants. ISP clarity, efficiency, and being hectic/busy were the next most frequently cited factors in ISP compliance for in-person participants. Suggestions to increase ISP compliance overlaps with the factors that influence ISP compliance, including the top four ways to increase ISP compliance availability, proper training, automation, and enforcement. Providing more knowledge sharing via security updates and setting up rewards systems for compliance were additional suggestions from in-person participants that may increase ISP compliance.

RQ4: What factors influence remote employees to comply with ISP compliance?

Factors that influenced remote study participants to comply with ISP compliance included factors that made the ease of IPS compliance easier such as availability, efficiency, and automation as influences. Following up, remote study participants also created ideas and factors that might increase ISP compliance in the future, should organizations implement the suggestions.

Factors with ISP Compliance

Remote participants contributed to narratives about their lived experiences, in their current and past organizations, regarding decisions and actions influencing ISP compliance. Table 18 shows the 15 codes, and the breakdown of the amount and percentages of remote participant mentions and examples. Availability and efficiency were the most noted factors for remote participants for ISP compliance. The theme of factors that influence ISP compliance directly apply to RQ4: What factors influence remote (RQ4) employees to comply with ISP compliance?

Table 18

Remote Factors That Influence Following ISP

Factors	Remote	% Remote
Availability	10	83%
Efficiency	10	83%
Clarity	9	75%
Automated	7	58%
Enforcement	7	58%
Hectic/busy	7	58%
Proper training	7	58%
Leadership	4	33%
Organizational culture	4	33%
Integrity	3	25%
Intentional	3	25%
Compliance	2	17%
Social Media	2	17%
Cost	1	8%

Note. One factor was counted per study participant, for each category, even if the participant mentioned the factor multiple times in their interview. Percentage of remote participants was calculated with 12 remote study participants.

Availability

Ten or 83% of remote participants claimed ISP availability as a factor that influences their or their peers' ISP compliance. Some participants commented that the availability and

searchability of ISPs in their organizations contributed to increased ISP compliance, while if an ISP was not available or easily found, that would likely decrease ISP compliance. Ray said, “if you can’t find it [an ISP], it’s easy to ask the relevant folks,” while Roman commented, “I have not looked up [ISP] policies in the last 5 years. I’m probably more detached.” Regarding ISP availability, Rhys commented, “if I'm not aware of the ISP, I'm less likely to follow it” and “employees generally want to do the right thing for the company, and therefore you just have to make it easy for them to find the information security policies.”

Rupert’s organization allowed employees to “go and look that up specifics to a topic, raising compliance rates. So, having the documents themselves searchable, as opposed to reading hundreds and hundreds of pages of policy documents, certainly helps as well.” Other remote study participants noted that ISP access is restricted to those with access in layers of need-to-know basis or that they didn’t know where the ISPs were located in their organization. Raven’s organization also does not share the entire library of policies with all employees; Raven said, “if it’s an organization wide ISP, then everybody has access to it. If it’s only for the governance risk and compliance team, then it’s accessible to a much smaller number of people.” Ray admitted, “I have no idea” where ISPs are located in their organization and there is an “overwhelming amount of documentation” to sort through.

Efficiency

10 remote participants or 83% of remote participants remarked on the efficiency of ISPs as a factor in ISP compliance. A few study participants commented that if the ISP were inconvenient, that they may work around an ISP to make their life easier. Reid explained, “Security is often seen as like a barrier to protect productivity. It's usually just not wanting to be slowed down and wanting things to be more convenient.”

On the topic of being too strict with ISPs, Ray said, “most security choices you make are just that trade off of like convenience versus security” and added regarding their organization training and inefficient implementation of ISPs said, “Watch out for 2 factor fatigue. And it's literally like, this is the fifth time I've had to do 2 factors today I got to do 7 more. Clearly, whoever [is] setting out these videos is not aware of the policies in the company or is not watching the videos and doesn't give a shit.” Raven explained, “the easier the ISP is to follow, the more likely it is to be followed” and:

> If the ISP requires you to take a bunch of very specific steps to do a thing, or it makes your job harder in a way that isn't easily modified, or in a way that the security team isn't willing to budge on, then people were going to find ways around it.

Rhett remarked:

> There's tons of people in the [military branch] that constantly complain about how strict the military is for simple things. They overdo it. I get it. It's the military... You need certain level of credentials. I get that, but there is a certain level of overkill.

For example, Rhett continued:

> I would say half the military, and I say this for all branches. They don't have high security clearance, like the documentation they're dealing with is not super sensitive. No one's going to get hurt, so just make that stuff more accessible. Make their life a little easier. In general, the military ISPs to the point of overkill makes the job slower.

Remington provided their experience, “To do our job as quickly as we were required to without having like thumb drives on us as engineers. So maybe that's a good one where it's like, maybe you're technically not supposed to have it.”

Clarity

Nine or 75% of remote study participants mentioned clarity of ISPs as a factor in ISP compliance. If employees do not understand ISPs and they were not clear, study participants generally found that it was difficult to comply with these types of ISPs. For example, Reid said, “if it were clear to employees that they were outright forbidden from using their own device [in an ISP], they probably wouldn't.” Clarity of ISPs is somewhat related to availability of ISPs, depending on the scenario. Rachel said, “if they could make it easier for us to understand the differences between the regulations and the countries, for the different information security policies that would be helpful.” According to Rhys:

> If they have questions about those policies, it's very important that they know to ask their manager. That is what a management structure is there for, is to enable people to solve problems they're not aware of how to solve or that they have questions about.

Raven said that if ISPs aren’t clear then employees will say:

> “The policy wasn't clear, and so I didn't know what to do in this situation,” and so they made an executive decision, and it was kind of the wrong one, just because they didn't know sometimes, necessarily, that it was the wrong one. Sometimes they did know, and they just kind of fall back on like, “Well, it wasn't super clear.”

Roman provided an example of when they sought clarity of an ISP and was provided with a good experience behind the why:

> There was a debate [about] whether a particular piece of data constituted confidential information. It was an 8 digit number. And I asked them [security team], “Why is this confidential information?” And they said, “because it identifies a business entity.” And I said, “but it's just an eight digit number. I can throw the dice and come up with an eight

> digit number. It carries no confidentiality in it." and the individual with whom I was discussing it with referred me to the information security policy which was new… so what I learned is that even though that number by itself is just an eight digit number… meaningless. [When] combined with other pieces of information it could be revealing… And that's what the information security policy was saying… We need to think of how it can be used and whether it can be used to reveal confidential information. If so, it becomes confidential information itself and that was a paradigm shift for me.

Organizations may need to customize and target the audience of ISPs to ensure that all levels of the organization may understand them and comply to them. Rupert commented,

> We do get into some reading through of the policies or standards with users. And sometimes we make changes based off the insights that they give us through their interpretation being different than ours. So, it helps us [security team] find gaps or areas where we can kind of tighten up that language to remove that uncertainty. In some cases, we need that [uncertainty], you can't necessarily bolt it down to be so specific that it excludes everything and anything. But in other cases, we can definitely tinker with the language a little bit to make it not confusing for the next person that comes along.

Automated

Seven or 58% of remote study participants referenced automated tooling or methods as factors that influence ISP compliance. Automated ISPs are technically enforced by the organization or require minimal interaction so that employees would not need to think readily about complying with ISP. As Rufus said, "I would put security policy into that bin of things that people don't get excited about and don't want to focus the brain power on and those are exactly the things that you should automate, because they are the things where mistakes get made."

Rupert recommended that organizations "automate the control or make it a hard control as opposed to a soft control." Rusty spoke about technically implemented automated ISPs where the organization does not allow employees to be "on your mobile device and access company data when you're connecting to a restaurant wi-fi." Reid added "if you're using automated tool tooling, there's less chance of human interaction manually, then you're more likely to have a more compliant process around how you deploy and develop software." Additionally, Rhys provided an example of a technically automated ISP intended to increase compliance:

> It's not a PCI violation for a consumer to send their credit card to the bank or merchant using an insecure technology. It's their choice to send a credit card over email, but if you as the customer service agent hit reply and you don't redact or remove that credit card number, then that is a violation of policy. And so, we just implemented technology for a client that pops up a box and says to the customer service agent, "Hey, looks like there could be a credit card number in this email. Are you sure you want to send it?"

Enforcement

Enforcement of ISPs is defined differently than consequences or results of ISP non-compliance, even though it is similar. In this study, ISP enforcement is the following up from an organizational level to enforce and check-in on employees and their ISP compliance. Seven remote participants mentioned this type of enforcement as an influence in ISP compliance in their organizations. Rufus agreed regarding ISP compliance and enforcement in their organization, "The current situation is so lenient that I'm not sure it's all that helpful." Raven claimed that enforcement depends on the manager, where some managers care, and some do not care to enforce ISPs. Rhett remarked, "You still have to monitor your people because your people are what's going to slip in ISP is going to be. *The people get that all these systems are*

only as good as people that follow them [ISPs] [emphasis added]."

Hectic/Busy

Seven or 58% of remote participants noted that being busy at work made them less likely to comply to ISPs. Project timelines, urgency in completing tasks, or production fixes were reasons that participants may opt to work around ISPs. Rusty expressed "it's very simple to get kind of caught up when things get kind of hectic for junior guys. They may just cave into it for someone like me [senior engineer]. I can't do it." Raven added that in their organization, "once they [employees] start getting busy, start to ignore ISPs, and then we have to have a conversation with them that consists of like you can't send data like that over email like you just can't."

Proper Training

Training is mentioned by most study participants as an ISP, however, if the training is applicable, understood by the audience, covers the right material, or is helpful is another subject. Proper training where employees understand the why behind the training and how to handle different scenarios is cited by 58% of remote participants, as a factor of ISP compliance. Reid noted, "I've had gigs in the past where management was essentially saying, like, look. just do the ISP training say, yes, a yes, and it'll be out of your hair" making the case for the support of proper security training, rather than just checking it off the list of things to do. Similarly, Rachel added, "*if you don't have the right people that understand the right policies like coming into review, I think that's where the mistakes happen* [emphasis added]."

Leadership

Leadership attitude towards ISPs was a reason study participants decided ISP compliance. Four remote study participants noted that leadership is a factor in ISP compliance, while a couple of participants also commented that leadership was the largest offenders of ISP

non-compliance. Raven explained:

> We have some leaders who are definitively, this is gonna sound bad, but definitively on our side, the side of the security team basically saying, like, you guys have to actually like, look at these and follow these. And it matters. We have some other leaders at the same level that are a lot less concerned with security and a lot more concerned with profits and sales, and the sort of money making side of the business, and to them ISPs are just kind of a hassle that gets in the way of what they want to do because they want to move quickly.

Rachel provided an example of leadership influence on ISP compliance:

> We really want 100% of our people to complete it [security training]. And very few of our leadership team had done it. I find it very difficult to go on a call for like for my boss to go on a call and talk to 10,000 people and say, “Hey, have you done your information security?” When she [leader/boss] hasn't done it herself. And so, I really need them [leader/boss] to take it seriously, and I know that they do take it seriously. They wouldn't be in the positions that they were, if they didn't. But I would like for them to be compliant with their training, so that as they're talking to other people about being compliant with their training and the different policies that we have in place, that they've done it, and they've lived it themselves. I just think it's a little two-faced if you haven't done it, but then you tell people to do it [security training].

Organizational Culture

An organizational culture of whether actions and behaviors were acceptable to the organization and its stakeholders is a factor in ISP compliance according to four remote participants. Raven explained, “Once a culture becomes a culture, it's very difficult to sway it

one way or the other, especially rapidly," but that their organization is "still working on getting other people to agree that they [ISPs] are useful or helpful." In an example of organizational culture influencing ISP compliance, Rhys said:

> At the corporate office, when the CEO walks in the door. Everybody knows who he is. The security guard manning the physical security desk knows who he is. However, if there's a policy that says you have to have your badge to get through [the doors] and if the standard practices say if you don't have a badge, then somebody has to verify you [prior to access]. And it can't be the security guard because he should be independent. Then, when security is taken seriously at a physical level culturally is, if the CEO is willing to wait for someone, for the security guard to check with somebody and validate who he is before he's allowed, through whatever security controls there are physically, if he were to forget his badge. That type of support from executives is what is required to help enforce the security of an organization culturally. If when he forgets his badge or she forgets his or her badge, they are allowed to just walk through unverified, then that is a culture that doesn't support security. It's those little choices that managers and leaders have to enforce around the policies in order to help.

Integrity

Personal integrity or doing the right thing was mentioned by only three or 25% of remote participants, as a reason to comply to ISPs. Roman said that they were 100% complaint with ISPs "partially driven by my strong respect for information security not just my personal security, and not just my company. Security." Rex followed up similarly with following ISPs is about, "personal integrity. You've got to hire the right people to make sure that they're conscientious and they're going to follow those procedures."

Intentional

Only three remote participants commented that they or employees in their organization may not comply to ISPs intentionally, if the policy was stupid or if employees felt angry or upset with the organization. Ray disclosed that “if the policy is stupid, I'm going to make it as stupid as possible” and that it was a fun “thought experiment to see how you could circumvent these like terrible policies that you really didn't think made sense.” Rhett cautioned that some employees might break ISPs to “expose this wrong by going public” or:

> They could literally just be angry at the organization. I've seen that before. Where people were just angry. They feel like they've been overworked or they're unappreciated or they don't agree with the mission or the ethos of the organization, and they want to retaliate. They want to hurt it.

Compliance

Only two or 17% of remote study participants cited compliance as a factor in ISP compliance in their organization, though participants cited meeting regulations as an intention of ISPs in their organization. Compliance with laws and regulations were the factors that influenced ISP compliance. As an example, Ray said:

> If we're talking HIPAA, I would say definitely don't do it just because there's a legal aspect there and that's a problem. But, if my company [not a healthcare company] said that [don’t use your personal device for work in an ISP], I would probably just still put it on my phone, because what's the difference between my phone, which is super secure.

Social Media

Two remote participants or 17% of the remote population mentioned social media as a draw to employees in their organization deciding to comply to ISP. Both of these participants

mentioned the frenzied need of some individuals to share on social media as a factor or oversight in posting, regardless of if the social media posts broke organizational ISPs. Rhett contributed:

> I feel like as humanity where we have gone from social interaction. And we're used to social praise. Like, you do a good thing, and you get recognized by your church or your whatever. We have slowly broken in little, small chunks due to society as it's grown, or whatever we are calling it. And now people are seeking praise and gratification and approval online, or they're going for both. And so, I feel like a lot of ISPs get broken, especially when it comes to security like destinations and stuff like that, strictly because people are living these two lives of like Internet and in person. And they're not understanding the repercussions of a simple 100 character phrase.

Rachel explained their experience with social media influencing ISP compliance as well:

> So, I don't know that ignorance is kind of a strong word, but I think in the moment people don't think about it, especially from a social media perspective. They [employees] don't think that what they're doing is wrong. They're just trying to celebrate, “Hey! I just got staffed on a new project. I'm doing this really exciting thing.” They're just trying to celebrate with their friends, and they don't realize that they're potentially divulging information that shouldn't be public.

Cost

Only one remote participant remarked on the cost in dollars of compliance to ISPs as a factor. Rufus said about ISPs, “It’s not free. It certainly costs. And you know it’s just a trade” of compliance versus the people resources.

Remington pondered:

> Maybe [employees] potentially abuse the ISPs because they're bored. They're burned out. Whatever it is, sort of an ebb and flow… another reason why people might feel necessary to abuse an ISP is for personal gain. I know people have been like messaged on LinkedIn, "Hey, you get me some data, or you get me something, and I'll send you a bitcoin or something," and someone who might be feeling like they're not being paid what they're worth, or whatever it is, or who's having a hard time might be really into that. So maybe that comes down to that interpersonal sort of manager to employee level, just making sure that your people leaders are actually, plugged in with how your people are feeling. I feel like *people who are feeling seen, heard, compensated, [and] not burned out, they're less likely to make mistakes* [emphasis added].

Increase ISP Compliance

In Table 19, suggestions to increase ISP compliance from the remote study participants included ensuring employees get ISP help, security updates, reinforcement or reminders of the ISPs and best practices, and implementing a rewards system for compliance. Six factors that influence whether individuals comply to ISPs also overlap as suggestions from study participants as things that may increase ISP compliance in their organization. The theme of increasing ISP compliance aligns with additional factors that influence ISP and RQ4: What factors influence remote employees to comply with ISP compliance?

Table 19

Suggestions to Increase ISP Compliance from Remote Participants

Suggestions	Remote	% Remote
Availability*	10	83%
Automated*	7	58%
Enforcement*	7	58%
Proper training*	7	58%
Security updates	5	42%
Leadership*	4	33%
Organizational culture*	4	33%
Rewards system	3	25%
Reinforcement	2	17%
Get help	1	8%
Most important upfront	0	0%
Viable solutions	0	0%

Note. One suggestion was counted per study participant, for each category, even if the participant mentioned the suggestion multiple times in their interview. Percentage of remote participants was calculated with 12 remote study participants.

*Six codes overlapped between the themes of factors that influence following ISP and increasing ISP compliance. The six codes were ISP automation, availability, enforcement, leadership, organizational culture, and proper training.

Security Updates

Five remote participants recommended sharing more knowledge about security updates

as ways to increase ISP compliance. Rusty said that their organization hosts monthly conference calls to discuss new business and address questions; they said, “security doesn’t do that, and they should” to increase knowledge sharing. Rex suggested increasing the cadence of security reviews above the current quarterly cadence in their organization. Remington shared:

> We have weekly town hall group meetings where cybersecurity has their own little schtick that they'll share. They'll either share things like, “Hey, this is a common hack that we're seeing” or “Hey, this is a common infiltration that we're seeing” or “*Hey, here's some data about that humans are always the weakest link in your cyber security* [emphasis added] …” It’s an “open, two-way street when it comes to like the folks who are presenting versus like the rest of the group that's listening or participating within the meeting.

Rachel mused:

> One of the big issues that we have because we're so large is trying to communicate something to everyone, especially if you have like a change in policy or whatever. If you send an email, probably the majority of the people aren't going to see the email. So, we have different communication channels that we use. Try to get the information out. That's why some of the training is required.

Rupert agreed and added along the same lines of communication challenges:

> Some of that we've been trying to improve on, and we continue to improve on communication. So, when changes are made to the governance, it's tough, like in any organization. It's tough. But in a large organization trying to reach the right audience that needs to care about a particular change is sometimes difficult.

Rewards System

Three remote study participants suggested rewards systems, games, or competitions that may increase ISP compliance. Rachel's organization attempted to make compliance more fun with "gamification." Rupert provided an example at their organization, "we do keep track of phishing rates by some business units, and every now and then we'll have them [business units] ask us… to have a competition between our business units to see who has the lowest rates."

Reinforcement

Two remote study participants noted that reinforcement or reminders increase ISP compliance. Rusty commented, "we have a ton of guardrails in place, but I think that you need that constant reinforcement for people to follow them." Rufus said his managers could remind him about the ISPs, that if:

> They could be directly asking and communicating, making it a personal interest to me… Please do this, draw attention to it directly. Absolutely, I find that it [the reinforcement] is and I would guess most people are pretty responsive to that sort of thing.

Get Help

One remote study participant proposed ways to get help via mentoring to increase ISP compliance. According to Rusty, new inexperienced hires require senior engineer mentoring to get up to speed with ISP compliance and security best practices; while Rusty agreed that this was time well spent, the time it takes to do mentoring calls and video calls from a remote work experience does take away time from other tasks.

Most Important Upfront

None of the remote study participants commented on bringing the most important aspects of ISPs upfront to increase ISP compliance.

Viable Solutions

None of the remote participants mentioned viable solutions to increase ISP compliance.

Summary of Factors that Influence Remote Employees to Comply with ISP

Remote study participants emphasized that ISPs needed to be available and efficient for ISPs to be followed in their organization. Efficiency and similarly, automation, were factors that remote participants shared lived experiences about. Interestingly two remote participants cited social media influences as ISP compliance influences. Ways to increase ISP compliance overlapped with factors in ISP compliance, including the top four ways that remote participants suggested to increase ISP compliance: availability, automation, enforcement, and proper training.

There were a few notable comments from the remote participants. A couple remote participants that commented on social media as challenges to compliance brought up a shift in society and behavior that may be explored further, where employees may forget themselves and carelessly, but not maliciously, posted prohibited organization information on social media, breaking ISP. In addition, proper training was emphasized by remote participants to ensure that not only is training done to check compliance checkboxes, but that proper training should go one step further to ensure that employees understand the why of the policies, to reduce accidents and unintentional mistakes.

RQ5: What impact does a relationship between a manager and employee influence ISP compliance?

Organizational Relationships

The theme of organizational relationships directly applies to RQ5: What impact does a relationship between a manager and employee influence ISP compliance? All study participants typically reported good relationships with their managers and co-workers, even if they were not

best of friends. One participant was ambivalent towards leadership saying that they were not around or involved to have a relationship.

Co-Workers

Study participants overall were friendly or friends with co-workers. Ira suggested that there was a "small company vibe within our department." Ivan was more diplomatic and said, "I think you're influenced by everyone around you, good at or indifferent. You know you just have to choose what influences to follow" for ISP compliance. Remington said, "I work remote, but some of the people that I've worked with [in-person] over the years have become good friends," but in their current remote organization "it's that physical geographical distance that you can't really get over" to become good friends with co-workers.

Good Vibes

Reid said they feel "super connected" to their co-workers and manager because of constant communication through Slack or phone calls. Isaac spreads good vibes in the office to "make everyone's day better that meets me than what they started with." Rufus asserted:

> The positive outlook of an employee toward an organization and how they feel about the company's policies [goes] beyond security, just in a broad sense of social security policies. Compensation is everything. Whether you've got a friction sort of oriented [organization] or a punishment based kind of compliance to rules in general, I think that that's gonna lead to a very poor compliance of all policies.

Manager/Leadership

Rusty commented that the support from their management and leadership team drives them to work harder and double and triple check that everything is done correctly. Rusty added, "I'm enthusiastic every single day when I come in, and it's because the guys that I work with, and

my manager and my manager before him." They also said, "I value them [referring to their manager and leadership] and want them to look good." Remington said their manager is, "someone who's genuinely just feels like they're trying to eliminate obstacles and enable the resources and freedoms to get the tasks done, you need to which I really appreciate."

Relationships Don't Influence Decisions

Two study participants, one in-person and one remote, said that their relationships at work did not influence their decisions with ISP compliance. Ray stated that they were not influenced by their manager, "Definitely, no. No, I'm stubborn." Isadora also commented about their leadership, "I don't feel like there's a lot of influence there" around ISP compliance.

Summary of Organizational Relationships

Organizational relationships play a role in influencing ISP compliance, in the majority of the study participants' lived experiences. There were a couple exceptions where two study participants claimed that organizational relationships did not influence their decisions. Also, importantly, all study participants reported neutral or positive current organizational relationships, surprising the researcher.

Remote Versus In-Person

Table 20 displays the reported lived experiences from study participants on their in-person or remote experiences. The remote versus in-person theme ended up addressing a bit of all five research questions, including lived experiences with ISP compliance, factors that influence ISP compliance and relationships. Many participants seemed to indicate that relationships were better in person, though did not outweigh the convenience of not commuting for remote work.

Table 20

Remote Versus In-Person Codes

Codes	In-Person	% In-Person	Remote	% Remote
Better in-person	7	88%	9	75%
Better remote	1	13%	9	75%
Challenges in-person	2	25%	2	17%
Challenges remote	5	63%	6	50%
Same	4	50%	6	50%

Note. One code was counted per study participant, for each category, even if the participant mentioned the code multiple times in their interview. Percentage in-person was calculated with eight in-person study participants, while percentage of remote was calculated with 12 remote study participants.

Better In-Person

Ike said regarding remote work, “you don't have the daily interactions with not necessarily just people on your team, but everybody that’s in the office. So, you don't have that [working remotely].” Ray commented along the same lines, “you're slightly closer with people like when you worked in person. And just because you had a whole bunch of hours to fill.” Iver reminisced:

> From a pre-COVID viewpoint where we had more individuals engaged in-person, [the organization] was a tighter knit group. I think it was a closer team and so I think that the implementation of telework, as it's been handled, does provide that separation of [in-person or remote] activities that is lost when we had the strength of the team as a bonded group. It doesn't seem to be as strong as what it was.

Rex forewarned:

> When you're remote, my team, they're spread all across the country so that it's hard to find somebody when you have the situation come up like an ISA question and security question. You used to be able to just look over the cubicle and talk to them. Now you can't do that. You gotta find somebody [remotely].

Reid claimed, "if you're in an office, you're in a corporate network, … and if you're around a bunch of other people that are sitting behind you, you're probably less apt to be on Twitter or Reddit all day and screw around" and "you're going to act a little bit more professionally when you're in the office," including "I think in an office you're probably more apt to be more compliant."

Rhett argued, "now it's easier for people to work from home, and if anything is being more efficient for a lot of industries," but explained:

> I think it's great for people that can work 100% remotely and almost never meet their people in person. But I feel like things are always better if you actually met the person [in-person], and you have a relationship. It's my own personal thing, like I'm a fan of going to the office which I know is blaze, [since] people mostly are favoring working from home. And I get it. It's convenient, but I'm [social] in nature and socializing is like part of our culture. I understand both, but I do think, even working remotely, the remote [work] is more successful when they have personal relationships within those teams. Because now you want to succeed for that person more because there's a personal connection with them. That's how I see it. Versus if this system, random person that, as your boss, or as your supervisor, as your co-worker, but you never actually met them. There's no there's a motivation to really succeed for them because you don't really know

them.

Ray signaled:

> I think if I was younger, so like fresh out of college, I think it would have been weird to go into the workplace and not have those people immediately around you… having smart dudes. And when you hang out lunch you just bullshit, you learn a lot through those conversations and stuff. So, I think some of that in person is definitely it's a good opportunity to learn.

Better Remote

Ira said about remote work, "the pandemic kind of proved that you can still do that [work remote] and still be effective and still get things done." Rachel proposed, "if you're remote you probably have higher [ISP] compliance because I think companies make it more difficult for you to access the data that you need to do your job [remotely]." Reid said that remotely, sometimes you can get to know people better though digital communication because "you could share a little bit more openly when you're a little bit more anonymous."

Challenges In-Person

Challenges to in-person work surround the convenience of the commute. Rex said, "I enjoy working remote. I live outside of Atlanta. Traffic is horrendous. It's just awful. My commute was an hour plus to work and an hour plus home." Ray added, "I don't know if the like trade off [of working in-person] is worth it, because I like skipping an hour or two drive every day."

Challenges Remote

Communication is a challenge remotely, as is ensuring ISP compliance physically. Irvin claimed, "remote employees care less about the ISP than in office employees do." Rhys stated

that managers need:

> Different techniques are required for managing remotely, than in person. You have to create time for personal communication. You don't have a water cooler or a coffee pot to have a conversation over, but there needs to be trust between managers and employees, and that's two ways of trust and respect… It's important to acknowledge that those who have more experience with remote work tend to have solved some of these problems and those that are less experienced with remote work, struggle more with these problems.

Same

Rex maintained, "there's really not much of a difference [between in-person and remote], with the expectations. The expectation is the same" for ISP compliance. Rupert added, "COVID taught us how to deal with each other remotely and deal with the Webex. You know whether it's a blend of folks in a conference room and a couple of people that are remote, or whatever that mix may be, our workforce has become a lot more location diverse… So, I don't think that being seated at an office or not, has probably a ton of bearing on [ISP] compliance." Isaac response to the difference between remote and in-person:

> I mean, maybe 20 years ago I would have said differently. But nowadays we're so used to. We have cameras. We have gig networks, you don't see really a loss of the human interaction, plus most facilities have a policy where you shouldn't be touching your coworkers. So, you know, at that point. It's kind of like that. Human interaction is very easily implemented with our modern technology.

Summary of In-Person Versus Remote Experiences

Study participants appeared to appreciate the convenience of working remotely to avoid commutes or for other personal reasons, though cited examples of better relationship building

and knowledge transfer or learning in-person. The study participants also commented on challenges with remote work in finding resources and making time to connect with colleagues. Overall, technology has enabled remote work to facilitate a closer to in-person work experience that the majority of study participants seemed to favor, despite acknowledged remote work challenges.

Summary

The experiences of in-person and remote study participants were detailed in response to RQ1, RQ2, RQ3, and RQ4. RQ1 addressed in-person lived experiences with ISP, while RQ2 covered remote lived experiences with ISP. RQ3 described factors that contributed to ISP compliance for in-person employees, and RQ4 explored remote factors of ISP compliance. Study participants, both in-person and remote, acknowledged that building relationships in person and learning in an office setting with experienced colleagues around is a benefit. In response to RQ5, most participants agreed that their co-workers, managers, and leadership influenced them at least a little bit in decisions they made in their jobs. Some expressed that avoiding “looking like a fool” influenced their decisions about being careful about some decisions, while others praised their managers for creating an environment where they felt valued which, in turn, aided participants in wanted to ensure their decisions and performance made their managers look good.

CHAPTER 5

DISCUSSION

This study documented lived experiences of 20 study participants around in-person and remote employees and ISP compliance. The eleven, nine males and two females, participants were Generation X or aged 59-77, followed by eight (seven males and one female) Millennials, aged 28-46. The remaining participant was a male Baby Boomer in the 59-77 age range. Altogether, the average age of study participants was 44 and 85% of participants were male. Participants were located within the U.S., with 50% residing in Colorado, three in Florida, two in California, and one each in Alabama, Georgia, Indiana, North Carolina, and South Carolina. 85% of participants were engineers or technologists in some form, based off of their job titles and three participants had non-technical roles. Participants worked in many different industries, such as financial services, healthcare, security, supply chain, advertising, automotive, cloud services, contract and compliance, education, electronics, engineering, government, and management technology consulting. Participants self-rated their ISP familiarity on a scale of 1 to 5, with an average response of 3.85 out of 5, with 5 representing extremely familiar. This discussion summarizes the results to answer the research questions, relates the findings back to the literature, notes limitations to the research, provides practical implications, and makes recommendations for further research.

Summary of Findings by Research Question

This study's purpose was to investigate lived experiences to describe the phenomenon around ISP compliance. The literature review covered previous research to employee behavior and compliance, pandemic remote work, and social bonds; these topics were the basis of this study's research questions, along with the theoretical framework using TPB and SBT to explain behavior and compliance to ISPs aligned with the strength of organizational relationships. Contributions to the knowledge base around ISP compliance centers around the in-person and remote lived experiences within organizations, including awareness and knowledge that the participants said were a part of their organization and suggestions to increase ISP compliance. With many employees working remotely before and after the COVID-19 pandemic and employees working a traditional in-person job, organizations may be able to better understand the phenomena of these experiences as related to ISP compliance. ISP compliance is a tool that may assist organizations with protecting its systems and data, keeping organizations from the risk of fines, lawsuits, and loss of reputation.

The themes of intention of ISPs in organizations, the organization's ISP stance, results of non-compliance, and types of ISPs described the lived experiences of ISP compliance, or RQ1 and RQ2 for in-person and remote experiences. Factors that influence in-person and remote employees to comply with ISPs and ways to increase ISP compliance answer parts of research questions RQ3, RQ4, for in-person and remote employees, respectively. RQ3 and RQ4 addressed factors that influence ISP compliance as a part of the theoretical framework with TPB. Finally, organizational relationships were a factor of ISP compliance and the lived experience of ISPs in organization and specifically answers RQ5 which used SBT as the theoretical framework.

Combined these research questions sought to discover the lived experiences of in-person and remote employees, including the factors and relationships that may influence ISP compliance.

Relevance of Findings to the Literature

RQ1: What are in-person employee experiences with ISP compliance?

The in-person experiences of study participants varied within the themes of ISP intention, organization ISP stance, result of non-compliance to ISP, and types of ISPs. Some of the in-person participants were intimately involved with ISPs, although about half of the in-person participants were only aware of a couple ISPs. Bauer & Bernroider (2017) suggested that personal norms and attitudes towards security and compliance, along with social norms are factors in compliance. The results of this study align with this concept, as each study participant had a different experience, story, and attitude towards ISP compliance, where each participant brought unique perspectives to the study. Many participants shared their experiences and perspectives, some of which included how colleagues, managers, leadership, or the overall organization's culture influenced them.

The intention of ISPs within organizations is generally understood to protect the organization, its customers, and its data. Though, only one in-person study participant mentioned regulations as part of ISP intention, and this discrepancy does not seem to be explained by the industry of in-person participants as they were distributed over regulated, such as finance and healthcare, and non-regulated. The organization's stance towards ISPs may align with the ISP intentions, where only half of the in-person study participants said that following ISPs were mandatory. Most in-person participants reported that there were pros and cons to both in-person and remote work situations. Many in-person participants cited relationship building as stronger

or doing their job easier on-site, though one in-person participant also said that they felt that they could replicate the same job effectiveness remotely as well.

In-person study participants explained what could happen in the event of ISP non-compliance. In-person participants cited responses to non-compliance potentially being additional coaching/training, checking clarity of policy, fines or lawsuits, no consequences, security incidents, termination, written warnings, or verbal discussions. Two in-person participants also noted that the response to non-compliance was severity dependent. Interestingly, a few study participants provided examples of security incidents or breaches in their organization which explored scenarios of ISP non-compliance. In-person participants mentioned authentication policies the most frequently of ISPs, giving examples that include MFA and passwords for different applications. Data security was the next most popular ISP amongst in-person participants where participants mentioned encryption, data handling and classification as examples.

RQ2: What are remote employee experiences with ISP compliance?

Overall, the remote lived experiences were more technical due to their job functions and involved with creation, automation, implementation, or execution of ISPs. The remote experiences of study participants also varied within the themes of ISP intention, organization ISP stance, result of non-compliance to ISP, and types of ISPs. Previously, this study's literature review found a gap in literature for remote employees, specifically, around ISP compliance. This study's lived experiences begins to contribute knowledge about remote employees' experiences with ISP compliance.

For ISP intention, one remote study participant added that ISPs communicate management intent. Most of the remote participants said that ISPs existed to protect customers,

data, or the organization or system. Eight remote participants mentioned meeting regulations as the intent of ISPs. Like the in-person experiences, only half of remote study participants said that their organization's stance towards ISPs was mandatory.

Remote participants expressed that remote work was convenient, avoiding a long commute, and that technology enabled them to work remotely with good and frequent electronic communication with colleagues. Most remote participants said enjoying the convenience to their work/life balance as the key trade-off to the relationships that were a bit stronger when built in person. Remote participants also mentioned that in the past, when working in an office, they tended to not goof off as much and acted more professionally, while working remotely at home, pajamas and checking personal email were often happening. Being remote was noted by study participants as possibly being more effective and efficient, as technology enabled this, and the pandemic showed that it was possible. A few study participants also noted that when working remotely, finding folks to ask questions to was more challenging as well as remote managing of people resources required additional time and skill. Some participants claimed that working in-person or remote didn't make much of a difference because of the advancements in technology and the learnings from doing it during the COVID-19 pandemic.

Remote participants commented that potential results of non-compliance to ISP were severity dependent and included additional coaching/training, fines or lawsuits, loss of reputation, no consequences, removal of access, security incidents, termination, or verbal discussions. Interestingly, a few study participants provided examples of security incidents or breaches in their organization which explored scenarios of ISP non-compliance. All remote participants said that training was an ISP that they were aware of, followed closely with 75% of remote participants mentioning examples of authentication. Mobile device, such as what

employees may plug into devices, and vulnerability management, such as antivirus, were the next most popular ISPs named.

RQ3: What factors influence in-person employees to comply with ISP compliance?

Suggestions to increasing ISP compliance also overlap with factors that influence ISP compliance, while a few factors and suggestions also overlap with principles of human resources development (HRD). The six factors were also suggestions to increase ISP compliance: ISP automation, availability, enforcement, leadership, organizational culture, and proper training. Knowing where to get help to comply with ISPs, having a quick guide or introduction to the most important parts of ISPs in their organization, reinforcement or reminders to do things certain ways to comply, implementing a rewards system for compliance, providing frequent knowledge transfers of security updates, and ensuring ISPs were written or implemented as viable solutions to the employee base are the high level areas that in-person study participants mentioned that may help organizations increase ISP compliance. HRD emphasizes learning, performance, and change where mechanisms to achieve these goals include leadership, organizational culture, training, and rewards (Gilley & Maycunich, 2000). Comparing this study's ISP compliance factors with previous literature from R. Ali et al. (2021), there are many similarities. R. Ali et al. (2021) found ISP compliance factors national culture, intrinsic/extrinsic motivations, protection motivation behaviors, culture/aware behaviors, management behaviors, social behaviors, and actual compliance behaviors and noncompliant factors of security-related stress/neutralization, value conflicts, and deterrence.

In-person study participants stated that automation makes it easier to force compliance but is costly and not possible with some organizational budgets and staff. Availability of ISPs was key for in-person participants to comply with ISPs, although participants acknowledged that

even if ISPs were available, most people do not read them. In-person participants said that in order to comply with ISPs, they must be mostly clear and targeted to the audience. ISPs have an inherent cost to create and implement, per an in-person participant. Similar to previous research studies such as those from Hannah & Robertson (2015), Herath & Rao (2009), and Hofeditz et al. (2017), the study participants revealed that ISP compliance and possible workarounds depend on if the ISP enables work or is disruptive. In-person participants complained that ISPs should minimize the effort required for employees to follow ISPs to maximize compliance. This study's result for in-person experience agrees with the previous literature review finding where He & Zhang (2019) shared that minimizing security fatigue was important for compliance.

The results reported that some organizations were strict about enforcing ISPs, though many were not. As described by Jalali et al. (2020), employee noncompliant behavior increases with a higher workload. Similarly, the study finding included when times were more hectic or busy in an organization, this impacted the in-person participants' decisions on whether to follow ISPs. Being hectic or busy in an organization may tie to the efficiency of following ISPs manually and the concept of automating ISPs so that employees do not have to worry about them.

The majority of in-person participants, 63%, noted integrity or doing the right thing, as a reason that they would comply with ISPs. Leadership is a factor of ISP compliance that is linked with enforcement from managers to employee, as well as with relationships in RQ5. Leadership was described by some in-person study participants as being part of the ISP compliance problem. Kim & Han (2019) found that employees were more complaint when they understood the benefits and costs of noncompliance. The in-person study participants noted proper training with

ISPs and security as necessary to ensure employees understand why the ISPs were the way they were and how they contributed to security of the organization systems and data.

RQ4: What factors influence remote employees to comply with ISP compliance?

Remote study participants cited availability, efficiency, and clarity as the top factors that influence following ISP, followed by automation, enforcement, being hectic/busy, and proper training. The other factors mentioned by remote participants were less popular. Specifically for remote employees, this study found that a literature gap exists for remote employees and ISP compliance. This study's results and data begin a conversation to further extend how remote employees may increase ISP compliance.

Remote participants noted that automation removed the burden of ISP compliance on the employee and allowed for increase in compliance. Some remote study participants said that ISPs were not available to all levels of employees, though others said ISPs were searchable in their organization. Clarity was also a topic of conversation in the experiences of remote study participants where resources to ask questions to was brought up, as well as comments about increasing clarity in the ISPs. Compliance with laws and regulations were mentioned by a couple of remote participants as reasons for ISP compliance.

Many remote participants wished for ISPs to be more efficient, tying into the concept of automation of ISPs and the slipping of ISP compliance when times are hectic/busy. A few remote participants commented that personal integrity pushed them to follow ISPs, though on the other side, remote participants also detailed why some employees might intentionally not comply to ISP such as exposing wrong doings, being angry at the organization, or being bored.

Boss et al. (2009) claimed in a previous study that employees are more compliant when they believe compliance is mandatory and that management is watching. The remote participants

in this study agreed. If organizations monitored or enforced ISPs, ISP compliance should increase, per remote study participants. Also, leadership and organizational culture are factors to ISP compliance, according to remote participants, where leaders or the organizational culture set the tone for if ISPs are mandatory or can be skipped. Organizational culture was found by Alshaikh (2020) and D'Arcy & Greene (2014) to drive employee behavior and compliance in organizations.

Remote participants also commented that although they are subject to security training, proper training may be needed to ensure true understanding of ISPs and the reason for requiring ISP compliance. Proper training was repeated from many study participants as the missing factor with ISP compliance; most organizations had some sort of security training, though not all non-security employees understood the need and why behind the ISPs. Some previous research showed that proper training may include employee collaboration in developing ISPs (Nicolas-Rocca et al., 2014), real-world examples and feedback (Bauer et al., 2017), relating security back to employee personal lives (He & Zhang, 2019), and making security training situational (Jaeger & Eckhardt, 2021). Social media was also cited by two remote participants as reasons employees might be influenced to not comply with ISPs, including being careless and excited to display their work lives on social media. Increasing ISP compliance, per remote participants, includes ensuring availability, automation, enforcement, and proper training, security updates, leadership, organizational culture, rewards systems, reinforcement, and allowing employees to get help.

RQ5: What impact does a relationship between a manager and employee influence ISP compliance?

Most study participants agree that their managers influence their decisions including ISP compliance; this study's results from study participants agreed with past studies such as Hu et al.

(2012) who found that management participation influences employees directly or indirectly via the TPB. Only two study participants said that relationships in the organization do not influence their decisions. Adjacently, SBT claims that behavior is influenced by individual relationships and that negative or delinquent behavior is due to weak social bonds (Mears & Stafford, 2022). Since study participants reported overall very positive relationships with co-workers and managers, the direct results of delinquency resulting in noncompliance via SBT were not seen in this study, as the researcher expected, though the results of this study agree that the strong social bonds appear to influence employees with compliance. Some participants mentioned that the strength of their relationship with their manager increased their due diligence in decision-making and ISP compliance. This study results agreed with the findings from Toscano et al. (2022) that strong trust and quality of an employee and manager relationship predicts higher job performance. None of the study participants reported adverse or negative working relationships with anyone in their organization.

As most study participants reported, stronger relationships with co-workers and managers were developed in person, in past and current experiences. Some adjustments to management may explicitly need to be made for remote work. One remote participant mentioned that remote management of human resources requires more planning to set aside time to communicate and create relationships with remote resources.

Limitations of Research

Limitations of this research include that the results were not generalizable, used a convenience sample for the study population, and relied on the researcher's network's network for recruitment. The hesitation that the researcher felt from some study participants to discuss the sensitivity of violating ISPs, meaning they could have potentially admitted to breaking laws and

regulations and/or organizational policies and procedures, brings some skepticism to some of the participant's responses regarding their behavior in the research study. The convenience sample of the researcher's network's network was mainly comprised of male knowledge workers, who had a lot of experience and leaned heavily in the information technology field.

First Time Qualitative Interviewer

The researcher's inexperience with qualitative interviews likely impacted the richness of the data collected from the interviews. The researcher realized as the data collection process continued that questions could be phrased or asked differently to help encourage participants to share their lived experiences. Realizing a deficiency during the data collection process, the researcher adjusted the semi-structured interview guide and requested examples of specific experiences and using grounded prompts assisted in collecting rich data from participants, with about 30% of the interviews complete. Updating an interview guide iteratively through a study is common in qualitative research, as are using grounded prompts such as, "Tell me more about that" or "Please give me an example" (Hill et al., 2005; Hill et al., 1997). However, the interviewer still had a few participants that were not particularly vocal which led to shorter answers, even with follow up questions, and overall, less data collected from participants that were less talkative.

The researcher added questions to the demographic data section in the semi-structured interview guide midway through the interviews, thus not all participants were asked the new demographic questions. The new questions requested information about the length of time working remotely and the size of their organization. These additional questions were not reported in this study as the data was not collected for all participants. The additional questions were used as a basis for suggestions for future research in the conclusion.

Recruitment Challenges

The researcher misgauged the recruitment challenges for this study which impacted the proposed timeline to recruit and conduct interviews for this study. The researcher neglected to understand that many potential participants were turned off by the phrase "information security policy" that was included in the title of the study, where some knew ISPs via examples or as simply organizational policies. Potential participants told the researcher that they would not speak about their organization's security citing confidentiality, even after the research attempted to clear up the interview's subject matter focusing on participants' own lived experiences, not the actual security policies implemented by organizations. In addition, potential participants also declined to participate in an interview as they felt that they were not experts with ISP, even after the researcher attempted to explain that the participant did not need to be an expert, simply had to be aware of at least one security policy. Female recruits were frequently cited lack of expertise with ISP as a reason for not participating in the study.

Recruiting participants for the research study was ineffective with group messaging such as email or text message blasts or social media posts in LinkedIn and Facebook. No participants responded to any of the mass messages. All participants recruited were recruited individually using the researcher's professional and friend network or through snowball recruiting of a study participant. Many potential recruits in the researcher's network worked in information technology, as engineers or in other technical positions, and the "information" industry has taken to remote work in larger numbers, approximately 68% of workers telework or work remotely (BLS, 2022), making the recruiting of in-person employees more of a challenge for this study. In addition, many potential recruits for the study worked hybrid work schedules and thus were not mostly in-person or remote employees. Therefore, they did not qualify per the participation

criteria. Some potential recruits also declined to participate based on the one-hour interview request for their time, claiming that the time request was too great.

Senior Level and Mostly Male Participants

The convenience sample of the study participants ended up skewing towards senior level employees and males. As the study participants were pulled from the researcher's professional and friend network, the median age of the participants was approximately 44 which aligns with the researcher's network of experienced professionals and experience as a senior level practitioner. The youngest working generation, Gen Z, is not represented by the study participants. As a result of the strength of experience of participants, the data reflects the participants' level of expertise more so than entry level employees. In addition, the title of the study including "information security policy" and the leaning of the study participants in the technology industry also contributed to the heavy majority of male study participants. Females recruited for the study were very hesitant to do the study citing lack of knowledge, even after study content clarification; only 24% of females in the United Kingdom (U.K.) (WISE, 2023) and 27% of females in the U.S. (Census Bureau, 2021) make up the workforce in science, technology, engineering, and mathematics (STEM).

ISP Subject Sensitivity

Despite the promise of de-identification of their identity and their organization's identity, many participants appeared nervous to discuss their decisions and behaviors that did not comply to their organization's ISP. Only a few study participants admitted to knowingly skirting ISPs, however, some of the study participants provided examples of others in their organization that did not always follow ISPs. As a first-time qualitative research interviewer, the researcher attempted to ask questions for most of the interviews and not press the study participants on if

they themselves knowingly broke ISPs. Towards the latter half of the interviews, the researcher started to provide examples of the researcher violating ISPs, out of annoyance or laziness, which seemed to provide confidence to a few study participants to then recall instances where they also violated similar ISPs. The researcher feels that some participants held back on revealing their lived experiences with ISPs out of fear of revealing that they were not always complaint to ISPs.

Theoretical Implications

The theoretical framework for this study was based off the TPB and SBT. The TPB has been used in many behavioral studies, including with ISP compliance and employee behavior. SBT has also been used in many behavioral studies, with a few studies also typing SBT to ISP compliance. This study collected data of lived experiences of study participants and found many factors that may be plugged into the TPB that shape norms, culture, and behavior. For SBT, this study did not find any study participants that reported adverse, negative, or poor relationships within their organization. The results from this study for organizational relationships reported neutral to positive relationships towards ISP compliance and the poor social bonds of delinquent or noncompliant behavior with SBT was unexplored.

Practical Implications

As a practitioner and researcher, the researcher sought practical implications from the data collected to improve ISP compliance in real organizational practice. Based on the literature review and the results from this study, the following practical implications include influences from the theoretical framework of both TPB and SBT, with some corresponding with HRD key concepts for improving performance and encouraging employee behavior to be complaint. Encouraging complaint behavior should be tackled from multiple fronts, including focusing on proper training to ensure employees understand why they are being asked to comply with ISPs,

ensuring leadership and the organizational culture set tones for compliance, followed by non-punitive coaching when things go awry, and rewards for behaving compliantly.

Information Security Awareness and Training

Information security awareness and trainings intend to ensure knowledge is shared, though not all trainings provide enough information. Study participants, Ivan and Rachel, said that training should be improved from obligatory trainings into thoughtful and more challenging training so that employees can understand the why behind the ISPs. Nicolas-Rocca et al. (2014) suggested employee participation and collaborations with ISPs, while Bauer et al. (2017) and Jaeger & Eckhardt (2021) recommended real-world examples to increase ISP compliance.

Carrot or the Stick

Organizations may consider rewards programs to entice employees to learn about and comply with ISPs as well as punitive measures. Study participants, Ira and Irvin, suggested rewards and bribes to increase ISP compliance which aligns with the findings from Liang et al. (2013) that high promotion focus employees were motivated by rewards. On the other hand, perceived sanction celerity or perception of enforcement of ISP compliance strongly influenced employee compliance (Raddatz et al., 2020). Study participants, Ivan, Irvin, Rupert, and Rex, commented that security incidents should be handled on a case by case basis, depending on the severity, where many cases will simply result in remedial training or coaching.

Leadership and Organizational Culture

Organizational culture that is supported by leadership and values ISP compliance, influences employee ISP compliance (Hu et al., 2012). Study participant, Rhys, pointed out that leadership and organizational culture are linked and when leadership models ISP compliance,

then the organizational culture will follow. D'Arcy & Greene (2014) similarly found that organizational cultures that support security result in better ISP compliance from employees.

Despite the list of practical implications listed, the researcher acknowledges that ISP compliance is expensive. Organizations must consider software, hardware, consulting expertise, people resources, time, and money to pay for the time and people are required to implement these practical implications. Organizations may have budget and staffing challenges, though the risk of having a small or relaxed security program in organizations, large and small, is great in the age of information technology.

Future Research

As the popularity of remote work or hybrid work grows, future research in the ISP compliance space may be considered to add additional knowledge to the body of current research. Expanding on this study, a future research project may seek to quantify differences between in-person, remote, and hybrid populations to differentiate possible training or management tools that each population may respond to increase ISP compliance. One study participant suggested that the longer an individual works remotely, the better at working remotely the individual becomes at performing ISP compliance and remote work. Here, a future study may compare populations with different lengths of remote work and their effectiveness with remote work and ISP compliance levels and attitudes. In addition, a couple of the study participants mentioned “ma and pa” type organizations having less emphasis on ISP compliance; thus, a future area of research may be investigating the correlation between level of ISP compliance and size of organization or perhaps publicly versus privately owned organizations.

Most organizations have a variety of age ranges working in their workforce. This study was limited in that there were no participants from the youngest current working generation, Gen

Z. A generational research question may be considered surrounding the latest workforce that joined the workforce during or after COVID-19 and may never work in the office. Research the impact to Gen Z may be followed and studied, as well as compared, for remote, hybrid, and in-person populations to gather data on their experiences. Questions surrounding Gen Z and the value of in-person communication and mentorship may be answered over time.

Recently, social media has become more popular, and a couple of study participants commented on employee social media posts potentially violating ISPs. Social media and ISP compliance may be a prudent research study to discover how decisions are made when employees post on social media. Another study participant commented on older folks being less technology savvy and being more prone to have ISP violations, such as clicking on phishing links. A future investigation may include a phishing test or experiment with the different generations in the workforce or a study to catalog the number and types of security incidents aligned with their generation. Finally, a few participants commented that rewards for compliance may increase compliance and a potential future study may include what rewards were most effective and measuring any increase in the results of employee ISP compliance. This study gathered much data from study participants and their lived experiences, though many more questions may be asked from the data gathered and many more studies conducted to generalize findings and contribute back to the growing ISP compliance knowledge base.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. *Human Behavior and Emerging Technologies, 2*(4), 314-324. https://doi.org/10.1002/hbe2.195

Ali, R. F., Dominic, P. D. D., & Ali, K. (2020). Organizational governance, social bonds and information security policy compliance: A perspective towards oil and gas employees. *Sustainability (Basel, Switzerland), 12*(20), 8576. https://doi.org/10.3390/su12208576

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., Sohail, A., & Drosatos, G. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences (2076-3417), 11*(8), 3383. https://doi.org/10.3390/app11083383

Ali, S. E. A., Lai, F.-W., Hassan, R., & Shad, M. K. (2021). The long-run impact of information security breach announcements on investors' confidence: The context of efficient market hypothesis. *Sustainability (Basel, Switzerland), 13*(3), 1066. https://doi.org/10.3390/su13031066

Alqahtani, F. H. (2017). Developing an information security policy: A case study approach. *Procedia Computer Science, 124*, 691-697. https://doi.org/10.1016/j.procs.2017.12.206

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Anderson, V. (2017). Criteria for evaluating qualitative research. *Human Resource Development Quarterly, 28*(2), 125-133. https://doi.org/10.1002/hrdq.21282

Angraini, Alias, R. A., & Okfalisa. (2019). Information security policy compliance: Systematic literature review. *Procedia Computer Science, 161*, 1216-1224. https://doi.org/10.1016/j.procs.2019.11.235

Auerbach, C. F., & Silverstein, L. B. (2003). *Qualitative data: An introduction to coding and analysis*. New York University Press. https://doi.org/10.18574/nyu/9780814707807

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy & Security, 8*(2), 33–56. https://doi.org/10.1080/15536548.2012.10845654

Balozian, P., Leidner, D., & Warkentin, M. (2019). Managers' and employees' differing responses to security approaches. *The Journal of Computer Information Systems, 59*(3), 197-210. https://doi.org/10.1080/08874417.2017.1318687

Bauer, S., & Bernroider, E. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *The Data Base for Advances in Information Systems, 48*(3), 44-68. https://doi.org/10.1145/3130515.3130519

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security, 68*, 145-159. https://doi.org/10.1016/j.cose.2017.04.009

Bhattacharya, K. (2017). *Fundamentals of qualitative research: A practical guide*. New York, NY: Routledge/Taylor & Francis Group.

Birks, M., Chapman, Y., & Francis, K. (2008). Memoing in qualitative research: Probing data and processes. *Journal of Research in Nursing, 13*(1), 68-75. https://doi.org/10.1177/1744987107081254

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164. https://doi.org/10.1057/ejis.2009.8

Carmi, G., & Bouhnik, D. (2020). The effect of rational based beliefs and awareness on employee compliance with information security procedures: A case study of a financial corporation in Israel. *Interdisciplinary Journal of Information, Knowledge & Management, 15*, 109–125. https://doi.org/10.28945/4596

The Center for Generational Kinetics (CGK). (2023). Generational breakdown: Info about all of the generations. CGK. https://genhq.com/the-generations-hub/generational-faqs/

Checkpoint. (2022). The 2022 workforce security report. Checkpoint. https://www.checkpoint.com/downloads/resources/2022-workforce-security-report.pdf?mkt_tok=NzUwLURRSC01MjgAAAGKi5ai-qMVsbEus2lwvui9Xjhk3a0ac6RO0bcgYfnEYv1MFXZZjKnWqe8KBgv8x8ouW3aNFJ7RZCoTcWxQmE2c7o6pwTDjluJ7hM8ghtX38eS6N0fy

Chen, L., Zhen, J., Dong, K., & Xie, Z. (2020). Effects of sanction on the mentality of information security policy compliance. *Revista Argentina de Clínica Psicológica, 29*(1), 39–49.

Cheng, E. W. L. (2019). Choosing between the theory of planned behavior (TPB) and the technology acceptance model (TAM). *Educational Technology Research and Development, 67*(1), 21-37. https://doi.org/10.1007/s11423-018-9598-6

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security, 39*, 447-459. https://doi.org/10.1016/j.cose.2013.09.009

Choi, S. J., Johnson, M. E., & Lee, J. (2020). An event study of data breaches and hospital IT spending. *Health Policy and Technology, 9*(3), 372-378. https://doi.org/10.1016/j.hlpt.2020.04.008

Chudzicka-Czupała, A., Żywiołek-Szeja, M., Paliga, M., Grabowski, D., & Krauze, N. (2023). Remote and on-site work stress severity during the COVID-19 pandemic: Comparison and selected conditions. *International Journal of Occupational Medicine and Environmental Health, 36*(1), 96-111. https://doi.org/10.13075/ijomeh.1896.02001

Cilesiz, S. (2011). A phenomenological approach to experiences with technology: Current state, promise, and future directions for research. *Educational Technology Research and Development, 59*(4), 487-510. https://doi.org/10.1007/s11423-010-9173-2

Clark, O., Zickar, M., & Jex, S. (2014). Role definition as a moderator of the relationship between safety climate and organizational citizenship behavior among hospital nurses. *Journal of Business & Psychology, 29*(1), 101–110. https://doi.org/10.1007/s10869-013-9302-0

Clarke, S. (2013). Safety leadership: A meta-analytic review of transformational and transactional leadership styles as antecedents of safety behaviours. *Journal of Occupational & Organizational Psychology, 86*(1), 22–49. https://doi.org/10.1111/j.2044-8325.2012.02064.x

Connolly, L. Y., Lang, M., & Wall, D. S. (2019). Information security behavior: A cross-cultural comparison of Irish and US employees. *Information Systems Management, 36*(4), 306–322. https://doi.org/10.1080/10580530.2019.1651113

Creswell, J. W., & Creswell, J. D. (2020). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE.

Curran, K. (2020). Cyber security and the remote workforce. *Computer Fraud & Security, 2020*(6), 11-12. https://doi.org/10.1016/S1361-3723(20)30063-4

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

De Simone, D. M. (2019). Data breaches are not just information technology worries. *Pediatric Nursing, 45*(2), 59-62.

Deterding, N. M., & Waters, M. C. (2021). Flexible coding of in-depth interviews: A twenty-first-century approach. *Sociological Methods & Research, 50*(2), 708-739. https://doi.org/10.1177/0049124118799377

Dolezel, D., & McLeod, A. (2019). Managing security risk: Modeling the root causes of data breaches. *The Health Care Manager, 38*(4), 322-330. https://doi.org/10.1097/HCM.0000000000000282

Dong, K., Ali, R. F., Dominic, P. D. D., & Ali, S. E. A. (2021). The effect of organizational information security climate on information security policy compliance: The mediating effect of social bonding towards healthcare nurses. *Sustainability (Basel, Switzerland), 13*(5), 2800. https://doi.org/10.3390/su13052800

Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity (Oxford),* 2(1), 3-14. https://doi.org/10.1093/cybsec/tyw003

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis: A focus on trustworthiness. *SAGE Open, 4*(1), 2158244014522633. https://doi.org/10.1177/2158244014522633

EU General Data Protection Regulation (GDPR). (2023). *Complete guide to GCPR compliance*. GDPR. https://gdpr.eu/

Eurofound. (2020). Living, working and COVID-19. *Publications Office of the European Union, Luxembourg*.

Federal Bureau of Investigation (FBI). (2022). *Internet crime report*. FBI. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Feng, G., Zhu, J., Wang, N., & Liang, H. (2019). How paternalistic leadership influences IT security policy compliance: The mediating role of the social bond. *Journal of the Association for Information Systems, 20*(11), 1650–1691. https://doi.org/10.17705/1jais.00581

Fielding, J. (2020). Securing the remote workforce. *Computer Fraud & Security, 2020*(10), 20-20. https://doi.org/10.1016/S1361-3723(20)30110-X

Galanti, T., Guidetti, G., Mazzei, E., Zappalà, S., & Toscano, F. (2021). Work from home during the COVID-19 outbreak: The impact on employees' remote work productivity, engagement and stress. *Journal of Occupational and Environmental Medicine, 63*(7), e426-e432. https://doi.org/10.1097/JOM.0000000000002236

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review, 13*(1), 61-83. https://doi.org/10.1111/j.1540-6296.2010.01178.x

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. *British Dental Journal, 204*(6), 291. https://doi.org/10.1038/bdj.2008.192

Gilley, J.W., & Maycunich, A. (2000). *Organizational learning performance and change: An introduction to strategic human resource development*. Cambridge, MA: Perseus Publishing.

Gross, M. (2017). *Planned behavior: The relationship between human thought and action* (1st ed.). Taylor and Francis.

Guhr, N., Lebek, B., & Breitner, M. H. (2019). The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. *Information Systems Journal, 29*(2): 340-362. https://doi.org/10.1111/isj.12202

Gunawan, J., Marzilli, C., & Aungsuroch, Y. (2022). Online ‘chatting’ interviews: An acceptable method for qualitative data collection. *Belitung Nursing Journal, 8*(4), 277-279. https://doi.org/10.33546/bnj.2252

Gwebu, K. L., Wang, J., & Hu, M. Y. (2020). Information security policy noncompliance: An integrative social influence model. *Information Systems Journal, 30*(2), 220–269. https://doi.org/10.1111/isj.12257

Hannah, D. R., & Robertson, K. (2015). Why and how do employees break and bend confidential information protection rules? *Journal of Management Studies, 52*(3), 381-413. https://doi.org/10.1111/joms.12120

Hassan, A. F., Karim, A. M., & Hameed, J. (2022). Hybrid model for remote work practice in the post pandemic era: Prospects and challenges. *International Journal of Academic Research in Business and Social Sciences, 12*(12). https://doi.org/10.6007/IJARBSS/v12-i12/15988

Hatashima, T., & Sakamoto, Y. (2017). Study on effect of company rules and regulations in telework involving personal devices. *IEICE Transactions on Information and Systems, E100.D*(10), 2458-2461. https://doi.org/10.1587/transinf.2016OFL0001

Hays, D. G., & Wood, C. (2011). Infusing qualitative traditions in counseling research designs. *Journal of Counseling and Development, 89*(3), 288-295. https://doi.org/10.1002/j.1556-6678.2011.tb00091.x

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce, 29*(4), 249-257. https://doi.org/10.1080/10919392.2019.1611528

Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social Science & Medicine (1982), 292*, 114523-114523. https://doi.org/10.1016/j.socscimed.2021.114523

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125. https://doi.org/10.1057/ejis.2009.6

Hill, C. E., Knox, S., Thompson, B. J., Williams, E. N., Hess, S. A., & Ladany, N. (2005). Consensual qualitative research: An update. *Journal of Counseling Psychology, 52*(2), 196-205. https://doi.org/10.1037/0022-0167.52.2.196

Hill, C. E., Thompson, B. J., & Williams, E. N. (1997). A guide to conducting consensual qualitative research. *The Counseling Psychologist, 25*(4), 517-572. https://doi.org/10.1177/0011000097254001

Hina, S., Panneer Selvam, D. D. D., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security, 87*, 101594. https://doi.org/10.1016/j.cose.2019.101594

Hirschi, T. (2017). *Causes of delinquency* (1st ed.). Routledge.

Hofeditz, M., Nienaber, A. M., Dysvik, A., & Schewe, G. (2017). "Want to" versus "have to": Intrinsic and extrinsic motivators as predictors of compliance behavior intention. *Human Resource Management, 56*(1), 25-49. https://doi.org/10.1002/hrm.21774

Hooper, V., & Blunt, C. (2020). Factors influencing the information security behaviour of IT employees. *Behaviour & Information Technology, 39*(8), 862-874. https://doi.org/10.1080/0144929X.2019.1623322

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4): 615-660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Husserl, E., & Moran, D. (2001). *Logical investigations* (Vol. 2). Routledge.

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior, 81*, 282-293. https://doi.org/10.1016/j.chb.2017.12.022

Hwang, I., Kim, S. & Rebman, C. (2022). Impact of regulatory focus on security technostress and organizational outcomes: The moderating effect of security technostress inhibitors. *Information Technology & People, 35*(7): 2043-2074. https://doi.org/10.1108/ITP-05-2019-0239

IBM. (2022). *X-force threat intelligence index 2022*. IBM. https://www.ibm.com/downloads/cas/ADLMYLAZ

IBM Security. (2022). *Cost of a data breach report 2022*. IBM. https://www.ibm.com/downloads/cas/3R8N1DZJ

Identity Theft Resource Center (ITRC). (2023, January). 2022 data breach report. Idthefcenter.org. https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf

International Organization for Standardization (ISO). (n.d.). *ISO/IEC 27001 and related standards: Information security management*. ISO. https://www.iso.org/isoiec-27001-information-security.html

Jaeger, L., & Eckhardt, A. (2021). Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal (Oxford, England), 31*(3), 429-472. https://doi.org/10.1111/isj.12317

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why employees (still) click on phishing links: Investigation in hospitals. *Journal of Medical Internet Research, 22*(1). https://doi.org/10.2196/16775

Kalaiprasath, R., Elankavi, R., & Udayakumar, R. (2017). Cloud security and compliance – A semantic approach in end to end security. *International Journal on Smart Sensing and Intelligent Systems, 10*(4), 482-494. https://doi.org/10.21307/ijssis-2017-265

Kapoor, A., & Nazareth, D. L. (2013). Medical data breaches: What the reported data illustrates, and implications for transitioning to electronic medical records. *Journal of Applied Security Research, 8*(1), 61-79. https://doi.org/10.1080/19361610.2013.738397

Karjalainen, M., Siponen, M., Puhakainen, P., & Sarker, S. (2020). Universal and culture-dependent employee compliance of information systems security procedures. *Journal of Global Information Technology Management, 23*(1): 5-24. https://doi.org/10.1080/1097198X.2019.1701355

Kark, R., Katz-Navon, T., & Delegach, M. (2015). The dual effects of leading for safety: The mediating role of employee regulatory focus. *Journal of Applied Psychology, 100*(5): 1332-1348. https://doi.org/10.1037/a0038818

Kim, H. L., & Han, J. (2019). Do employees in a "good" company comply better with information security policy? A corporate social responsibility perspective. *Information Technology & People, 32*(4): 858-875. https://doi.org/10.1108/ITP-09-2017-0298

Kim, S. S., & Kim, Y. J. (2017). The effect of compliance knowledge and compliance support systems on information security compliance behavior. *Journal of Knowledge Management, 21*(4), 986-1010. https://doi.org/10.1108/JKM-08-2016-0353

Kolomoets, E. (2022). Ensuring information security in the field of remote work. *Journal of Physics. Conference Series, 2210*(1), 12008. https://doi.org/10.1088/1742-6596/2210/1/012008

Lange, M., & Kayser, I. (2022). The role of self-efficacy, work-related autonomy and work-family conflict on employee's stress level during home-based remote work in Germany. *International Journal of Environmental Research and Public Health, 19*(9), 4955. https://doi.org/10.3390/ijerph19094955

Larsen, H. G., & Adu, P. (2021). *The theoretical framework in phenomenological research: Development and application*. Taylor and Francis. https://doi.org/10.4324/9781003084259

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care, 4*(3), 324-327. https://doi.org/10.4103/2249-4863.161306

Li, W., Liu, R., Sun, L., Guo, Z., & Gao, J. (2022). An investigation of employees' intention to comply with information security system-A mixed approach based on regression analysis and fsQCA. *International Journal of Environmental Research and Public Health, 19*(23): 16038. https://doi.org/10.3390/ijerph192316038

Liang, H., Xue, Y., & Wu, L. (2013). Ensuring employees' IT compliance: Carrot or stick? *Information Systems Research, 24*(2), 279-294. https://doi.org/10.1287/isre.1120.0427

Linneberg, M. S., & Korsgaard, S. (2019). Coding qualitative data: A synthesis guiding the novice. *Qualitative Research Journal, 19*(3), 259-270. https://doi.org/10.1108/QRJ-12-2018-0012

Lundgren, B., & Möller, N. (2019). Defining information security. *Science and Engineering Ethics, 25*(2), 419-441. https://doi.org/10.1007/s11948-017-9992-1

Malwarebytes. (2020). Enduring from home: COVID-19's impact on business security. Malwarebytes. https://www.malwarebytes.com/resources/files/2020/08/malwarebytes_enduringfromhome_report_final.pdf

Mears, D. P., & Stafford, M. C. (2022). A reconceptualization of social bond theory to predict change sequences in offending. *Crime and Delinquency*, 1112872210880. https://doi.org/10.1177/00111287221088000

Meisner, M. (2018). Financial consequences of cyber attacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting, 6*(3), 63-73. https://doi.org/10.12775/CJFA.2017.017

Mitchell, W., & Irvine, A. (2008). I'm okay, you're okay? Reflections on the well-being and ethical requirements of researchers and research participants in conducting qualitative fieldwork interviews. *International Journal of Qualitative Methods, 7*(4), 31-44. https://doi.org/10.1177/160940690800700403

Müller, T., Schuberth, F., Bergsiek, M., & Henseler, J. (2022). How can the transition from office to telework be managed? The impact of tasks and workplace suitability on collaboration and work performance. *Frontiers in Psychology, 13*, 987530-987530. https://doi.org/10.3389/fpsyg.2022.987530

Nasir, A., Abdullah Arshah, R., & Ab Hamid, M. R. (2019). A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. *Information Security Journal., 28*(3), 55-80. https://doi.org/10.1080/19393555.2019.1643956

Nasirpouri Shadbad, F., & Biros, D. (2021). Understanding employee information security policy compliance from role theory perspective. *The Journal of Computer Information Systems*, 1-10. https://doi.org/10.1080/08874417.2020.1845584

Nasirpouri Shadbad, F. & Biros, D. (2022). Technostress and its influence on employee information security policy compliance. *Information Technology & People, 35*(1): 119-141. https://doi.org/10.1108/ITP-09-2020-0610

National Institute of Standards and Technology (NIST). (n.d.) *Cybersecurity*. NIST. https://www.nist.gov/cybersecurity

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing, 18*(2), 34-35. https://doi.org/10.1136/eb-2015-102054

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*(1), 1-13. https://doi.org/10.1177/1609406917733847

Oliveira, G. (2022). Developing a codebook for qualitative data analysis: Insights from a study on learning transfer between university and the workplace. *International Journal of Research & Method in Education*, 1-13. https://doi.org/10.1080/1743727X.2022.2128745

Percy, W., Kostere, K., & Kostere, S. (2015). Generic qualitative research in psychology. *Qualitative Report, 20*(2), 76. https://doi.org/10.46743/2160-3715/2015.2097

Pew Research Center. (2020, December 9). How the coronavirus outbreak has – and hasn't – changed the way Americans work. Pew Research Center. https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work/

Pew Research Center. (2022, February 16). COVID-19 pandemic continues to reshape work in America. Pew Research Center. https://www.pewresearch.org/social-trends/2022/02/16/covid-19-pandemic-continues-to-reshape-work-in-america/

Phillippi, J., & Lauderdale, J. (2018). A guide to field notes for qualitative research: Context and conversation. *Qualitative Health Research, 28*(3), 381-388. https://doi.org/10.1177/1049732317697102

Ponemon Institute. (2017, June). *2017 cost of data breach study: United States*. Ponemon Institute. https://www.ponemon.org/userfiles/filemanager/qrylc104ssftu5sxcz32/

Privacy Rights Clearinghouse (PRC). (2019, July 19). *What is a data breach?* Privacyrights.org. https://privacyrights.org/resources/whats-data-breach

Probst, T. M., Lee, H. J., & Bazzoli, A. (2020). Economic stressors and the enactment of CDC-recommended COVID-19 prevention behaviors: The impact of state-level context. *Journal of Applied Psychology, 105*(12), 1397-1407. https://doi.org/10.1037/apl0000797

Pullan, P. (2022). Virtual leadership practical strategies for success with remote or hybrid work and teams (2nd ed.). Kogan Page, Limited.

Raddatz, N. I., Marett, K., & Trinkle, B. S. (2020). The impact of awareness of being monitored on computer usage policy compliance: An agency view. *Journal of Information Systems, 34*(1), 135-149. https://doi.org/10.2308/isys-52246

Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures: Organizations to societies. *Information Security for South Africa*, 1-7. https://doi.org/10.1109/ISSA.2014.6950492

Renaud, K., Flowerday, S., & Dupuis, M. (2021). Moving from employee compliance to employee success in the cyber security domain. *Computer Fraud & Security, 2021*(4), 16-19. https://doi.org/10.1016/S1361-3723(21)00043-9

Rogers, R. (2018). Coding and writing analytic memos on qualitative data: A review of Johnny Saldaña's the Coding Manual for Qualitative Researchers. *Qualitative Report, 23*(4), 889-892. https://doi.org/10.46743/2160-3715/2018.3459

Rose, J., & Johnson, C. W. (2020). Contextualizing reliability and validity in qualitative research: toward more rigorous and trustworthy qualitative social science in leisure research. *Journal of Leisure Research, 51*(4), 432-451. https://doi.org/10.1080/00222216.2020.1722042

Ryan, G. W., & Bernard, H. R. (2003). Techniques to identify themes. *Field Methods, 15*(1), 85-109. https://doi.org/10.1177/1525822X02239569

Ryutov, T., Sintov, N., Zhao, M., & John, R. S. (2017). Predicting information security policy compliance intentions and behavior for six employee-based risks. *Journal of Information Privacy & Security, 13*(4), 260-281. https://doi.org/10.1080/15536548.2017.1418632

San Nicolas-Rocca, T., Schooley, B., & Spears, J. L. (2014). Exploring the effect of knowledge transfer practices on user compliance to IS security practices. *International Journal of Knowledge Management, 10*(2), 62-78. https://doi.org/10.4018/ijkm.2014040105

Sandoval-Reyes, J., Idrovo-Carlier, S., & Duque-Oliva, E. J. (2021). Remote work, work stress, and work-life during pandemic times: A Latin America Situation. *International Journal of Environmental Research and Public Health, 18*(13), 7069. https://doi.org/10.3390/ijerph18137069

SANS Institute. (2023). *Security policy templates*. SANS Institute. https://www.sans.org/information-security-policy/?per-page=100

Sarkar, S., Vance, A., Ramesh, B., Demestihas, M., & Wu, D. T. (2020). The influence of professional subculture on information security policy violations: A field study in a healthcare context. *Information Systems Research, 31*(4), 1240-1259. https://doi.org/10.1287/isre.2020.0941

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity, 52*(4), 1893-1907. https://doi.org/10.1007/s11135-017-0574-8

Saunders, M. N. K., & Townsend, K. (2016). Reporting and justifying the number of interview participants in organization and workplace research. *British Journal of Management, 27*(4), 836-852. https://doi.org/10.1111/1467-8551.12182

Shih, H.-P., & Huang, E. (2014). Influences of web interactivity and social identity and bonds on the quality of online discussion in a virtual community. *Information Systems Frontiers, 16*(4), 627-641. https://doi.org/10.1007/s10796-012-9376-7

Shimura, A., Yokoi, K., Ishibashi, Y., Akatsuka, Y., & Inoue, T. (2021). Remote work decreases psychological and physical stress responses, but full-remote work increases presenteeism. *Frontiers in Psychology, 12*, 730969-730969. https://doi.org/10.3389/fpsyg.2021.730969

Sidor-Rządkowska, M. (2022). Human - the weakest or the strongest link? The role of organisational culture in ensuring security of remote work. *Journal of Modern Science, 49*(2), 608-620. https://doi.org/10.13166/jms/156776

Singh, P., Bala, H., Dey, B. L., & Filieri, R. (2022). Enforced remote working: The impact of digital platform-induced stress and remote working experience on technology exhaustion and subjective wellbeing. *Journal of Business Research, 151*, 269-286. https://doi.org/10.1016/j.jbusres.2022.07.002

Sloan, A., & Bowe, B. (2014). Phenomenology and hermeneutic phenomenology: the philosophy, the methodologies, and using hermeneutic phenomenology to investigate lecturers' experiences of curriculum design. *Quality & Quantity, 48*(3), 1291-1303. https://doi.org/10.1007/s11135-013-9835-3

Steinmetz, H., Knappstein, M., Ajzen, I., Schmidt, P., & Kabst, R. (2016). How effective are behavior change interventions based on the Theory of Planned Behavior? A three-level meta-analysis. *Zeitschrift für Psychologie, 224*(3), 216-233. https://doi.org/10.1027/2151-2604/a000255

Symantec. (2014, September). *Symantec intelligence report*. Broadcom. https://docs.broadcom.com/doc/intelligence-report-sept-14-en

Taherdoost, H. (2022). Cybersecurity vs. information security. *Procedia Computer Science, 215*, 483-487. https://doi.org/10.1016/j.procs.2022.12.050

Thelwall, M., & Nevill, T. (2021). Is research with qualitative data more prevalent and impactful now? Interviews, case studies, focus groups and ethnographies. *Library & Information Science Research, 43*(2). https://doi.org/10.1016/j.lisr.2021.101094

Toscano, F., Bigliardi, E., Polevaya, M. V., Kamneva, E. V., & Zappalà, S. (2022). Working remotely during the COVID-19 pandemic: Work-related psychosocial factors, work satisfaction, and job performance among Russian employees. *Psychology in Russia: State of the Art, 15*(1), 3-19. https://doi.org/10.11621/pir.2022.0101

Trang, S., & Brendel, B. (2019). A meta-analysis of deterrence theory in information security policy compliance research. *Information Systems Frontiers, 21*(6), 1265-1284. https://doi.org/10.1007/s10796-019-09956-4

Trang, S., & Nastjuk, I. (2021). Examining the role of stress and information security policy design in information security compliance behaviour: An experimental study of in-task behaviour. *Computers & Security, 104*, 102222. https://doi.org/10.1016/j.cose.2021.102222

Ucho, A., & Gbande, A. (2012). Personality and gender differences in compliance with safety behaviour among factory workers of Dangote Cement Company, Gboko. *IFE Psychologia: An International Journal, 20*(2), 196-207.

U.S. Bureau of Labor Statistics (BLS). (2022, March). *Telework during the COVID-19 pandemic: Estimates using the 2021 business response survey*. BLS. https://www.bls.gov/opub/mlr/2022/article/telework-during-the-covid-19-pandemic.htm

U.S. Census Bureau (Census Bureau). (2022, September 15). *The number of people primarily working from home tripled between 2019 and 2021*. U.S. Census Bureau. https://www.census.gov/newsroom/press-releases/2022/people-working-from-home.html

U.S. Census Bureau (Census Bureau). (2021, January 26). *Women are nearly half of U.S. workforce but only 27% of STEM workers*. U.S. Census Bureau. https://www.census.gov/library/stories/2021/01/women-making-gains-in-stem-occupations-but-still-underrepresented.html

U.S. Department of Health & Human Services (HHS). (2022, October 19). *Summary of HIPAA Security Rule*. HHS. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html#:~:text=The%20Security%20Rule%20protects%20a,%22%20(e%2DPHI)

Vagle, M. D. (2018). *Crafting phenomenological research* (2nd ed.). Routledge.

van Manen, M. (2016). *Researching lived experience: Human science for an action sensitive pedagogy*. Taylor and Francis. https://doi.org/10.4324/9781315421056

Verizon. (2022). *Data breach investigations report*. Verizon. https://www.verizon.com/business/resources/T7dd/reports/dbir/2022-data-breach-investigations-report-dbir.pdf

WISE. (2023). *Women in STEM workforce 2017*. WISE. https://www.wisecampaign.org.uk/women-in-stem-workforce-2017/

Wolfzorn, M., Heckert, A., & Heckert, D. M. (2006). Positive deviance and social bond theory. *Free Inquiry in Creative Sociology, 34*(2), 107-121.

World Economic Forum (WEF). (2023, April 16). *Where remote jobs are growing fastest - 4 charts show the locations and sectors*. World Economic Forum. https://www.weforum.org/agenda/2023/04/remote-jobs-growing-fastest-locations-sectors/

Xin, L., Han, L., Qing, H., & Heng, X. (2020). Why individual employees commit malicious computer abuse: A routine activity theory perspective. *Journal of the Association for Information Systems, 21*(6), 1552-1593. https://doi.org/10.17705/1jais.000646

Xu, A., Baysari, M. T., Stocker, S. L., Leow, L. J., Day, R. O., & Carland, J. E. (2020). Researchers' views on, and experiences with, the requirement to obtain informed consent in research involving human participants: a qualitative study. *BMC Medical Ethics, 21*(1), 93-11. https://doi.org/10.1186/s12910-020-00538-7

Yuan, X., Xu, Y., & Li, Y. (2020). Resource depletion perspective on the link between abusive supervision and safety behaviors. *Journal of Business Ethics, 162*(1), 213-228. https://doi.org/10.1007/s10551-018-3983-2

Zaidi, A. U., Couture-Carron, A., & Maticka-Tyndale, E. (2016). 'Should I or Should I Not'? An exploration of South Asian youth's resistance to cultural deviancy. *International Journal of Adolescence and Youth, 21*(2), 232-251. https://doi.org/10.1080/02673843.2013.836978

Zhen, J., Dong, K., Xie, Z., & Chen, L. (2022). Factors influencing employees' information security awareness in the telework environment. *Electronics (Basel), 11*(21), 3458. https://doi.org/10.3390/electronics11213458

APPENDIX A

Interview Guide

Introductions

- Interviewer introduction and rapport building
- Review research purpose
- Explain guidelines and structure of interview.

Interview

What are in-person employee experiences with ISP compliance? (RQ1)

What are remote employee experiences with ISP compliance? (RQ2)

- Tell me what you know about information security policies (ISP)?
    - Please provide examples of ISP that you are aware of.
    - Are the ISP helpful/informative?
    - What is the intention of these ISP?

What factors influence in-person employees to comply with ISP compliance? (RQ3)

What factors influence remote employees to comply with ISP compliance? (RQ4)

- What makes you more or less likely to follow ISP?
    - Prompts: stress, workload, clarity of ISP, automation, tools
- What is your organization's stance on ISP compliance?
    - Are ISP mandatory or just a nice to have?
    - Does anything happen to you if ISPs are or are not followed?
- What would you change in your organization to increase your ISP compliance?
    - Do you have easy access to ISP documents?
    - Are there automated workflows and tools that help with ISP compliance?
    - What resources do you have available to ensure that you have the ability to

comply with ISP?

What impact does a relationship between a manager and employee influence ISP compliance? (RQ5)

- How connected to you feel to your co-workers, managers, and leadership?
    - Do you consider yourself friends with people from work?
    - How does your connectedness impact/influence your ISP compliance?
    - If you ever worked in-person and now work remote (or vice versa), how are your work relationships different?
    - If you ever worked in-person and now work remote (or vice versa), how did your work relationships impact your ISP compliance?

Demographic Questions

- What is your gender?
- What year were you born in?
- How long have you worked for your organization?
- Where do you live?
- Where is your organization headquartered?
- What is your title in your organization?
- What type of industry is your organization? (Retail, financial, education, healthcare, etc.)
- Are you mostly remote or in-person?
- How familiar are you with ISP on a scale of 1 to 5 with 5 being extremely familiar?

APPENDIX B

Verbal Recruitment Script

Hello, I am recruiting participants for my research study. The study explores the lived experiences of in-person and remote employees that have information security policies or procedures (ISP) to follow. Participation includes up to a one hour Zoom online, recorded, video conference interview and optional review of interview transcript and findings. Individuals may be eligible if they agree to spend approximately one hour in a video call with researcher, are employed by an organization (not self-employed), work full-time 100% remote or 100% in-person, and are aware that their organization requires them to follow at least one ISP. The goal is to understand the lived experiences of in-person and remote employees regarding ISP compliance within organizations. Please let me know if you have any questions.

APPENDIX C

Text Recruitment Script for Email and Social Media

This study explores the lived experiences of in-person and remote employees that have information security policies or procedures (ISP) to follow. Participation includes up to a one hour Zoom online, recorded, video conference interview and optional review of interview transcript and findings. Individuals may be eligible if they agree to spend approximately one hour in a video call with researcher, are employed by an organization (not self-employed), work full-time 100% remote or 100% in-person, and are aware that their organization requires them to follow at least one ISP. The goal is to understand the lived experiences of in-person and remote employees regarding ISP compliance within organizations. For more information, please contact the study principal investigator.

Study ID: TBD

Principal Investigator: Joyce Mui

APPENDIX D

Participant Pseudonym	**Generation**
Rusty	Baby Boomer
Reid	Generation X
Roman	Generation X
Isaac	Generation X
Ray	Millennial
Raven	Millennial
Rhett	Millennial
Remington	Millennial
Ira	Generation X
Rhys	Generation X
Ivan	Millennial
Rupert	Millennial
Rufus	Millennial
Rex	Generation X
Irvin	Millennial
Rachel	Generation X
Iver	Millennial
Ike	Millennial
Isadora	Generation X
Ilya	Millennial