A Qualitative Study of Self-Determination Theory in Cybersecurity Using Autonomy Framing

By

Philip Mercer Romero-Masters

A dissertation submitted in partial fulfillment of

The requirement for the degree of

Doctor of Philosophy

(Information)

at the

UNIVERISTY OF WISCONSIN-MADISON

2023

Date of final oral examination: 04/28/2023

The dissertation is approved by the following members of the Final Oral Committee:

Kristin Eschenfelder, Professor, Information School

Alan Rubel, Professor, Information School

Corey Jackson, Assistant Professor, Information School

Mike Xenos, Professor, Life Sciences Communication

Abstract

Organizations consider cybersecurity important to prevent costly cybersecurity breaches. Using cybersecurity awareness training organizations motivate their users to engage in cybersecurity best practices to prevent cybersecurity incidents. Recent cybersecurity motivation research has shown that intrinsic motivation using Self-Determination Theory (SDT) effectively motivates compliance intentions. SDT holds that supporting autonomy, competence and relatedness will lead to higher reported well-being. While the research shows positive compliance intentions, it is unclear if SDT-based motivation in cybersecurity leads to higher well-being. To explore this, this study interviewed 20 participants. We divided participants into two groups. One group received a cybersecurity training document with autonomy framing, while the other group received a cybersecurity training document without autonomy framing. After reviewing the cybersecurity training document, we administered three scales to measure autonomy and wellbeing: the Subjective Vitality Scale, the Learning Self-Regulation Questionnaire, and the Perceived Autonomy Support Questionnaire – Work Climate Questionnaire. Then, participants were questioned about their preferences on the cybersecurity training document around autonomy framing and how cybersecurity can support their well-being. As part of the interview, participants viewed both the autonomy and non-autonomy cybersecurity training document and offered their impressions on the language differences between the two versions. The mean Self-regulation Relative Index for the autonomy group was 2.01 where the non-autonomy group was .63, which is suggestive that a significant difference might be found with a study with more participants. Participants responses to interview questions followed these trends: participants indicated cybersecurity training should include contextual information, participants indicated cybersecurity training should treat users in a caring manner, participants hold a variety of views on negative extrinsic motivation, participants perceive negative extrinsic motivation when none is used, participant recognize others' communication preferences, participant believe engaging in cybersecurity best practices is a personal responsibility but recognize that employers are mandating the behavior, some participants view autonomy language positively while others do not, and participants were familiar with the training content and indicated that this increases their confidence. The results of these interviews suggest participants feel autonomy in cybersecurity, but that autonomy framing in cybersecurity training documents is not always viewed favorably. Participant responses inform the research on wellbeing and cybersecurity communication. Future research should further explore cybersecurity communication preferences through qualitative study and test for self-regulation through quantitative studies with more participants.

Acknowledgments

My husband James, who inspires me and believes in me when I don’t. My mom, who held me up when I felt down and kept me going when the last year felt like torture. My friends and colleagues, who were there when I needed them. My advisor and each member of the committee, who have provided patient guidance helping me in their own ways. The UW-Madison department of Educational Psychology, who supported me through my MA and the early years of my PhD program. The UW-Madison iSchool staff, who have helped me with the all the administrative aspects of going through the program. My dog Luke, my cat Anakin, and my other cat Ashelia, who kept me company through taking online classes, grading papers, and writing.

Thank you.

Table of Contents

Table and Figure Legend

Chapter 1 Introduction

The focus of this dissertation is to explore how organizations can support their users in cybersecurity training by using effective communication. Cybersecurity is a crucial concern for organizations, as cyber-attacks happen frequently and can result in millions of dollars in damages (Pagliery, 2015; Spring, 2021). To protect the organization from cyber-attacks organizations must rely on both technical and human means of preventing a successful attack (Hancock, 2022). However, the human factor can be exploited by cybercriminals who try to manipulate users into compromising their organization's cybersecurity (Abroshan et al., 2021; Burns et al., 2019). Therefore, organizations use cybersecurity awareness training to teach and influence their users to behave in ways that protect their organization.

Users who adopt cybersecurity best practices into their personal cybersecurity practice are better protected from cybersecurity incident that can harm the organization. Unfortunately, users tend to be resistant to cybersecurity awareness training, as they view best practices as an obstacle to their work (Albrechtsen, 2007). To study how to better support organizational cybersecurity through cybersecurity awareness training, this dissertation study uses a qualitatively focused mix-method design to test communication changes to a cybersecurity training document. Participants were randomly assigned to one of two groups in an A/B test and presented either an autonomy or non-autonomy version of the same cybersecurity awareness training document. Next participants responded to several scales to measure their vitality, self-regulation, and perceived autonomy support. Following this, participants provided feedback through open-ended questions and compared both versions of the training to uncover their preferences and perceptions about autonomy and well-being in cybersecurity awareness training.

The study of cybersecurity human factors is crucial for safeguarding organizations This research goes beyond the study of compliance intentions and instead adopts a values-in-design approach to modify cybersecurity awareness training, to promote user perceptions of autonomy and well-being. The goal is to encourage users to view cybersecurity as a positive, autonomy-supporting aspect of their lives, rather than coercing them into best practices. Framing techniques were employed to manipulate user perceptions of cybersecurity with an added focus on achieving user well-being. Users often report negative emotions when considering cybersecurity, and this research utilizes Self-Determination Theory to support perceptions of autonomy, competence, and relatedness, resulting in greater well-being (Albrechtsen, 2007; McDermott, 2012; Renaud et al., 2021; Ryan, 2017). Previous work with autonomy support has shown it leads to compliance motivation in cybersecurity while studies have not explored its impact on user wellbeing – the gap in the literature this dissertation seeks to fill (A. Johnston, 2020; Lee, 2015; Menard et al., 2017).

This dissertation uses interviews to understand user experiences, recognizing that reality is fixed, and human knowledge of reality remains limited. Participants' meaningful experiences offer valuable insights that shape the research. This dissertation aims to answer two questions: 1) What are professionals' impressions of autonomy-framed cybersecurity training content? 2) What are professionals' impressions of cybersecurity training content regarding wellness? The study uses three instruments to measure autonomy and well-being, including the Subjective Vitality Scale, the Learning Self-Regulation Questionnaire, and the Perceived Autonomy Support Questionnaire-Work Climate Questionnaire. The Subjective Vitality Scale measures vitality which is considered part of wellbeing. The Learning Self-Regulation Questionnaire measures the level of autonomous and controlled regulation in a learning environment and computes a self-regulation score. Self-regulating is part of wellbeing and is experienced autonomy. The Perceived Autonomy Support

Questionnaire – Work Climate Questionnaire measures perceived autonomy in a work environment. Additionally, several open-ended questions were used to uncover positive and negative experiences related to the version of the cybersecurity training document they received. Participants then directly compare both versions of the training document and offer their preferences. Analysis includes both the computation of scores from the instruments as well as both inductive and deductive coding of the interview transcripts. Several rounds of coding led to the development of themes. Importantly there are limits to our methodology such as limitations regarding external validity, internal validity, construct validity, objectivity, and the Hawthorne effect.

This dissertation involved the participation of 20 professional and pre-professionals but only 19 of the participant's data could be used. With a small N, the results of the questionnaire should be considered only as a pilot for a larger quantitative study. Neither the Subjective Vitality Scale, nor the Perceived Autonomy Support Questionnaire – Work Climate Questionnaire produced any significant results. The Learning Self-Regulation Questionnaire did produce a significant difference in self-regulation scores between the autonomy and non-autonomy group. This effect appears as a small insignificant difference between the groups in perceived autonomous regulation and a larger insignificant difference in perceived controlled regulation. Thematic analysis revealed 7 main themes, 2 themes had multiple perspectives, and Theme III had a subtheme. The Themes are:

- Theme I: Participants Indicated Cybersecurity Training Should Include Contextual Information
- Theme II: Participants Indicated Cybersecurity Training Should Treat Users in a Caring Manner

- Theme III: Participants hold a Variety of Views on Negative Extrinsic Motivation
    - Perspective: Repercussions are Necessary
    - Perspective: Threats can Deter Compliance
- Theme III-B: Participants Perceive Negative Extrinsic Motivation When None is Used
- Theme IV: Participant Recognize Others' Communication Preferences
- Theme V: Participant Believe Engaging in Cybersecurity Best Practices is a Personal Responsibility but Recognize that Employers are Mandating the Behavior
- Theme VI: Some Participants View Autonomy Language Positively While Others Do Not
    - Perspective: Autonomy Language Creates Positive Perceptions
    - Perspective: Autonomy Language is Bad for Cybersecurity
- Theme VII: Participants were Familiar with the Training Content and Indicated That This Increases Their Confidence

The findings of this dissertation make significant contributions to the existing literature on cybersecurity. The results indicate that autonomy framing might support self-regulation and wellbeing among users, and that users appreciate being treated in a caring manner. However, the study also suggests that autonomy framing may not necessarily produce autonomy perceptions in participants, but rather prevent autonomy loss. Additionally, participants appear to be divided on negative extrinsic motivation, which may be indicative of a divide between those who have internalized cybersecurity practices and those who have not.

These results offer cybersecurity professionals important guidance on how to communicate effectively with users. Participants preferred cybersecurity communication that offered context and treated them in a caring manner. However, they were divided on whether autonomy framing was effective in promoting cybersecurity practices. Nonetheless, the fact that participants recognize their communication preferences as preferences suggests that they are understanding of communication that may not necessarily align with their preferences.

Further research is needed to explore the divide among users and to investigate the kinds of information users want to see in cybersecurity training. Quantitative studies can also be conducted to test whether autonomy framing supports wellbeing in cybersecurity. Despite the limitations of this study, the results offer valuable insights that can help to improve cybersecurity awareness training and ultimately protect organizations from cyber threats.

This chapter continues by providing background information on the purpose and methodology of this dissertation. It covers the essential knowledge necessary for readers to understand the reasons for conducting research in cybersecurity, including the role of human decision making in cybersecurity incidents and the potential for error and malicious influence. Additionally, the chapter discusses why information technology users may be reluctant to participate in cybersecurity training programs and how user behavior plays a critical role in preventing cybersecurity incidents. The chapter also outlines how communication around cybersecurity can effectively promote cybersecurity to users which will ultimately prevent cybersecurity incidents. The chapter concludes by outlining the research aims, introducing the research questions (see the research methods section for more details), discussing the significance of the study for research and practice, and highlighting potential limitations of the research methodology.

Cybersecurity and the Human Factor

According to a top cybersecurity organization, 88% of cybersecurity breaches are caused by employee errors (Hancock, 2022). Users can compromise the security of their organization by choosing weak, compromised, or previously used passwords, as well as by not following cybersecurity procedures such as locking their device when not in use, clicking on malicious links, or neglecting to update their antivirus and other software.

While technical cybersecurity systems provide protection, they are not foolproof, and ultimately, the cybersecurity of an information system relies on the actions of its users. Anti-virus software relies on users to update the virus definitions to be effective protection. A password prevents an unauthorized user from accessing an information system only if the password cannot be acquired by an unauthorized user. Organizations attempt to protect their users by providing cybersecurity awareness training, while malicious actors attempt to manipulate users through phishing emails. The conflict between cybersecurity experts and malicious actors has escalated to a war of competing influence, with humans being the most vulnerable component of a cybersecurity system (Proctor & Chen, 2015). Malicious actors attempt to trick users into compromising their cybersecurity and cybersecurity offices attempt to persuade users to develop habits that protect their cybersecurity. Effective cybersecurity requires the technical and human elements of an organization to work in tandem to protect against potential security breaches.

Human Error

Human errors have led to costly data breaches such as the Equifax Breach (*Actions Taken by Equifax And Federal Agencies in Response to The 2017 Breach*, 2018). Failure to patch a known security vulnerability caused the Equifax Breach which allowed hackers access to the personal information of 145.5 million people(*Actions Taken by Equifax And Federal Agencies in Response to The 2017 Breach*, 2018). The Equifax credit agency handles the financial information of people across the country. The compromise of sensitive information of so many upset a lot of people. Another example of an employee mistake leading to a cybersecurity incident happened in higher education. An employee at Strathmore College published student records on the school intranet which exposed confidential student information to all the employees of the college (Press, 2018). Routine cybersecurity-related decisions have caused large economic disruptions such as how reusing a password caused the Colonial Pipeline to be shut down (Spring, 2021). The shutdown pipeline led to a rush on fuel in the eastern United States which created shortages and huge price spikes. Routine security decisions have large impacts and errors lead to harms.

The Malicious Influence

Social engineering attacks occur when a malicious actor attempts to trick a user into compromising the security of their system (Burns et al., 2019). Malicious actors often send phishing emails that attempt to install or exploit a technical vulnerability on a system by sending deceptive emails (Abroshan et al., 2021). In these cases, a technical vulnerability can only be exploited after a user does some action. Malicious actors often use emails to manipulate the user to perform such actions. These attacks trick users in order to breach the cybersecurity of organizations. Clicking a malicious link can lead to unauthorized access to sensitive systems. Poorly managed or generated passwords can also introduce vulnerabilities to systems with strong technical defenses.

Organizations invest significantly in preventing cybersecurity incidents. The cost of failing to prevent a security breach can be high in terms of reputation, financial losses, and time (*Actions Taken by Equifax And Federal Agencies in Response to The 2017 Breach*, 2018; Press, 2018; Spring, 2021). Small human errors or misjudgments can cost organizations billions of dollars and have negative impacts for people across the world (Sobers, 2019; *The Human Factor in IT Security: How Employees Are Making Businesses Vulnerable from Within*, n.d.; "Usability & Human Factors," 2016).

Organizations spend a lot of time and money to encourage secure behavior in their users. A security conscious individual with knowledge of how to avoid the latest social-engineering attack helps protect the security of an organization.

Robust organizational cybersecurity engages with users and implements cybersecurity awareness programs to educate users on the latest threats (Abawajy, 2014). Cybersecurity awareness training (CAT) is one of the main methods organizations use to prevent user errors that lead to data breaches. CAT educates and communicates the organizations expectations to users regarding cybersecurity. CAT encourages cybersecurity behavior or decisions that minimize the likelihood an employee will compromise the cybersecurity of the organization. Seemingly small tasks such as performing security updates, or using multi-factor authentication, decrease the likelihood of a cybersecurity incident occurring (*What Is Cybersecurity?*, 2019).

Resistance to Cybersecurity Awareness Training

In many professional settings, it's common for new personnel to receive cybersecurity awareness training (CAT) during their onboarding process, with updates typically provided annually. Typically, CAT emphasizes what users must do to safeguard their organization and the risks associated with cyber threats. There are various ways to frame, alter the wording and emphasis of a message, CAT. Common approaches emphasizes the danger of cyberthreats or that performing cybersecurity practice is a requirement of employment (Boss et al., 2015; Faizi & Rahman, 2020). These approaches use fear and control (Boss et al., 2015). As an alternative to fear and control framing, this dissertation explores the potential of using autonomy framing, which is a way of communicating about cybersecurity in a way that supports autonomy perceptions.

It's been noted that cybersecurity training often fails to motivate users in a positive manner. This is due to the perception by users that secure practices are an inconvenience and can interfere with their primary work tasks (Albrechtsen, 2007). Consequently, organizations face the challenge of motivating their users to adopt secure behaviors to safeguard their interests. To overcome this challenge, researchers must identify the external and internal factors that impact user behavior, including organizational communication (Camp, 2004; Jenkins et al., 2016). By understanding the role of security communication preceding cybersecurity behavior, we can better support strong cybersecurity practices (Crossler et al., 2013).

Cybersecurity Behavior

While previous research indicates that people are concerned about their security and privacy, their behavior may not always align with these reported concerns (Kokolakis, 2017). Unfortunately, users frequently view security as secondary to other priorities, and organizational cultures tend to prioritize efficiency over security (Albrechtsen, 2007).

Organizations are highly motivated to prevent cybersecurity incidents due to their high likelihood and potential impact (Reeves et al., 2021). To achieve this, they actively communicate with users about cybersecurity and motivate them to adopt secure behaviors. However, simply informing users about cybersecurity best-practices does not necessarily lead to behavioral change. To truly prevent security breaches, organizations must adopt effective communication strategies that encourage a cybersecurity culture where users prioritize safeguarding data and information systems. By doing so, organizations can go beyond merely educating users about cyber threats and create a culture where cybersecurity is viewed as a top priority.

Cybersecurity Communication

Large organizations often use mass communication to efficiently convey information or influence the behavior of their users. However, the way in which organizations frame their communication is critical. Framing alters the wording and emphasis of communication. Framing refers to the way communication is worded and emphasized, and good framing can effectively change behavior and influence the audience of a message (Cacciatore et al., 2016; Entman, 1993; D. A. Scheufele & Iyengar, 2014). Framing can be an important method for motivating behavior change, particularly in the context of cybersecurity. By using effective framing strategies, organizations can effectively motivate users to adopt secure behaviors and prioritize cybersecurity.

Cybersecurity compliance requirements are often communicated via CAT, and how organizations construct these training materials has the potential to change employee behavior. In this study, we explore the impact of autonomy framing on cybersecurity training materials and its effects on professionals' perceptions (see research methods sections for details). This study seeks to create a sense of autonomy (rather than generating true autonomy) to support the wellbeing of users.

Aims of the Study

Given the difficulties in motivating productive cybersecurity behavior, this study aims to investigate users' experiences when presented with CAT framed using autonomy framing and framing from the field. While previous studies have explored user preferences regarding CAT format and design. Our study seeks to understand how framing CAT content with autonomy affects user perceptions (Abawajy, 2014; Al-Hamdani, 2006; Torten et al., 2018). Specifically, we aim to uncover professionals' perceptions of autonomy and wellbeing when interacting with a laboratory-based CAT.

The Research Problem and Related Questions

This study aimed to investigate user perceptions within CAT contexts, specifically focusing on the constructs of Self-Determination Theory (SDT): autonomy and wellbeing. Multiple methods were used and both quantitative and qualitative data were collected. Participants were presented with either a standard CAT document or a modified version with autonomy framing. The standard CAT document represents current CAT practices as it is not modified from how it was presented on the Cybersecurity and Infrastructure Agency website. They were then asked a series of open-ended questions related to how they felt about the training they received before being presented with both versions and asked about their preferences between the two. They were also given structured questionnaires that collected data about autonomy, and well-being. This dissertation aims to explore the following research questions (see the research methods chapter for more details):

Research Question: What are the autonomy impressions of professionals regarding autonomy-framed cybersecurity training content?

Research Question: What are the wellbeing impressions of professionals regarding autonomy-framed cybersecurity training content?

Significance

Contribution to Research: This dissertation aims to make significant contributions to the existing research literature in the field of cybersecurity by investigating the relationship between autonomy support and wellness. While previous studies have established that autonomy support can motivate users in home and work contexts, this study seeks to add a new dimension to the research by exploring the impact of autonomy support on user wellness. (Ryan, 2017) suggests that autonomy support will lead to higher wellness in users (Ryan, 2017). Although previous research has looked at the link between autonomy support and compliance in cybersecurity using surveys and experiments, there is a gap in the literature when it comes to interview studies (A. Johnston, 2020; Lee, 2015; Menard et al., 2017). Through this study, we hope to shed light on the potential benefits of autonomy support in cybersecurity motivation efforts and uncover whether perceived autonomy can bring wellness benefits to users in this context. By building upon the principles of SDT, this research will advance our understanding of the role of autonomy support in promoting wellness and motivation in cybersecurity (Ryan, 2017).

Contribution to practice: The findings of this study hold promise for enhancing cybersecurity practices. By shedding light on users' attitudes towards cybersecurity training, this research deepens our understanding of the subject. Moreover, it builds on previous studies that have used SDT to explore cybersecurity motivation (Lee, 2015; Menard et al., 2017). While earlier research has demonstrated the potential of SDT to motivate users, it has yet to establish its advantage over fear or control-based approaches to cybersecurity (A. Johnston, 2020; Lee, 2015; Menard et al., 2017; Wall et al., 2013). By evaluating participants' perceptions of autonomy within the context of CAT content, this study provides valuable insights into the viability of SDT in cybersecurity. Ultimately, these findings may guide future efforts to improve cybersecurity practices, whether by further exploring SDT approaches or pursuing alternative strategies.

Chapter 2: Literature Review

Introduction

This chapter delves into the literature relevant to the dissertation. It commences with an overview of human factors in cybersecurity. The subsequent section introduces the concepts of influence, persuasion, and manipulation. Autonomy is then introduced as a crucial value, and subsequent sections elaborate on its role in self-determination, its connection to well-being, and previous studies on autonomy in cybersecurity. Framing is also discussed, with a focus on its relationship to cybersecurity, and the distinctions between appeals, support, and framing are clarified. Given the dissertation's close ties to emotions, the following section examines emotions in cybersecurity. Lastly, the literature review chapter concludes with an analysis of the gaps and requirements in the field.

Human Factors in Cybersecurity

In the realm of cybersecurity, behavior modification is not only appropriate but also crucial. One way to achieve this is by providing cybersecurity training to users and modifying their behavior (Yaokumah et al., 2019). CAT presents an opportunity to influence the behavior of organizational end-users. Previous studies have shown that appeals based on autonomy can be used to motivate individuals (Menard et al., 2017). The application of autonomy in cybersecurity motivation is grounded in Self-Determination Theory, which posits that promoting autonomy, competence, and relatedness leads to well-being (Deci et al., 1989; Ryan, 2017; Williams et al., 1996, 1999). Despite individuals reporting concern for their security, their behavior does not always align with these sentiments (Albrechtsen, 2007; De Keukelaere et al., 2009; Jenkins et al., 2016). Organizational users often view cybersecurity behavior as a hindrance to their primary work tasks (Albrechtsen, 2007). This may be because security is often viewed as secondary, and organizational cultures tend to prioritize efficiency (Albrechtsen, 2007).

Influence, Persuasion, Manipulation

There are various ways that influence can be categorized, and it's important to understand the distinctions between them. Persuasion, for example, is a form of influence that appeals to the rational mind, and it allows individuals to make a choice based on their own judgment (Susser et al., 2018). When someone is persuaded, they have the space to deliberate and consider different options before coming to a decision. However, persuasion should never restrict or limit someone's choices (Susser et al., 2018). On the other hand, coercion is a type of influence that gives an individual no choice but to comply (Susser et al., 2018). It involves applying pressure, threats, or incentives that are so strong that they leave no room for alternative choices (Susser et al., 2018). Coercion may alter the decision-making space, but it does not allow for rational deliberation (Susser et al., 2018). It's important to note that coercion is different from persuasion, and it can be harmful when used to limit someone's freedom of choice (Susser et al., 2018).

Another form of influence is manipulation (Susser et al., 2018). When someone is manipulated, they do not make choices based on rational considerations but instead rely on psychological levers that alter their beliefs, desires, or emotions (Susser et al., 2018). Manipulation removes the ability to make rational decisions. Unlike persuasion or coercion, manipulation aims to control the decision-making process, giving the manipulator an unfair advantage (Susser et al., 2018). Most importantly manipulation must be hidden (Susser et al., 2018). Manipulative actions when detected no longer manipulate a person. If an actor plays upon desire but the person feels no other choice, they have been coerced. In the same scenario, if the person feels they still retain a choice but still decides to act in line with the actor attempting to manipulate them, then the person was not manipulated and instead persuaded by bad reasons (Susser et al., 2018). A person must not understand or detect how they are being influenced to be manipulated (Susser et al., 2018).

Understanding manipulation is important because framing is a manipulation if it is undetected. Framing seeks to alter how a topic is considered in favor of one aspect of the topic (Entman, 1993). When receiving framed content then the audience may experience 1) manipulation if the framing is undetected, or 2) persuasion, if the framing is detected. When organizations apply irresistible incentives or threats to pressure the adoption of cybersecurity practices then they coerce their users, this study uses framing to modify participant perceptions, but importantly the framing should be detectable to participants (Susser et al., 2018). This study seeks to openly appeal to users but not by rational considerations of danger and risk but rather by altering how they think about the topic of cybersecurity.

Self-Determination Theory

Self-determination Theory (SDT) posits that promoting autonomy can enhance an individual's well-being (Ryan, 2017). This theory emphasizes that supporting a person's basic needs can lead to positive motivation which encompasses autonomy, relatedness, and competence (Ryan, 2017). Unlike conventional motivational techniques that rely on controlling language or fear appeals, SDT advocates for intrinsic motivation(Menard et al., 2017).

According to SDT, satisfying these fundamental needs fosters intrinsic motivation, which is characterized by an inner desire to engage in an activity for its own sake (Ryan, 2017). Conversely, extrinsic motivation stems from external factors and manifests when individuals perform actions to attain rewards or avoid negative outcomes (Ryan, 2017). By promoting intrinsic motivation, SDT seeks to enhance individuals' pleasure and involvement in their activities (Ryan, 2017).

Organismic Integration Theory

Within SDT, there exist several mini theories, including Organismic Integration Theory (OIT). OIT does not assume that supporting the basic needs of people will morph extrinsically motivated activities to intrinsically motivated activities, instead OIT suggests that supporting the three basic needs will move the motivation along the Perceived Relative Autonomy Scale (see Figure 1) where fully extrinsic motivation is at one end and the further along the scale the more intrinsic the motivation is (Ryan, 2017). OIT also identifies four types of extrinsic motivation that rank from most to least extrinsic: external regulation, introjected regulation, identified regulation, and integrated regulation (Ryan, 2017). Through supporting the three basic needs, motivation becomes more intrinsic and internalized within the self, thus moving it along the perceived relative autonomy scale (Ryan, 2017). Internalization refers to the process by which an individual incorporates beliefs, attitudes, or feelings as their own and integrates them into their sense of self.

External Regulation

External regulation occurs when the perception of an external contingency motivates behavior (Ryan, 2017). External regulation falls on the low end of perceived relative autonomy. People experiencing external regulation perceive a reward for engaging in an activity or a punishment for not engaging in the activity. External regulation lacks in sustained motivation. When the contingent reward or punishment is withdrawn then the behavior is not sustained. The perceived locus of causality in external regulation is external, thus the behavior is controlled. A perceived locus of control can be detrimental to autonomy.

Introjected Regulation

Introjection is a kind of internalization that occurs when a person adopts or takes in a regulation or value with incomplete assimilation (Ryan, 2017). Introjected regulation falls between external regulation and identified regulation in terms of relative autonomy. People experiencing introjected regulation when an internal pressure to engage in a behavior motivates said behavior. The internal pressure presents to a person as a feeling “should” or “must” engage in the behavior. Introjection is intrapersonal and occurs within an individual and the pressure stems from self-esteem contingencies rather than external contingencies in external regulation. Feelings of pride , guilt, self-consciousness, and critical self-evaluation are associated with introjected regulation.

Identified Regulation

Identification is a kind of internalization that occurs when a person consciously endorses regulations or values (Ryan, 2017). Identified regulation falls closer to intrinsic motivation than introjected or external regulation in terms of relative autonomy. People experiencing identified regulation consider the regulation or value as important for themselves. Identified regulation is associated with an internal perceived locus of causality and greater experiences of autonomy than external or introjected regulation.

Integrated Regulation

Integration is a kind of internalization that occurs when a person actively and in a transformative manner brings a value or regulation into congruence with other aspects of oneself (Ryan, 2017). Integrated regulation falls closest to intrinsic motivation in terms of relative autonomy but is still considered extrinsic motivation. People experiencing integrated regulation have holistically embraced the regulation or value without incongruence with other aspects of the self.

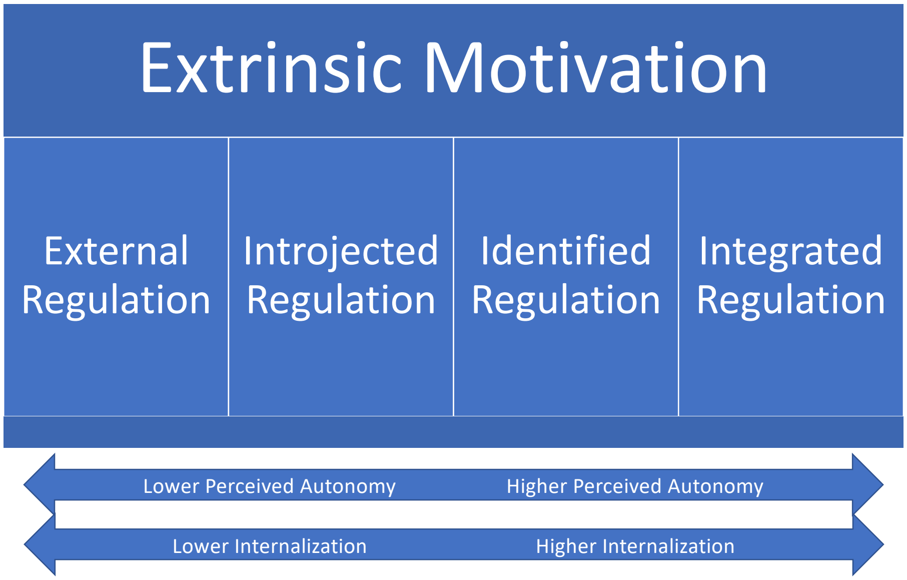

Figure 1: Perceived Relative Autonomy Scale

Basic Psychological Needs Theory

SDT stands out among other theories by prioritizing the self (Ryan, 2017). Unlike using "a person," the self within SDT refers to the fully integrated aspects of an individual (Ryan, 2017). Another of the min-theories within SDT, the Basic Psychological Needs Theory describes that supporting the three basic needs contributes to individual well-being (Ryan, 2017). To avoid confusion, this dissertation refers to SDT in general rather than specific mini theories.

Several studies utilizing SDT have reported favorable outcomes in organizational training (Strempfl et al., 2022; Tafvelin & Stenling, 2021). For instance, a recent study revealed that self-determination promotes learning in the context of CAT (Kam et al., 2021). The researchers conducted an experiment using an online security awareness training program and found that supporting autonomy, competence, and relatedness correlated with actual learning behaviors and learning effort in the CAT context (Kam et al., 2021).

Perceived Autonomy

In this dissertation, we focus on autonomy in the design of a cybersecurity training and explore how users experience the training compares between those who receive autonomy language and those who do not. According to SDT, autonomy is one of the essential components necessary for a person to function at their fullest (Ryan, 2017).

SDT relies on a psychological view of autonomy and is concerned with behavior as a function of consciousness (Ryan, 2017). In this dissertation and within SDT theory, autonomy does not refer to the theoretical conditions of if or when a person can exist in a state of autonomy. Whether individuals experience true autonomy and what the nature of being autonomous is lies beyond the scope of this dissertation. When referring to autonomy throughout this dissertation we are really referring to perceived autonomy. We explore autonomy here to describe the phenomenon of perceived autonomy as a predictor for wellbeing. This dissertation relies on the characteristics of autonomy to help identify when participants may be experiencing perception of autonomy.

SDT considers autonomy to refer to the need of a person to self-regulate their actions and experiences (Ryan, 2017). Autonomous functioning is volitional, congruous, and integrated (Ryan, 2017). Autonomy is not independence or self-reliance but rather endorsement of the actions a person takes (Ryan, 2017). Autonomous functioning is characterized by actions that align with a person's values or interests and lead to wholehearted engagement (Ryan, 2017). SDT also acknowledges that external or non-integrated factors may motivate behavior and that not all intentional actions are autonomous, instead SDT considers that external or nonintegrated aspects of a person may motivate behavior (Ryan, 2017). Acting without autonomy can lead to internal conflict and a lack of alignment between a person's values and actions (Ryan, 2017).

The libertarian perspective on autonomy defines it as "freedom from undue influence," which this dissertation considers an important viewpoint (Mackenzie, 2008; van der Vossen, 2019). Negative freedom or freedom from external influence plays a significant role in our conception of autonomy, although complete freedom from undue influence is not possible, as individuals are shaped by their society (Mackenzie, 2008; Rubel et al., 2020). Our conception of autonomy instead seeks to support autonomy by limiting the perception of undue influence. The standard cybersecurity document includes language such as “be sure to”, “select passwords”, “You should”, and “be suspicious.” Each of these are snippets of the document are imperatives. The standard cybersecurity training uses imperative and command language to influence the user. While the purpose of cybersecurity training is to influence the user, the excessive use of controlling language reads like a list of orders, undermining the user's autonomy. An autonomous person should instead feel ownership, responsibility, and an authentic desire to engage in cybersecurity to protect the assets of themselves and their organization. To support the autonomy of the user, we have reframed the standard document to reduce the controlling language that subverts the user's autonomy needs. The definition we use for autonomy in this dissertation is as follows:

Autonomy is freedom from undue influence and is characterized by feelings of ownership, responsibility, and an authentic connection to behavior.

Autonomy in Cybersecurity

SDT when applied to cybersecurity supportive behavior has yielded varying results, and as such I shall examine the work in this area in detail (A. Johnston, 2020; Kam et al., 2020; Lee, 2015; Menard et al., 2017; Wall et al., 2013).

A multi-theory approach combining psychological reactance theory and SDT to compliance intentions indicated trait-based autonomy might increase security compliance (Wall et al., 2013). According to psychological reactance theory people prefer to be free from the control of others (Wall et al., 2013).People will strive to restore their freedom when it is controlled by an external force. Reactance is the action of someone trying to restore their own freedom. Reactance and autonomy each consider feelings of control and freedom from outside pressure (Rosenberg & Siegel, 2018). Another interest of this study was self-efficacy a predictor of cybersecurity compliance intentions (Almuqrin, 2019; Bandura, 1977; Chen et al., 2019; Wall et al., 2013). The Wall study surveyed government employees for efficacy measures, self-determination, reactance, and information security compliance intentions (Wall et al., 2013). This study considered psychological reactance as trait-based; however, an alternate view approaches reactance as a state (Wall et al., 2013). The study concluded that autonomy increased perceptions of self-efficacy, while reactance decreased self-efficacy (Wall et al., 2013).

A more SDT focused approach showed that “perceived autonomy, perceived competence, and perceived relatedness significantly predicted security compliant behavior” (Lee, 2015). The study by Lee administered a survey to 155 survey monkey users (Lee, 2015). The survey included the basic needs satisfaction at work scale and the compliant at work scale (Lee, 2015). The predictive capability of perceived competence made a significant contribution to explaining the criterion variable of the study.

Perceived autonomy rather trait-based autonomy has been shown effective as well (Menard et al., 2017). The Menard study used a full factorial design to test appeals to adopt a password manager with elements of protection motivation theory and SDT (Menard et al., 2017). After receiving a persuasive message, individuals were assessed for their intention to comply with the message and their perceptions of autonomy and other SDT and protection motivation theory variables (Menard et al., 2017). A replication of that same study in organizational users confirmed the importance of autonomy over other variables in the study (A. Johnston, 2020).

A laboratory experiment looking at the behavior of people trying to learn to perform a SQL injection confirmed the role of autonomy in cybersecurity using behavioral data (Kam et al., 2020). This study was focused on technology students and not on the non-technology oriented user (Kam et al., 2020).

Wellbeing

A person who is well has had their basic psychological needs supported, which includes the perception of autonomy, competence, and relatedness in their life (Ryan, 2017). When these needs are met, a person can function at their full capacity and self-regulate in their human capacities (Ryan, 2017).

Although a person who experiences sustained wellbeing is likely to report higher levels of happiness than someone who is less well, it is important to note that wellbeing encompasses more than just happiness (Ryan, 2017). Wellbeing describes at a general level how a person is functioning (Ryan, 2017).Full functioning requires the perception that one governs their own life (Ryan, 2017). A person can experience happiness without feeling in control of their life, but they are not fully functioning in this case (Ryan, 2017). Furthermore, a person can also experience happiness without feeling competent or connected to others, which can be detrimental to their wellbeing.

Wellness is a state of higher positivity that empowers a person to make choices, feel capable, and connected with others (Ryan, 2017). Autonomy, competence, and relatedness enable a person to achieve more and experience greater satisfaction (Ryan, 2017).

The most general characteristic of wellbeing is vitality (Ryan, 2017). Vitality describes the state of feeling energetic and alive (Ryan, 2017). However, vitality is not solely impacted by psychological states, as other factors also contribute to it. Controlled activities dimmish vitality and autonomous activities sustained or enhance vitality (Ryan, 2017). The concept of vitality is akin to the idea of ego-depletion, which suggests that individuals have limited self-regulation or self-control (Ryan, 2017). Nevertheless, SDT (Self-Determination Theory) distinguishes between self-control and self-regulation, whereas the ego-depletion model does not (Ryan, 2017). SDT posits that autonomously motivated activities can decrease or increase vitality, whereas the ego-depletion model only considers the depletion of self-control (Ryan, 2017). The theories concur that controlling motivation depletes the self-control (in the case of the ego-depletion model) or vitality (in SDT) of an individual (Ryan, 2017).

Self-regulation, while less broad than vitality, is a more essential component of SDT (Self-Determination Theory) (Ryan, 2017). However, this aspect of the theory can appear circular. Autonomy support leads to well-being, and one aspect of well-being is self-regulation, which is not entirely differentiated from autonomy (Ryan, 2017). The most significant distinction between autonomy support as a precursor to well-being and autonomy as a feature of well-being is that autonomy support is perceived, while autonomy as a characteristic is described as a state of being (Ryan, 2017). Therefore, it is possible for an individual to perceive autonomy support but not experience autonomy (Ryan, 2017). This becomes complex as research relies on self-reported information to measure both autonomy support and autonomy as a feature of well-being, referred to as self-regulation (Ryan, 2017). The fundamental difference between these perceptions of autonomy is the origin from which it arises (Ryan, 2017). Autonomy support comes from the external environment, while self-regulation, the autonomy an individual feels they possess, comes from within themselves (Ryan, 2017).

Other Psychological Needs

Wellness relates to other theorized psychological needs: meaning, self-esteem, and security (Ryan, 2017). Meaning can be perceived as having a purpose in life or believing that one's life is fulfilling (Ryan, 2017). Achieving a sense of meaning is essential to promoting wellness (Ryan, 2017). SDT considers wellness as an outcome of support for autonomy, competence, and relatedness rather than a basic need (Ryan, 2017). Self-esteem can be regarded as a defensive need arising from a belief or worldview that conflicts with others (Ryan, 2017). Self-esteem must be present to defend beliefs to others and oppose the opposition (Ryan, 2017). SDT considers self-esteem a measure of love, confidence, worthiness, and self-acceptance (Ryan, 2017). Much like how SDT treats meaning, SDT considers self-esteem an outcome of the three basic needs rather than a separate basic need (Ryan, 2017). Security (not cybersecurity) refers to the need to be safe from danger or harm (Ryan, 2017). Concerns for security arise from threats or being thwarted in a way that leaves an individual feeling insecure (Ryan, 2017). However, SDT does not consider security as one of the basic needs (Ryan, 2017).

Wellbeing in Other fields

Studies across disciplines show positive experiences associated with self-determined motivation and autonomously controlled behavior (Deci et al., 1989; Pelletier et al., 1997; Vansteenkiste et al., 2004; Williams et al., 1996). In children, the more the autonomous motivation the higher the enjoyment the child reported (Vansteenkiste et al., 2004). Therapy patients report less tension, more positive moods during therapy, less distraction, greater intentions to continue therapy, and higher levels of satisfaction when they perceived their motivation as self-determined (Pelletier et al., 1997). People trying to lose weight when autonomously motivated attend their weight-loss programs more often, lose more weight, and maintained weight loss more than non-autonomously motivated people on the weight-loss program (Williams et al., 1996). In organizations self-determined motivation predicted greater creativity and conceptual learning, also more positive social tone, and self-esteem (Deci et al., 1989).

Framing

The communication field possess diverse views on framing (Cacciatore et al., 2016; Entman, 1993; D. Scheufele, 1999; D. A. Scheufele & Iyengar, 2014). Framing alters a message to emphasize one aspect of a message over another (Entman, 1993). To frame a message is to alter the communication in order to alter the reception of the message content (Entman, 1993). Framing connects with two other media effects; However, there is not a consensus on the relationship between framing and the other media effects (D. A. Scheufele & Tewksbury, 2007).The first of the other media effects, priming, seeks to alter the reception of a subsequent message. The other media effect, agenda setting, seeks to alter a message to encourage the audience to interpret one aspect or another as the most important (D. A. Scheufele & Tewksbury, 2007).

A first view of framing considers it as second-level agenda setting (Cacciatore et al., 2016; Entman, 1993; D. Scheufele, 1999; D. A. Scheufele & Tewksbury, 2007). There are similarities between agenda setting and framing that can be difficult to distinguish and placing these media effects together simplifies the media effects theoretical framework (Cacciatore et al., 2016; Entman, 1993; D. Scheufele, 1999; D. A. Scheufele & Tewksbury, 2007). Within this view agenda setting tells the audience what to think about among other aspects of the information presented while framing extends this and refers to how the wording and emphasis to tells the audience how to think about the information (Cacciatore et al., 2016; Entman, 1993; D. Scheufele, 1999; D. A. Scheufele & Tewksbury, 2007). If an article possesses agenda setting elements that emphasizes the monetary cost of a war, it might also possess framing that guides the audience to consider the topic of war as an economic issue (Cacciatore et al., 2016; Entman, 1993; D. Scheufele, 1999; D. A. Scheufele & Tewksbury, 2007). The mechanism for this interpretation relies on salience of framing but the distinction between agenda setting, and framing are less clear using this interpretation (D. Scheufele, 1999).

A second view of framing considers agenda-setting and framing as distinct media effects (Cacciatore et al., 2016; Entman, 1993; D. Scheufele, 1999; D. A. Scheufele & Tewksbury, 2007). This view contrasts the mechanism for how framing and agenda setting operate on the mind (Cacciatore et al., 2016; Entman, 1993; D. Scheufele, 1999; D. A. Scheufele & Tewksbury, 2007). Agenda setting functions by increasing the salience or frequency of an idea within a piece of media to increase the importance of that idea for the audience (Cacciatore et al., 2016; Entman, 1993; D.

Scheufele, 1999; D. A. Scheufele & Tewksbury, 2007). Priming presents an idea to the audience prior to the piece of media to alter how the audience will think about it (Cacciatore et al., 2016; Entman, 1993; D. Scheufele, 1999; D. A. Scheufele & Tewksbury, 2007). Priming functions by sequence to alter how the audience interprets a piece of media (Cacciatore et al., 2016; Entman, 1993; D. Scheufele, 1999; D. A. Scheufele & Tewksbury, 2007). Framing operates through cultural reference (Cacciatore et al., 2016; Entman, 1993; B. T. Scheufele & Scheufele, 2009; D. Scheufele, 1999; D. A. Scheufele & Tewksbury, 2007). A piece of media connects to a cluster of ideas that pre-exists within the audience known as a schemata (Cacciatore et al., 2016; Entman, 1993; B. T. Scheufele & Scheufele, 2009; D. Scheufele, 1999; D. A. Scheufele & Tewksbury, 2007). By creating a connection with a schemata within the audience the piece of media guides the audience to think about the topic in a way based upon that schemata (Cacciatore et al., 2016; Entman, 1993; B. T. Scheufele & Scheufele, 2009; D. Scheufele, 1999; D. A. Scheufele & Tewksbury, 2007). This cluster of ideas is a schemata and is culturally constructed and needs to be shared among members of the population to be effective (Cacciatore et al., 2016). By activating this schemata and associating it with the message content behavior may be altered (D. Scheufele, 1999).

A third view of framing uses framing to refer to only a narrow interpretation of losses versus gains in message presentation (Cacciatore et al., 2016; Levin et al., 1998). This view sees framing more as a cognitive bias than as a broad media effect. This view would consider differences in presentation between present an audience with a 20% chance of winning money vs an 80% chance of losing money (Tversky & Kahneman, 1981). The logically equivalent statement produces different resulting behaviors in the audience based upon this narrow alteration of a message (Tversky & Kahneman, 1981).

This study relies on the second view of framing introduced. This view connects how a change in a piece of media can change how a person thinks and therefore how they act.

Why Framing?

A recent study highlighted the need for the study of the cybersecurity behavior field to recognize that people do a lot of quick decision making without careful consideration (Dennis & Minas, 2018; Kahneman, 2011). Framing fits this need. Framing modifies behavior by activating the preexisting schemata people already have without the need for people to carefully consider the action.

Framing in Cybersecurity

The framing literature in cybersecurity supportive behavior look at a variety of frames and behaviors (Barlow et al., 2013; Burns et al., 2019; Chen et al., 2015; Proctor & Chen, 2015). One issue in cybersecurity supportive behavior is neutralization, or the things people tell themselves to reduce guilt for not engaging in behavior they feel they should (Barlow et al., 2013). Framing communications in cybersecurity supportive behavior around nullifying neutralization by people works as effectively as sanctions-oriented communications (Barlow et al., 2013). A loss versus gain approach to framing tested whether highlighting individual-losses, group-losses, individual-gains, or group-gains produced more effective remedial phishing training (Burns et al., 2019). Individual-losses framing showed the most effective results (Burns et al., 2019). Other framing techniques that show effectiveness in cybersecurity supportive behavior include using safety scores or a risk-safety index in mobile app installation decision making (Chen et al., 2015). Framing with social information related to how many of the user's friends used a security feature using a prompt that includes the number of a social media "friends" the user has did not produce differences in the adoption of security features (Das et al., 2014). A study of help desk customers found that even subtle changes in framing such as changing “our” to “your” worked to change if users changed their password or not (A. C. Johnston et al., 2019). In summary the following frames have been studied neutralization, sanction, individual -loss, individual-gain, group-loss, group-gain, using mobile app risk scores, a mobile app safety/risk index, social pressure using number of friends using a feature, and singular versus plural pronouns (Chen et al., 2015, 2015; Das et al., 2014; A. C. Johnston et al., 2019). Framing has been studied in the following behaviors: general security compliance, remedial phishing training, mobile app selections, social media users’ adoption of security features, and password modification by helpdesk customers (Burns et al., 2019; Chen et al., 2015; Das et al., 2014; A. C. Johnston et al., 2019; Proctor & Chen, 2015). There remains a variety of framing devices or preexisting schemata to engage with and many cybersecurity supportive behavior that have not yet been directly addresses through framing.

Appeals, Support, and Framing

This dissertation uses autonomy framing while previous work using SDT in cybersecurity used autonomy appeals. Autonomy appeals persuade users to perform an action or adopt a behavior while maintaining support for the autonomy of the user (Menard et al., 2017). Autonomy support provides choices, demonstrates concern for a user, interest in alternative views, and communicates to the user that it is possible to not comply with suggested actions (Menard et al., 2017). Autonomy framing reconfigures how a user perceives about the material and subject of the communication. The framing alters how the user considers the topic and makes them consider it differently than other framing would (Entman, 1993). Autonomy framing uses word choice and emphasis to give a sense of autonomy regarding the information presented (Entman, 1993). If the user thinks about the topic and connects the feeling of autonomy to it, then that provides autonomy support to the user. Autonomy framing is a form of autonomy support.

Emotion and Cybersecurity

People have reported that cybersecurity supportive behavior slows down their work (Davis, 1989). One study found that people were four time more likely to describe security with negative words than positive ones (Renaud et al., 2021). Negative descriptions of cybersecurity include feelings of anxiety, anger, or feeling overwhelmed (Renaud et al., 2021). Other fields have shown negative views of a topic may interfere with motivation (Perugini & Bagozzi, 2001). Cybersecurity is associated with negative emotions such as guilt, shame, anger, withdrawal, and frustration (Albrechtsen, 2007; McDermott, 2012; Renaud et al., 2021).

Gaps and Needs of the Literature

Autonomy appears to have a positive effect on security compliance intentions or intent to install a password manager in organizational or home contexts (A. Johnston, 2020; Lee, 2015; Menard et al., 2017; Wall et al., 2013). The study by Lee indicates perceived autonomy, perceived competence, and perceived relatedness correlate with compliance intentions in organizational contexts; however, only perceived competence showed significance when explaining the criterion variable (Lee, 2015). Self-efficacy a related but distinct variable has been correlated with cybersecurity supportive behavior and compliance intentions (A. Johnston, 2020; Lee, 2015; Menard et al., 2017; Wall et al., 2013). The Johnston replication study showed only perceived autonomy strongly correlated with installing a password manager (A. Johnston, 2020). These results indicate autonomy support motivates cybersecurity supportive behavior and intentions; However, there has not been a study examining a wellbeing benefit to using autonomy in cybersecurity over controlling language. Furthermore, the experiences of users when they receive autonomy support I cybersecurity have not been described.

The literature indicates that autonomy support is beneficial for cybersecurity compliance efforts. This dissertation critically examines this by exploring if wellbeing is experienced when autonomy support is provided around cybersecurity. This will offer insight into how to support user wellbeing in cybersecurity communications and whether providing autonomy support in cybersecurity is associated with any drawbacks.

Chapter 3: Research Methods

Introduction

This chapter describes the multiple methods used in this dissertation. It first describes my research philosophy, reviews the study questions, and describes my initial expectations for the results. The chapter then describes early work to develop and test my research protocol and instruments. Next it describes the final instruments of data collection including a vignette, CAT documents, scales, and open-ended questions. It continues by describing how I recruited participants and my sampling approach. It then describes the multi-method data collection procedure. It then describes the analysis approaches I took for both the quantitative and the qualitative data. Next, I describe how analysis developed and changed over the time I was doing data collection. I then explain how I determined I reached theoretical saturation and decided to stop collecting data. The chapter ends with a discussion of study quality issues.

My Research Philosophy

This study takes a post-positivist approach to social sciences. Epistemically the viewpoint of this study reflects my own, which is an objectivist perspective (Creswell & Creswell, 2007). This work presumes reality as fixed, and human knowledge of said fixed reality remains limited. The beliefs and thoughts of individuals are relevant phenomena which express meaningful patterns within reality that serve the research enterprise. As a post positivist researcher, I recognize that my biases will play a role in my search for objective truth. To better access the truth, I identify my biases and perspectives to better interpret my data. My experience as technology support has generated a holistic approach to problems of humans and technology. These concerns must prioritize the human while relying on technology as a tool. Understanding and knowledge regarding technology should first and foremost serve the greater interest of helping people. The complicated and layered meaning of technology in society assures that all experiences and understanding of technology is limited, flawed, and personal. As a cybersecurity human factors, I place high value on security practices but understand that stronger cybersecurity relies upon the layered social reality of minds and cultures. Human perception and cultural factors of cybersecurity are the focus of this study.

Subjectivity

It is important for researchers to acknowledge the position they hold in relation to their research topic (Creswell & Creswell, 2007). A large part of my identity will interact with this research and the process of data collection (Creswell & Creswell, 2007). As a technology professional with a stereotypical appearance for the field, I realize I come to the research with an identity of knowledgeability regarding the subject of the research. I made an active effort to welcome honest responses regarding participant views of cybersecurity rather than any expectation of objectively correct responses. One method I employed is to assure participants both before the interview and during the interview that the interview is not a knowledge test and that participants are not expected to be experts. Further still, I built rapport during one of the statements in the vitality scale: "Currently I feel so alive I just want to burst." This statement can sound silly when asked aloud and using this moment to share in the acknowledgement of the way the statement sounds helps build trust with participants.

Motivating Question

As discussed in the literature review section, motivating people to engage in cybersecurity prevents costly cybersecurity incidents. This dissertation seeks to understand how autonomy framing applied to cybersecurity training content impacts how users feel in terms of wellness about cybersecurity and the cybersecurity training. This dissertation investigates wellness perceptions of users because Self-Determination Theory states that autonomy support will lead to wellness.

Research Questions

The dissertation examines two research questions to understand how users experience SDT based communication in cybersecurity.

1. Research Question: What are the autonomy impressions of professionals regarding autonomy-framed cybersecurity training content?

Autonomy is the central component of SDT, and past studies have shown it can predict security behavior (see Literature Review section). Autonomy support is also theorized to lead to better wellness outcomes and has been shown to do so in health, organizational, therapy, and other contexts (see Literature Review section). This study investigates the relationship if users who perceive autonomy will perceive cybersecurity differently when presented with autonomy framed communications.

2. Research Question: What are the wellness impressions of professionals regarding autonomy-framed cybersecurity training content?

According to SDT, autonomy support should lead to wellness. Vitality and self-regulation are established characteristics of wellness and closely related to autonomy. Understanding how participants experience characteristics of wellness will increase understanding of any relationship between user wellness and autonomy framing in the cybersecurity context.

Initial Expectations

The initial expectation of this study was that **when cybersecurity training content is framed with autonomy, then professionals (and future professionals) will report the characteristics of wellness.** As the later results show, the data did not fully support my expectation and **I did not find evidence that framing cybersecurity training content with autonomy produces perceptions of the characteristics of wellness in professionals.**

This case study used analytic induction, where a hypothesis is formulated to explain a phenomenon and then cases are examined (Gomm et al., 2009). In our case study we do not pose a formal hypothesis. Instead, we state our expectations since the investigation is primary qualitative and quantitative elements should be considered as a pilot for future work. Examining cases allows for the refinement of the hypothesis (in our case the expectations) and description of the phenomenon (Gomm et al., 2009). When a case that contradicts the hypothesis is discovered, the hypothesis in its current form is proven wrong and then refined. There is also the possibility that the definition of the phenomenon rather than the hypothesis may be refined to exclude the case (Gomm et al., 2009). Analytic induction produces universal statements rather than correlations.

Development of Research Protocol

To develop my mixed methods research protocol, I conducted 10 semi-structured interviews with preliminary pilot participants (PPP) and developed and tested several questionnaires. During the interviews, I showed participants draft copies of fictionalized cybersecurity awareness training (CAT) materials and asked them to respond to the materials. Furthermore, I began to test structured questionnaires that elicited data about demographics and variables related to Self Determination Theory (SDT), Vitality, and Autonomy. Pilot participants included 4 who identified as male, 5 who identified as female, and 1 who identified as non-binary. 2 participants work as fulltime staff, 3 are masters students, and 5 are doctoral students.

My preliminary interviews focused on the quality of the interview questions and experience of the participant in the research. The interview with preliminary pilot participant (PPP) 1 revealed the significant impact of previous experience with cybersecurity training on questions regarding training. PPP1 related a lot of sentiment related to CAT. This would lead me to include fewer questions about previous CAT experience. The interview with PPP2 similarly showed that information technology experience confounded some of the early piloted questions. PPP2 gave answers that approached the questions from an information technology professional perspective. This interview helped solidify the requirement that participants should not have information technology experience. At this point I restructured some of my questions.PPP3 provided better quality responses that indicated my changes improved the questions and study design. Furthermore, PPP3 gave more insight into what questions prompted responses about the psychology of participants regarding cybersecurity as a general topic.

With PPP4, I used Qualtrics as a platform to present the structured questionnaires to elicit data about the proposed variables of interest. I found the Qualtrics procedure with PPP4 felt awkward. For PPP5, I administered the structured questionnaire with a hybrid interview format where I presented questions via screensharing but also administered them verbally. PPP5 indicated that the length of the training materials felt like overwhelming and repetitive. Based on this, I reduced the training content amount. PPP5 also clearly picked up on the treatment intent and provided answers in line with what might be desired from true study participants.

For PPP6 I delivered all the questionnaire content as a semi-structured interview. The interview responses were unexpected, but the process proceeded without incident. The responses indicate that even when responses do not relate well to SDT, that they provided interesting insight into how users approach CAT and policy. For PPP7 I converted the questionnaire into a PowerPoint presentation to present each question or scale one at a time rather than sharing my screen with a Qualtrics survey pulled up. I presented scale instructions, the vignette instructions, the training document, and initial non-scale questions on slides to PPP7 alongside a verbal delivery of the questions. I refined the question wording based upon feedback received up until that point (PPP1-7) PPP8 indicated a dislike of some of the autonomy framing, so I removed these elements. At this point the vitality scale appeared to not provide meaningful data, so the Self-Regulation in Learning Questionnaire was added. Further, I moved the vignette to before the first administration of the Subjective Vitality Scale and Self-Regulation Questionnaire.

I addition to improving the data collection instruments and procedures, during the pretesting I also improved the autonomy framing of the training content. Interviews with PPP4-PPP6 indicated that many of the aspects of autonomy suggested by the Perceived Autonomy Support Questionnaire were missing from the training document. I improved the document to offer choice and feedback options to the participants. The control document was altered to offer an email address for questions as would be expected from an organizational document. At this point I moved from administering the scales twice to only once after the participants reviewed the training. I presented PPP9 and PPP10 the protocol as described in this document without a pre-test phase. Both interviews proceeded without issue.

Alterations of Pre-existing Questionaries

A major alteration of the existing Perceived Autonomy Support Questionnaire was the alteration of the term ‘manager’ to the term ‘training creator.’ The original questionnaire aims at assessing autonomy support from a manager, so the questions needed to be changed to refer to the term training and training creator. But initial interviews indicated this wording should be further refined to training content and training content author. The pilots further iterated through different fictional workplace departments of cybersecurity in the questions, but some participants seemed to slide into their real-life perspectives of such departments not based upon the training content.

As presentation of the training content moved from Qualtrics to screensharing of pdfs and then into PowerPoint, the term ‘training document’ and ‘training document author’ arose as the most natural way to refer to the training content. This study thus uses the following terms: training document, document, and document author in place of manager in the Perceived Autonomy Support Questionnaire and other questions.

Theory-based Improvements to Pilot Version

Several concerns were raised in the proposal stage of this dissertation and this section describes how these concerns have been addressed. One concern was whether the proposed dissertation project used framing or priming. After review we still believe we are using framing. Priming refers to “changes in the standards that people use to make political evaluations” and framing “refers to modes of presentation that journalists and other communicators use to present information in a way that resonates with existing underlying schemas among their audience” (D. A. Scheufele & Tewksbury, 2007). Put simply, priming determines whether we think about an issue and framing determines how we think about an issue (D. A. Scheufele & Tewksbury, 2007). In this dissertation project we implicitly tell participants to think about cybersecurity. Both groups are primed to think about cybersecurity by receiving a document about cybersecurity. We altered the original non-autonomy document to influence the autonomy group recipients to consider cybersecurity as a domain where they have autonomy. The non-autonomy document presented to the other group does not possess these alterations. Both groups will be primed to think about cybersecurity, but the autonomy document is framed to influence the group to view cybersecurity decisions as belonging to the participants. The non-autonomy group will be presented the same information but are intended to view the information as the decisions of the organization that the participant should follow.

Another concern regarding the dissertation project as proposed was that the alterations to the autonomy document might not create an appreciable effect between the groups. This concern is valid and as such I made alterations to the autonomy framed document to increase the strength of the framing.

The key theme of the alterations to the autonomy document concerns responsibility. Responsibility connects both with our definition of autonomy and framing. Shanto Iyenegar explains that framing defines a problem and can attribute who is responsible for the problem (Iyengar, 1994). Responsibility is key to social knowledge and treatment responsibility establishes who can resolve the problem (Iyengar, 1994). Attribution of who is responsible changes the way a message is interpreted and how a problem is perceived (Iyengar, 1994). For example, Nancy Pelosi, a liberal, may blame social conditions for the struggles impoverished people endure while Greg Abbot, a conservative, may consider the struggles of impoverished people to be the fault of people being lazy and not wanting to work hard. This may manifest in the language these politicians use. Nancy Pelosi may refer to impoverished people as “the less fortunate” because that makes them more sympathetic whereas Greg Abbot may refer to them as “people on welfare” because that casts them as people living off the government.

Connecting back to the dissertation project, the autonomy framed document establishes that there is a problem – that unauthorized and criminal access and use of networks, devices, and data occurs. The responsibility for solving the problem is originally not addressed in the non-autonomy document and thus it is left to the reader to interpret. We altered the autonomy document to include the following: “Cybersecurity relies on the decisions you make every day. You contribute to the cybersecurity of our organization, and your choices make a difference.” These extra sentences establish that the responsibility for resolving the problem of cybersecurity as one that belongs to the recipient of the document. We take this change in narrative in the framing a step further by altering the autonomy document title to “Knowing About Cybersecurity Lets You Do Cybersecurity Your Way” from “What is your role in Cybersecurity?” We also altered a sentence to include the following: “consider how you support the cybersecurity of the organization.” To accommodate these changes, we replace the wording of the autonomy document that the pilot participants noted as not coming across positively including that reference to how scary cybersecurity can be.

I believe these changes improve the quality of the study. I anticipated that participants in the non-autonomy group will attribute less responsibility to themselves than the autonomy group will. I expected this should play a significant role in generating autonomy in the participants who receive the autonomy frames.

The pretesting, alterations of pre-existing questionaries, and theory-based changed resulted in the final research protocol, interview questions and structured questionnaires described in the next section.

Instruments for Data Collection

This section introduces the participant demographic survey, the Subjective Vitality Scale, the Learning Self-Regulation Questionnaire, and the Perceived Autonomy Support Questionnaire – Work Climate Questionnaire.

Participant Demographic Information

A demographic poll was conducted prior to the interviews. The questions included in this survey are included in Table 1: Demographic Questionnaire.

Question	Possible responses
What is your Gender?	Male, Female, Other with free response
What is your Age?	Under 18, 18-24, 25-34, 35-44,45-54,55-64,65-74, 75-84, 85 and older
Are you of Hispanic, Latino, or Spanish origin?	Yes, No
How would you describe yourself? Please select all that apply.	White, Black or African American, American Indian or Alaskan Native, Asian, Native Hawaiian or Pacific Islander, Other
What is the highest degree or level of school you have completed?	Less than a high school diploma, High school degree or equivalent (e.g., GED), Some college, no degree, associate degree (e.g., AA, AS), bachelor’s degree (e.g., BA, BS), master's degree (e.g., MA, MS, MEd), doctorate or professional degree (e.g., MD, DDS, PhD)
What is your marital status?	Single (never married), Married, or in a domestic partnership, Widowed, Divorced, Separated
What is your current employment status?	Employed full time (40 or more hours per week), Employed part time (up to 39 hours per week), Unemployed and currently looking for work, Unemployed not currently looking for work, Student, Retired, Homemaker, Self-employed, Unable to work

Table 1: Demographic Questionnaire

Subjective Vitality Scale

This dissertation operationalized wellness using vitality, a characteristic of well-being, and it measured vitality with the Subjective Vitality Scale (*Metrics & Methods*, 2021). Previous researchers have verified the validity of the subject vitality scale to measure the state vitality of a subject (Bostic et al., 2000). The vitality of an individual refers to the current state of being of a person at a moment in time (*Metrics & Methods*, 2021). While this study does not seek to show statistical significance, the scores of the Subjective Vitality Scale are calculated and reported in the results section. This scale has been used to evaluate the level of vitality and wellbeing in various fields and in this study the scale will be used to measure the level of vitality participants experience after reviewing the training document.

Administration

Participants were asked to indicate their agreement with statements about their perception of the training content on a scale from 1 – 7. 1 indicates the statement is not true at all, while 7 indicates the statement is very true. For the complete scale see the appendix. The following are examples of statements presented to participants:

1. At this moment, I feel alive and vital
2. I am looking forward to each new day

Scoring

There are two ways to score using the Subjective Vitality Scale (*Metrics & Methods*, 2021). The six-item scoring method omits the response to the statement “I don't feel very energetic right now” and averages the remaining scores. The seven-item scoring methods reverses the scoring of “I don't feel very energetic right now” and averages the reverse score with the other items. This dissertation utilizes the seven-item scoring method since it includes an additional statement and more data.

Learning Self-Regulation Questionnaire

This dissertation operationalized wellness using self-regulation, a characteristic of well-being. It measured self-regulation with a modified Learning Self-Regulation Questionnaire (SRQ-L) (*Metrics & Methods*, 2021). The self-regulation of an individual represents the level of self-determined vs. controlled functioning (*Metrics & Methods*, 2021). While my study does not seek to show statistical significance using the scores of the modified Learning Self-Regulation Questionnaire; I report the scores in the results section. This scale has been used to evaluate the level of self-regulation in learning environments and in this study the scale will be used to measure the level of self-regulation participants experience after reviewing the training document.

Administration

Participants were asked to indicate their agreement with statements about their perception of the training content on a scale from 1 – 7. One indicates the statement is not true at all, while 7 indicates the statement is very true. For the complete scale see the appendix. The following are examples of statements presented to participants:

1. I will participate actively in the Cybersecurity Training because I feel like it's a good way to improve my skills and my understanding of cybersecurity.
2. I am likely to follow the cybersecurity training’s suggestions for cybersecurity because I will get a reward if I do what the cybersecurity training suggests.

Scoring

The SRQ-L scale produces two subscales: an autonomous regulation score and a controlled regulation score. The controlled regulation score measures both introjected and external regulation and the autonomous regulation score measures identified and integrated regulation (*Metrics & Methods*, 2021).

Items 1, 3, 6, 9, 11, 13, and 14 are averaged for the autonomous regulation score. Items 2, 4, 5, 7, 8 ,10, and 12 are averaged for a controlled regulation score (*Metrics & Methods*, 2021). A relative autonomy index is calculated by subtracting the controlled score from the autonomous score (*Metrics & Methods*, 2021). The modified Learning Self-Regulation Questionnaire was be administered during stage 2 and included follow-up questions such as "Why did you choose X score?"

Perceived Autonomy Support Questionnaire – Work Climate Questionnaire (PAS).

To explore the effectiveness of the autonomy framing, this dissertation used a modified Perceived Autonomy Support Questionnaire – Work Climate Questionnaire (PAS) (*Metrics & Methods*, 2021). While the study does not seek to show statistical significance, I report the scores in the results section. The researcher made some changes to PAS options, specifically changing the role of a manager to the role of the training as described in the development section. This scale has been used to evaluate the level of perceived autonomy support from managers in work environments and in this study the scale was used to measure the level of autonomy support the participants experience from the training document.

Administration

Participants are asked to indicate their agreement with statements about their perception of the training content on a scale from 1 – 7. One indicates strong disagreement, while 7 indicates strong agreement. For the complete scale see the appendix. The following are examples of statements presented to participants:

1) I feel that the document provides me choices and options

2) I feel understood by the document

Scoring

The PAS is scored by averaging the scores of each response other than the response to “I don't feel very good about the way the document creator talks to me.” The response to “I don't feel very good about the way the document creator talks to me” should be reverse scored before averaging with the other questionnaire items (*Metrics & Methods*, 2021). The higher a score the higher the perceived autonomy support. This questionnaire appeared in stage 2 of the interview. Interview transcripts include answers to question scale items and follow-up questions such as “Why did you choose X score?”

CAT Training Documents and Vignette

Interview data collection took place using a vignette to establish a scenario for participants to approach the training from. The vignette is as follows:

“For the following sections, please imagine the following situation: You are an employee of Alpha Corporation and are provided with cybersecurity training. Alpha Corporation also includes links throughout the training to additional information which are not included here. The following is the training content Alpha Corporation provides you with:”

The autonomy group received the CAT documents with autonomy framing, while the non-autonomy group received unaltered training material from the Cybersecurity Infrastructure and Security Agency. This material was selected because it comes from a government agency, includes general cybersecurity information, and is presented tersely. The study altered the autonomy group training content to replace fear and control elements with autonomy framing (see the Non-Autonomy Framing and Autonomy Framing Sections). The non-autonomy framed version represents current messaging in the field -- not intentional fear or control framing. Each CAT document was approximately 1 page long.

Open-Ended Questions

This next section describes the open-ended interview questions that guided the interviews with the participants. The interview questions were asked after the participants reviewed their assigned CAT training document (i.e., autonomy-framed vs. non-autonomy-framed). The open-ended questions checked the effectiveness of the framing in the autonomy-framed document, gathered data on the positive or negative feelings participants experienced related to the documents, and allowed the participants to examine both documents to identify elements that impacted them. The interview questions were as follows.

1. Based on the document, why should you learn about cybersecurity?
2. After reading this document, do you feel any different about the topic of cybersecurity?
3. How does the document make you feel?
4. Based on this training, who decides whether you adopt these best practices?
5. Which of these versions of the training do you prefer and why?
6. Employers want you to engage in better cybersecurity practice. Would you rather be threatened that you will be fired for noncompliance or motivated in a gentler way and why?

Recruitment of Participants and Sampling

This study recruited participants via email advertisements and posted flyers at several locations. Participants were active or future professionals with limited information technology expertise. I refer to these as “professionals” in this chapter. Participants were disqualified for previous professional work in the information technology field or cybersecurity field. Participants could be currently employed professionals or professional program graduate students that are soon to be professionals within two years of seeking professional employment.

I used convenience samples of professionals due to the difficulty in securing a random sample. I presumed difficulty in getting participation from professionals due to the significant demands on the time of a professional. Early in the study, I identified that most participants recruited identified as female. To counteract this later recruitment focused on getting more male participants through criterion sampling. I did not reject female volunteers, but I began pursuing male volunteers by advertising in locations that more males would be likely to see them. I eventually reached 25% male to 75% female up from a low of 7% male and 93% female.

I assigned each participant a pseudo-random number using an online tool to represent their group assignment. Odd numbers were assigned to receive non-autonomy framing and even numbers received autonomy framing.

Interviews ceased once the data reached theoretical saturation (Creswell & Creswell, 2007). Participant responses to the open-ended questions began to repeat and be predictable. Each participant reported similar experiences. The rough themes appeared around the 8th interview and additional interviews only refined the results. I reached theoretical saturation with 15 interviews completed and an additional 5 interviews were completed to add more data for the results (Creswell & Creswell, 2007).

Data Collection Procedure

Once a participant was recruited, data collection proceeded in 4 stages: Stage 1: The greeting stage, Stage 2: the document review and structured questionnaires, Stage 3: the open-ended questions, and stage 4: parting stage. Based on pre-testing, all stages could be completed in one participant sessions of approximately 45 minutes. Prior to the interview sessions I provided the participants with an online form to collect demographic information.

Stage 1: Greeting

During stage 1, I introduced myself, and supplied the IRB consent form for their review and consent.

Stage 2: The Document Review and Structured Questionnaires

During Stage 2, I presented participants with the vignette, the cybersecurity training content, and scale-based questions.

Prior to the training content a short vignette was presented to contextualize the training. Next, I ask the participants to review a training document. Stage 2 differs slightly for those assigned to the autonomy or non-autonomy group. The autonomy group received the training documents with autonomy framing, while the non-autonomy group received unaltered training material from the Cybersecurity Infrastructure and Security Agency.

Next, I orally administered a series of structured questions from the Subjective Vitality Scale, the Learning Self-Regulation Questionnaire, and Perceived Autonomy Support Questionnaire. Scale-based questions were administered verbally to participants. Reviewing the cybersecurity training document and completing the scale-based questions took from 5-12 minutes.

Stage 3. Open Ended Questions

During stage 3, I asked opened ended questions developed during the pilot phase of this project. This study used a semi-structured interview to gain deeper insight into how participants view the autonomy framing in this study (Braun & Clarke, 2012). The interviews were audio recorded and recording was kept in a secure location. The second to last question of this section asked participants to compare the two versions of the training document to identify preferences and perceptions based upon the two versions.

Stage 4: Departing Stage

During stage 4, I thanked the participant, offered to answer any questions they had about the project or about cybersecurity, and provided the participant with a small token of appreciation.

Additional Data Collection

I believed I had reached theoretical saturation with the professionals who use computers often, but I was curious about professional workers who use computers less frequently. So, I attempted to recruit people who don't use computers in their daily work to see if the results might be different. Unfortunately, recruitment efforts were not successful. Given limited time, I decided to confirm my draft findings with 5 more future professional interviews.

Analysis Approaches

Analysis of quantitative data employed descriptive statistics. Analysis of qualitative data included both deductive and inductive approaches.

Analysis Procedure-Quantitative Data

Each of the scales used in this study produced a score. These scores were recorded, and I report descriptive statistics including mean, and standard deviation for both the autonomy-framed group and the non-autonomy framed group. I also present and describe the differences between the descriptive statistics of the treatment or control groups in tabular form (Huberman & Miles, 2002). This presentation will report of the data without relying on statistical significance (Huberman & Miles, 2002).

Analysis Procedure-Qualitative Data: Deductive coding and Expectation Testing codes

Interviews were audio recorded and transcribed. I used the Nvivo analysis software to assist with coding and memoing.

In addition to more open coding described below, I used expectation codes to indicate interview portions specifically related to my expectation that participants using autonomy framed materials will experience higher levels of autonomy and well-being (Saldana, 2015). This allowed me to more easily find data that supported or refuted my expectation.

First, I deductively applied codes derived from SDT concepts of autonomy, and wellbeing. Using the definitions of these concepts, I read through the interview transcripts searching for similar meaning among participant responses. When I identified a statement that resembles an SDT concept, I applied the codes therefore, I coded parts of the interview as being a reference to autonomy or wellness.

Inductive Coding: Thematic Analysis

With deductive SDT codes completed I began a second round of coding using thematic analysis based upon patterns detected during the analysis process. Thematic analysis allowed me to analyze an interview for themes (Braun & Clarke, 2012). Such codes might be related to emotional states, preferences in training content, as well as other emergent patterns.

To conduct thematic analysis I read through the interview transcripts first (Braun & Clarke, 2012). Then subsequently, I ascribed codes to sections of text that described patterns I saw in the data (Braun & Clarke, 2012). The coding process was iterative in that codes were refined and recoded as further work was done (Braun & Clarke, 2012). I next used the coded sections to generate themes (Braun & Clarke, 2012). The themes needed to be broad enough to encompass the accounts of multiple participants, yet specific enough to yield interesting findings (Braun & Clarke, 2012). Themes also had to be limited in number to produce a story and they needed to not be based upon the interview questions (Braun & Clarke, 2012). I refined and iteratively improved the codes until they were of sufficient quality to report (Braun & Clarke, 2012). I also separated the transcripts from the two groups and analyzed them separately to detect any differences that might have appeared between the groups.

In line with the perspective that qualitative research reveals unique perspectives and social realties, this dissertation uses only a single coder. Relying on a single coder aligns with the notion that the interview process and active personal engagement with participants is a resource for understanding (O'Connor & Joffe, 2020). Additional coders would not be able to draw from the experiences of the interview to facilitate understanding of participant expressions.

Once coding was complete, I began to group the transcript data around the codes and analyzing the details within code. For instance, if I viewed all transcript lines coded as autonomy, I looked for patterns in how the autonomy presented itself and what the participants were trying to communicate. Once coding reached a level where I believed no more insight could be gained through additional codes, I began construction of larger themes. Using these themes, I produced the themes and insights from the study.

To look for differences between the groups I put the data side by side and compared the two data sets for similarities and differences. I compared codes and themes from both expectation and inductively derived codes between the groups.

The Data Collection and Analysis Timeline

Upon interviewing the first five participants in September and October of 2022, I began the coding process. The first stage of coding began with establishing the deductive codes for 'autonomy' and 'well-being.' Other initial codes I created at this stage included codes for 'preference for the autonomy version' and 'preference for the non-autonomy version.' These codes were used to indicate parts of the transcript that illustrated the preferences of the participants for one of the two versions of the training document. Codes were also used for tracking whether a participant received the autonomy or non-autonomy version of the training as well as the scores of the three scales administered.

As I proceeded to review additional interviews and code for the initial codes in early November 2022, I developed more inductive codes as I read each transcript. Prominent ideas that stood out from my memory of the interviews and in the text of the transcripts were assigned new codes. Codes I developed and coded for are listed and described in Table 2: Codes.

As more interviews were conducted and transcribed, they were coded with the codes developed through the initial rounds of coding. Interviews 6 through 15 were coded from mid-November to late December. All transcripts, including the initial 5, were coded a second time for thorough analysis. This round of coding generated additional codes listed in Table 2 as secondary codes. Some instances of a code were uncoded if upon re-reading the transcript the code appeared to have been erroneous.

Memos were developed in December 2022 based upon initial codes were written. These memos are described in Table 3: Memos. The memos assisted in the development of the codes into eventual themes of the dissertation. Theme codes were developed for another round of coding in early January 2023. The relationships and development of the codes and memos are described in Figure 2: Code, Memo, and Theme Hierarchical Relationships and Theme Development in the appendix. Five more confirmatory interviews were conducted in late January. These 5 interviews were then coded with the theme codes in late January through early February 2023.

Code	Type of Code	Description
Autonomy	Initial	Participants express attitudes or feelings that appear to be autonomy
Wellbeing	Initial	Participants express feelings or needs related to their wellbeing
Formality	Initial	Participants express a desire or preference for formal communication or a dislike for a part of the training document because it is not formal enough
Condescending	Initial	Participants express the training document sounds condescending or like it is talking down to them.
Relatedness	Initial	Participants express a feeling of connection to the author of the training document or the organization. Participants express a desire for more personal or softer communication
Positive Feelings	Initial	Participants express positive feelings about some aspect of the cybersecurity training document
Negative Feelings	Initial	Participants express negative feelings about some aspect of the cybersecurity training document
I've Seen This Before	Initial	Participants express that they have seen the content of the cybersecurity training document before
Desire for more info	Initial	Participants express a desire or need for more information.
Practical Matters	Initial	Participants express that the cybersecurity training document doesn't support the practical concerns of employees. Participants express a practical concern such as time, difficulty, or how realistic adopting a security best practice is in the day-to-day work routine.
Personal Responsibility	Initial	Participants expressed they feel they are personally responsible for implementing cybersecurity best practices
Different Strokes	Initial	Participants expressed that they recognized other people might want different things from their cybersecurity training. Participants expressed their preferences as an aspect of their personality rather than a universal thing to do.
Insincere	Initial	Participants express that the cybersecurity training document sounded insincere. Participants expressed a lack of genuineness by the author of the cybersecurity training document.
Brevity	Initial	Participants express that the cybersecurity training document was too long.

Lack of Commitment	Initial	Participants expressed they or others are not committed to cybersecurity or will not follow through with their intention to adopt cybersecurity best practices.
Dislike threats	Initial	Participants expressed that they disliked threats or other negative extrinsic motivation.
Disconnected	Initial	Participants expressed feelings of disconnectedness
Pro-enforcement	Initial	Participants expressed positive feelings for extrinsic motivation, compliance efforts, and organizations using their authority to force the adoption of cybersecurity best practices
It’s a mandate	Initial	Participants acknowledged that cybersecurity is mandated by their employer
Needs for Cyber	Secondary	Participants expressed something that wanted cybersecurity to do such as provide more context or treat them like a human.
Wellness needs	Secondary	A code that overlapped with Needs for Cyber and was redundant.
Clarity	Secondary	Participants expressed that the language of the cybersecurity training document was unclear or confusing.
Deference to Org	Secondary	Participants expressed that they would do what the organization wanted or that the needs or desires of the organization were understood.
Familiarity is Bad	Secondary	Participants expressed familiarity with the cybersecurity training document content was not ideal. These are expressions of negative impressions related to familiar content.
Familiarity = Neutral	Secondary	Descriptions of Familiarity with cybersecurity training content being a neutral experience. These are expression that are not positive nor negative.
Auto Lang = more choices	Secondary	Participants expressed that autonomy language made them feel as if they had more choices or options in their cybersecurity behavior.
Like a Person	Theme	Participants expressed a desire to be treated like a person by a cybersecurity training document or communication.
Context	Theme	Participants expressed they want more context or information from a cybersecurity training document or communication.

Extrinsic Motivation	Theme	Participants expressed an opinion on negative extrinsic motivation. There are 3 subcodes: extrinsic is necessary, implied, and threats-less comply. Extrinsic is necessary is coded when extrinsic motivation is mentioned positively. Implied is coded when a participant implies or states that an employer will punish noncompliance. Threats-less comply is coded when negative extrinsic motivation is mentioned as demotivating, bad, or causing negative feelings.
Recognize others' preferences	Theme	Participants expressed that they recognized other people might want different things from their cybersecurity training. Participants expressed their preferences as an aspect of their personality rather than a universal thing to do.
Personal responsibility	Theme	Participants express that they are personally responsible for cybersecurity. One subcode: still a mandate is coded when a participant expressed both personal responsibility and that the employer is mandating the behavior.
Familiar with content	Theme	Participants express familiarity with content. One subcode: Familiarity increases confidence is coded when the participant expressed their familiarity with the cybersecurity training content makes them feel more confidence in their cybersecurity abilities.
Autonomy Language	Theme	Participants expressed an opinion related to autonomy language. There are two sub codes: 'Auto Lang=positive' which is coded for positive perceptions of autonomy language and 'Auto Lang is Bad for cybersecurity' which is coded when negative perceptions of autonomy language are expressed.

Table 2: Codes

Memo Short Name	Memo Topic	Main Ideas of the Memo
Familiarity	Familiarity With the Content and A Need for More Information	Participants in this study indicated both a familiarity with the content of the cybersecurity training and a desire for more information on the content.
Pro-Enforcement	Pro-enforcement – some desire extrinsic motivation even if its punishment/threats	A subset of participants indicated they preferred extrinsic motivation, specifically threats of employee termination or other repercussions. Other ‘pro-enforcement’ attitudes surfaced in participant responses that included attribution of responsibility for these kinds of decisions to the organization, a tendency to give the organization the benefit of the doubt, and a sense that repercussions for noncompliance are understood to exist without their explicit mention.
Personal Preference	Those who prefer the autonomy-wellness supporting elements recognize that not everyone is that way – not reported by those	Participants with autonomy preferences expressed an understanding that not everyone wants to see caring language. Participants who prefer the autonomy cybersecurity training document recognize this as a personal preference

	that prefer the unmodified version.	
Autonomy	Participants expressed a variety of expressions about autonomy and autonomy support.	Participants expressed they didn't like autonomy support, autonomy support was not commanding, autonomy support was a suggestion not an instruction, the power the autonomy support seemed to project on them meant they felt more responsibility for cybersecurity, autonomy support didn't make them feel guilt for noncompliance, autonomy support appeared more conversational, autonomy support gave them the option whether to comply, autonomy support was empowering, and that autonomy was more motivating.
Personal Responsibility	Autonomy – personal responsibility – no matter if the document says so or not -they sense it is a mandate from the source but know it is up to them.	Participants express they feel autonomy as personal responsibility in cybersecurity but that employers are mandating their compliance.

Better Support	Better Support from Cybersecurity	Participants expressed that cybersecurity compliance and training efforts could better support their wellness by providing additional context and treating them ‘like human beings’

Table 3: Memos

Theoretical Saturation

I stopped interviews once the data reached theoretical saturation (Creswell & Creswell, 2007). At this point I found that major themes of perceptions repeated in the interviews, and I did not find new or unique themes (Creswell & Creswell, 2007).

Study Quality Issues

External Validity: The laboratory nature of the research limits some aspects. The study's cybersecurity training does not carry the weight of a real organizational required training. The impressions of the laboratory training may not reflect the impressions the participant might experience in everyday life.

Internal validity: To maintain internal validity, I only modified autonomy word choices and emphasis between the two training versions.

Construct validity: This dissertation explores the relationship between wellness and autonomy framing of cybersecurity messages. This study measured wellness using two of its characteristics identified in SDT: vitality and self-regulation. These measures are well used within the literature and by the authors of SDT (Ryan, 2017). These characteristics of wellness do not fully explain wellness thus some aspects of experience may not appear in the transcripts. The scales and questionaries similarly do not provide completely reliable information. These scales may miss some important aspects of experience in cybersecurity with autonomy and are not substitutes for the open-ended components of this study.

Objectivity: I strived to be open to all information gained from this study whether it supported or refuted my expectations. Early pilot participants reported several unexpected perspectives on the pilot training they received (see research design development section). Each additional perspective, no matter how unrelated to SDT and my initial expectations, furthers the development of better cybersecurity communication knowledge.

I implemented this study consistently by asking the questions the same way during each interview. I did not arbitrarily deviate from the established procedure. Ten pilot interviews contributed to the development of the procedures and questions for this study. I removed the ineffective components of the procedure during the piloting process. I treated each person as identically as possible through every stage of the interview to prevent biasing the study. But, as each person will experience my treatment through the lens of their own experiences, I did not expect identical reactions from participants. Each additional participant or repeated version of this study produces additional information upon which to refine understandings and extend knowledge.

Hawthorne Effect: Asking for detailed descriptions via interview may have promoted participants to respond in ways more rational and detailed than they would experience naturally. This could have resulted in idealized descriptions of their perceptions and thinking. Participants might have sought to please the interviewer, make themselves sound better, or value signal. To combat this, I encouraged honestly and made it clear that it was ok to have no opinion or not know how to answer.

Wording of questions inevitable changed slightly from interview to interview. I followed each question that did not produce much insight with follow up clarifications or prompts. One instance of this that worked well during piloting is following up the questions: “Based on this training, who decides whether you adopt these best practices?” with the follow up “how does that make you feel?” This may seem repetitive since the prior question asks about the feelings the document produces this question uncovers more about the preferences around autonomy framing and controlling language. I rephrased questions and statements as needed to communicate the information needing to be conveyed to the participants without biasing their responses.

This study used several scales used previously with SDT to maintain construct validity. The Subject Vitality Scale was validated to measure vitality (Ryan & Frederick, 1997). The Perceived Autonomy Support: Climate Questionnaire and the Self-Regulation Questionnaire, and the Subject Vitality Scale are designed for use with the theoretical constructs in SDT. In conjunction with the scale-based questions, the open-ended questions will provide me with good insight into the impressions of participants of CAT and autonomy framing.

Chapter 5: Results

Introduction

This chapter presents the results of the interviews with minimal discussion and includes summative demographic information collected, summative results of the Subjective Vitality Scale, summative results of the Learning Self-Regulation Questionnaire, summative results of the Perceived Autonomy Support Questionnaire – Work Climate Questionnaire, the results of thematic analysis, and the results of deductive analysis. Deductive and thematic analysis results shall be presented together.

Participant Demographic Information

A demographic poll was conducted prior to the interviews. The results of the demographic survey along with group membership are available in Table 6: Demographic Results. Twenty participants were interviewed. Participation was 75% female and 25% male. 45% of participants indicated their employment as students, 30% indicated they were employed part-time or less, and 25% indicated they were employed full-time. 40% of participants indicated they highest degree of education was a bachelor's degree, 25% completed some college, 15% completed a master's degree, 10% completed a high school degree, and 10% completed a doctorate degree. 75% of participants identified themselves as white, 20% of participants identified themselves as Asian, and 5% of participants identified themselves as black or African American. None of the participants identified themselves as being of Hispanic origin. 45% of participants were between 18-24 years old. 30% of participants were between 25-34 years old. 15% of participants were between 35-44 years old. 5% of participants were between 45-54 years old. 5% of participants were between 55-64 years old. 75% of participants indicated they were single and never married while 25% indicated they were currently married or in a domestic partnership.

Pseudonym	Group	Gender	Age	Ethnicity	Education Level	Employment Status
Abby	Autonomy	Female	18 - 24	White	Bachelor's degree	Student
Barbara	Autonomy	Female	25 - 34	Asian	Bachelor's degree	Student
Chloe	Non-Autonomy	Female	45 - 54	White	Bachelor's degree	Employed full time
David	Autonomy	Male	25 - 34	White	Bachelor's degree	Employed part time
Emma	Autonomy	Female	18 - 24	White	High school degree	Student
Grace	Autonomy	Female	55 - 64	White	Bachelor's degree	Employed full time
Hope	Autonomy	Female	18 - 24	Asian	High school degree	Student
John	Non-Autonomy	Male	25 - 34	White	Bachelor's degree	Employed part time
Kate	Non-Autonomy	Female	35 - 44	White	Doctorate Degree	Employed full time
Lita	Non-Autonomy	Female	18 - 24	White	Some college	Student
Michelle	Non-Autonomy	Female	35 - 44	White	Doctorate Degree	Employed full time
Nicole	Non-Autonomy	Female	18 - 24	White	Some college	Employed part time
Olivia*	Non-Autonomy	Female	35 - 44	White	Master's degree	Employed full time
Paul	Autonomy	Male	18 - 24	Asian	Bachelor's degree	Student
Quintin	Non-Autonomy	Male	25 - 34	White	Some college	Student
Rei	Non-Autonomy	Female	18 - 24	White	Some college	Student
Sarah	Non-Autonomy	Female	25 - 34	White	Master's degree	Employed part time

Trista	Autonomy	Female	25 - 34	Black or African American	Master's degree	Employed part time
Vanessa	Non-Autonomy	Female	18-24	White	Some college	Employed part time
Xander	Non-Autonomy	Male	18 - 24	Asian	Bachelor's degree	Student

Table 4: Demographic Results

*Participant Olivia was interviewed but is excluded from the results. See appendix notes for details.

Subjective Vitality Scale Results

SDT considers vitality a part of wellbeing and the Subjective Vitality Scale measures participant vitality. This dissertation uses this scale to compare participant vitality between the autonomy and non-autonomy group to see if modifications to the autonomy training document alter participant reported vitality. The results of the Subjective Vitality Scale are summarized below in Table 7: Subjective Vitality Results. For each scale item, and the vitality score a mean was calculated for the complete participant group, the control group, and the autonomy group. There were no appreciable differences between the groups. See Appendix for Statistical test.

Scale Item	All Participants Mean(Standard Deviation)	Non-Autonomy Group	Autonomy Group
1. At this moment, I feel alive and vital	5.68 (1.63)	5.73 (1.19)	5.63 (2.2)
2. I don't feel very energetic right now	2.9 (1.91)	3.55 (2.07)	2 (1.31)
3. Currently I feel so alive I just want to burst	3.11 (1.24)	2.55 (0.82)	3.88 (1.36)
4. At this time, I have energy and spirit	4.84 (1.54)	4.55 (1.69)	5.25 (1.28)
5. I am looking forward to each new day	5.79 (1.18)	5.45 (1.13)	6.25 (1.16)
6. At this moment, I feel alert and awake	6 (1.11)	6 (0.89)	6 (1.41)
7. I feel energized right now	5.42 (1.35)	5.09 (1.45)	5.88 (1.13)
Vitality Score	5.14 (1.05)	4.83 (1.16)	5.55 (0.88)

Table 5:Subjective Vitality Results

Learning Self-Regulation Questionnaire Results

SDT considers self-regulation a part of wellbeing and the Learning Self-Regulation Questionnaire measures participant self-regulation in relation to the cybersecurity training document. This dissertation uses this scale to compare participant self-regulation levels between the autonomy and non-autonomy group to see if modifications to the autonomy training document alter participant self-regulation levels. The results of the Self-Regulation Questionnaire are summarized below in Table 8: Self-Regulation Results and Table 9: Regulation Subscales and Self-Regulation Index. For each scale item, subscale, and the index score a mean was calculated for the complete participant group, the control group, and the autonomy group. The Self-Regulation autonomous subscale mean for the non-autonomy group is 5.03 and the autonomy group mean is 5.35. There is no significant difference between the groups for the autonomous subscale. The Self-Regulation controlled subscale mean for the non-autonomy group is 4.4 and the mean for the autonomy group was 3.3. The controlled subscale narrowly missed the significance threshold of .05 with a p value of .051. The Self-Regulation Relative index mean for the non-autonomy group is .63 while the autonomy group index mean was 2.01. The p value of .03 is suggestive of significance in the difference between the self-regulation indices of the groups; However, given the small sample size a repeat of this measurement with a larger group is recommended. See Appendix for more details on Statistical tests.

Scale Item	All Participants Mean(Standard Deviation)	Non-Autonomy Group	Autonomy Group
I will participate actively in the Cybersecurity Training Because I feel like it's a good way to improve my skills and my understanding of cybersecurity.	5.47 (1.47)	4.91 (1.58)	6.25 (0.89)
I will participate actively in the Cybersecurity Training Because others would think badly of me if I didn't.	3.47 (2.22)	3.91 (1.87)	2.88 (2.64)
I will participate actively in the Cybersecurity Training Because learning to protecting against cyberthreats is an important part of being a professional.	6.05 (1.13)	6.09 (0.94)	6 (1.41)
I will participate actively in the Cybersecurity Training Because I would feel bad about myself if I didn't read this information.	4 (2)	4.45 (1.81)	3.38 (2.2)
I am likely to follow the cybersecurity training's suggestions for cybersecurity Because I will get a reward if I do what the cybersecurity training suggests.	2.79 (1.81)	3.27 (1.85)	2.13 (1.64)
I am likely to follow the cybersecurity training's suggestions for cybersecurity Because I believe the	6.37 (1.01)	6.09 (1.22)	6.75 (0.46)

cybersecurity training’s suggestions will help me protect against cyberthreats.			
I am likely to follow the cybersecurity training’s suggestions for cybersecurity Because I want others to think that I have good cybersecurity habits.	4.11 (2.18)	4.45 (1.86)	3.63 (2.62)
I am likely to follow the cybersecurity training’s suggestions for cybersecurity Because it's easier to do what I'm told than to think about it.	3.74 (1.94)	4.09 (2.3)	3.25 (1.28)
I am likely to follow the cybersecurity training’s suggestions for cybersecurity Because it's important to me to do well at this.	4.9 (1.45)	5.18 (1.54)	4.5 (1.31)
I am likely to follow the cybersecurity training’s suggestions for cybersecurity Because I would probably feel guilty if I didn't comply with the cybersecurity training’s suggestions	4.58 (2.24)	5.18 (1.89)	3.75 (2.55)
Because it's exciting to try new ways to protect against cyberthreats.	3.9 (1.76)	3.91 (1.64)	3.88 (2.03)
Because I would feel proud if I did continue to improve my cybersecurity skills.	5 (1.49)	5.45 (1.04)	4.38 (1.85)
Because it's a challenge to really understand how to protect against cyberthreats.	4.89 (1.6)	4.82 (1.25)	5 (2.16)
Because it’s interesting	4.32 (2.03)	4.36 (1.86)	4.25 (2.38)

Table 6: Self-Regulation Results

Scales	Mean all Participants	Mean Non-Autonomy Group	Mean Autonomy Group
Autonomous Regulation Subscale	5.17 (1.06)	5.03 (1.05)	5.35 (1.19)
Controlled Regulation Subscale	3.96 (1.16)	4.4 (1.01)	3.34 (1.11)
Relative Self-Regulation Index	1.21 (1.35)	0.63 (1.11)	2.01 (1.33)

Table 7: Regulation Subscales and Self-Regulation Index

Perceived Autonomy Support Questionnaire – Work Climate Questionnaire Results

SDT posits that supporting the autonomy of individuals will lead to greater wellbeing. The Perceived Autonomy Support Questionnaire – Work Climate Questionnaire measures participant perceptions of autonomy support in a work environment. This dissertation uses this scale to compare participant perceived autonomy levels between the autonomy and non-autonomy group to see if modifications to the autonomy training document alter perceived autonomy support. The results of the Perceived Autonomy Support Questionnaire – Work Climate Questionnaire are summarized below in Table 10: Autonomy Support Results. For each scale item, and the perceived autonomy score a mean was calculated for the complete participant group, the control group, and the autonomy group. There were no appreciable differences between the groups. One participant was removed from non-autonomy group analysis because of data collection error that resulted in a score being unable to be calculated. This participant's scores are removed from all scale items. See Appendix for Statistical test.

Scale Item	All Participants Mean(Standard Deviation)	Non-Autonomy Group	Autonomy Group
1) I feel that the document provides me choices and options	4.61 (2)	4.5 (2.17)	4.75 (1.91)
2) I feel understood by the document	4.44 (1.92)	4.2 (1.62)	4.75 (2.31)
3) I feel I am able to be open with the document's author	4.33 (1.88)	3.9 (1.79)	4.88 (1.96)
4) The document conveyed confidence in my ability to do well at managing my cybersecurity	5.28 (1.53)	5.5 (1.08)	5 (2)
5) I feel that the document's author accepts me	4.83 (1.38)	4.6 (1.17)	5.13 (1.64)
6) The document made sure I really understood the goals of my role in cybersecurity and what I need to do	4.83 (1.89)	4.5 (1.96)	5.25 (1.83)
7) The document encouraged me to ask questions	3.39 (1.94)	3.2 (1.87)	3.63 (2.13)
8) I feel a lot of trust in the document's author	4.78 (1.7)	4.4 (1.43)	5.25 (1.98)
9) The document answers my questions fully and carefully	3.5 (1.69)	3.1 (1.37)	4 (2)
10) The document's author listens to how I would like to do things	3.11 (1.78)	2.8 (1.32)	3.5 (2.27)
11) The document handles people's emotions very well.	3.78 (1.83)	3.8 (1.62)	3.75 (2.19)

12) I feel that the document's author cares about me as a person	3.83 (1.92)	3.9 (1.79)	3.75 (2.19)
13) I don't feel very good about the way the document talks to me	2.28 (1.56)	2.3 (1.16)	2.25 (2.05)
14) The document tries to understand how I see things before suggesting a new way to do things	3.28 (2.11)	3 (1.83)	3.63 (2.5)
15) I feel able to share my feelings with the document's author	3.94 (1.76)	3.7 (1.25)	4.25 (2.31)
Perceived Autonomy Score	4.24 (1.17)	4.05 (0.75)	4.48 (1.63)

Table 8: Autonomy Support Results

Development of Deductive Codes into Themes

The results of deductive analysis revealed several themes. Deductive analysis for autonomy and well-being codes iteratively developed into several of the themes in this section as initial codes and impressions became more nuanced through data collection (see methods section for full coding development timeline). Analysis identified autonomy in user through the interview transcripts. Autonomy codes ultimately solidified into two of the six themes of this analysis. 'Theme V: participant believe engaging in cybersecurity best practices is a personal responsibility but recognize that employers are mandating the behavior' developed from iterative coding around autonomy codes. 'Theme VI: some participants view autonomy language positively while others do not feel it is appropriate for the cybersecurity context' similarly developed from autonomy codes. Theme VI codes however developed as responses to autonomy language rather than expressions of autonomy in action. Well-being codes interactively developed into 'theme I: participants indicated cybersecurity training should include contextual information', 'theme II: participants indicated cybersecurity training should treat users 'like people'', and 'theme III: participants hold a variety of views on extrinsic motivation' in the perspective that threats can deter compliance.

Thematic and Inductive Analysis Results

Inductively derived codes represent common patterns in the text. Coding was completed by an individual coder. I coded deductively for autonomy and wellbeing codes. Inductive codes developed as analysis of the interview began. As the study progressed and more the analysis included more data the inductive and deductive codes developed to better reflect the data as themes (For more details see Methods section). Selected quotations from the interviews in this section illustrate themes that appeared within the interview transcripts. Not all incidences of a theme are included in the quotations included in this section. The themes of the interviews represent common descriptions of experiences described by the participants. For some themes several perspectives are also described. These perspectives represent participant responses that are more specific to fewer participants and represent divergences within the responses of participants. Each theme is introduced and described in relation to the full group of participants and then described in relation to the autonomy and non-autonomy groups so that both similarities and differences can be fully described.

Theme I: Participants Indicated Cybersecurity Training Should Include Contextual Information

Participants indicated an array of ways that communications about cybersecurity could better support them. Participants (8/19 of the participants) indicated that more information or context would benefit the cybersecurity training document. Participants indicated they desired more context about the training and cybersecurity best practices. These responses came in response to questions about how cybersecurity should be communicated. Participants desire more information about the cybersecurity training, the possible repercussions of not following the training suggestions, and if the training was precipitated by a pattern of cybersecurity attacks across the country. The information each participant wanted to know was slightly different so we include more participant quotations to describe the breadth of the information participants thought might be useful.

Kate wanted to know about the negative potential outcomes of not engaging in the cybersecurity best practices. She wanted more information about what the threats were and why she should be wary. The additional information wasn't about what she needed to do but why she should do the things she was being asked to do.

"I do think though non-compliance should be explained and how what the dangers of that are" [Kate]

Chloe wanted to know if there was an event that precipitated the communication about cybersecurity. Chloe expressed a need to know why the information about cybersecurity was being provided. Chloe wanted a connection to her work environment to contextualize the best practices document. She explained how she might expect or want the context of the training to be presented through her example of relating the cybersecurity training content to an uptick in recent cybersecurity attacks.

"I think is an additional piece to the training. Like you want to just (sic) I wouldn't think you would just hand somebody this sheet of paper and say okay, go learn about cybersecurity training, …So having some of that information I think is important. It's always important to relate to your specific environment. You might instead preface it with there's been a great uptick in the number of cybersecurity threats and attacks that have happened throughout the United States in the past week." [Chloe]

David indicated that the training document lacked information on the purpose of the training and why cybersecurity was important. David indicated he knew why cybersecurity was important through the interview but indicated the information should be included in the training document.

"Why do we care about cybersecurity other than like people are trying to like steal (sic) your information. There's like a little bit about an email, like the email one where they're trying to steal

money or something like that. But for the most part, there wasn't a lot of why cybersecurity kind of matters…it's not got a very clear purpose for why we're doing it." [David]

Sarah wanted to know the advantages or disadvantages of the best practices themselves. Sarah indicates here that how the practice impacts her is important to what she wants from cybersecurity training.

"[the training] doesn't tell you, the repercussion of not doing it or … advantages of following the instruction." [Sarah]

Grace expressed how important the why behind cybersecurity best practices is. Her response indicates that she wants to better contextualize the information she is provided. The larger understanding of cybersecurity best practices appears to be important to Grace.

"I always like to know the reason why I'm doing something instead of just do this. I think that's just part of my nature, it's always like to know why I'm doing something. Because I want things to make sense." [Grace]

Participants want more context to their cybersecurity training. Receiving a list of best practices without broader contextual information both about the cybersecurity training and the best practices themselves does not satisfy users.

Between Group Results - Theme I

Theme I appears in five autonomy framed interview transcripts and three non-autonomy framed interview transcripts. This theme appears in both groups at around the same frequency and there were not any notable differences between the groups in the way the theme presented. Participant responses described in Table 9: Between Group Results - Theme I. Users desire context to their cybersecurity training regardless of whether their cybersecurity training uses autonomy language or not.

Participant	Group	Illustration
David	Autonomy	*“there's no explanation of like, well, if you don't do these things, bad things are gonna (sic) happen to you or like if you do these things good things are happening to you”*
Trista	Autonomy	*“I guess to me like I wanted to know a little bit more. Like, it left me feeling like man, I feel like there's probably more to some of these certain bullet points. As to either like different strategies underneath each of those bullet points, or like reasons why that's recommended”*
Chloe	Non-Autonomy	*“If there was new knowledge if there were you know, other reasons why to do it.”*
Sarah	Non-Autonomy	*“[the training] doesn't tell you, the repercussion of not doing it or the advantage or disadvantages of following the instruction.”*

Table 9: Between Group Results - Theme I

Theme II: Participants Indicated Cybersecurity Training Should Treat Users in a Caring Manner

Participants (8/19 of the participants) indicated that they want their employer to treat them in a way that respects them as people. Participants indicate they want to feel cared for and be treated respectfully, in a way that cares, in a way that wants dialogue, personably, and supportively. These descriptions indicate participants want to be treated with dignity and respect. The responses indicated two-way dialogue appears important to them. The way a cybersecurity training document communicates to employees matters to this group of participants and they desire communication that treats them in a caring manner.

Abby indicates how the autonomy version of the training content is preferable specifically because she perceived that that version cared more about her.

"I think version one. I think we're kind of saying like, if it sounds a bit nicer, it sounds like it kind of cares about the employee more" [Abby]

Michelle similarly indicated a preference for the autonomy version based upon what she characterized as a conversational and approachable tone. She communicates that she prefers cybersecurity communication to be two-way and that she wants to feel able to initiate further conversations on cybersecurity.

"When you have to read like a lot of text and you know, these guidelines to make it feel more like a conversation…the tone was definitely like more conversational and more approachable." [Michelle]

Sarah explains that people prefer to be treated like humans and don't like to be ordered around.

"I think most people would not like to be ordered around and you know, treated as non-Humans. I think everyone would relate better to anything that is human, not anything that is inhumane." [Sarah]

Trista indicated that using negative reinforcement to motivate her would hurt her and that she responds better to positive reinforcement.

"I don't like being motivated with negative reinforcement. I'm someone who responds better to positive reinforcement. So, I would just be hurt if my employer told me that." [Trista]

Users desire cybersecurity communication that instills a sense of care from the organization. Cybersecurity training information needs to make users feel they are cared for, and information should be communicated in a caring manner.

Between Group Results – Theme II

Theme II appears in two autonomy framed interview transcripts and six non-autonomy framed interview transcripts. This theme appears more often in the non-autonomy framed interviews. The theme desire for more caring communication appears to be stronger in those receiving the non-autonomy training document. Participant responses described in Table 10: Between Group Results - Theme II.

David, of the non-autonomy group describes how the autonomy version of the training takes a more humanizing approach and makes him feel a sense of closeness with the people in the organization. His description only indirectly communicates a desire for caring communication. Also in the autonomy group, Trista indicates the autonomy version of the training leaves room for a conversation between her and the organization or the organization's cybersecurity group. Her description focuses on the openness to further dialogue the autonomy version creates in the final line of the training document. Trista demonstrates a preference for caring language but only critiques a small portion of the non-autonomy version. Sarah, who received the non-autonomy version of the training strongly appreciated the changes in the autonomy version when offered the chance to review it. She comments how the autonomy language appreciates her viewpoint as a user rather than taking the perspective of the organization. Sarah goes on to appreciate the acknowledgement that cybersecurity can be scary that appears in the autonomy-version. Lita, in the non-autonomy group, indicates that the autonomy version intentionally tries to be more personable and reduce the prominence of the fear inducing concepts. Lita describes a preference for the caring language more broadly than the narrower or indirect descriptions of the autonomy group participants.

Users want caring language but indicate it more often and more strongly when they received the non-autonomy training document. Participants appreciated the caring manner of the autonomy training document when originally presented with the non-autonomy training document.

Participant	Group	Illustration
David	Autonomy	*"Being like, what, everybody's kind of, we're all in this together. And like for us to be successful, we need like, everybody to be doing this."*
Trista	Autonomy	*"I think that like leaves the reader feeling more like there's the opportunity for dialogue or learning more if they don't totally understand this, so I think it feels more open like whoever's writing this desires to desires to engage and answer questions if there are some whereas if it just says, If you have any questions, email, like I feel like most things say that so it doesn't really leave me with that sense that someone truly wants to dialogue and help me if I need it."*
Sarah	Non-Autonomy	*"It's like seeing it in the view of the user, not the organization or the facilitator of this also of this training, conflict. So, and it's also putting a kind of emotional intelligence like, trying to make it feel like we know cybersecurity threats. can be scary. We know that people get agitated when they hear about things like this. But you know, we are here to support it gives more like an emotional support and makes you feel calm about it."*
Lita	Non-Autonomy	*"Like makes it seem like the author is trying to be more like personable about the content and like it makes it more like we're on the same level than not like having these like scary concepts like projected onto me and like. Like it feels more like welcoming and encouraging to learn by inviting to like get it to these practices definitely noticed"*

Table 10:Between Group Results - Theme II

Theme III: Participants hold a Variety of Views on Negative Extrinsic Motivation

A subset of participants indicated they preferred extrinsic motivation, such as negative repercussions for not completing cybersecurity training. Participants (12/19 of the participants) indicated that repercussions for noncompliance or accountability were necessary, while others (9/19 of the participants) indicated extrinsic motivators discourage compliance. The participant responses indicated a divide in whether negative extrinsic motivators such as repercussions or punishment for noncompliance benefited cybersecurity. Some participants viewed repercussions as essential to achieving a compliance, while other participants noted that the focus on negative extrinsic motivation creates a less desirable experience when receiving cybersecurity information.

Perspective: Repercussions are Necessary

Participants indicated that repercussions successfully motivate them. This dissertation explores how intrinsic motivation might benefit cybersecurity compliance efforts, but participant responses indicated strong preferences for stated repercussions, a form of negative extrinsic motivation. The participants whose responses indicated this them indicated they want repercussions because they will motivate them to adopt the cybersecurity best practices they are being requested to. This group of participants indicate that they may not adopt the cybersecurity best practices without the pressure of negative extrinsic motivation.

Grace stated that repercussions worked to motivate compliance with cybersecurity training. The sentiment here is that given the choice of a repercussion being stated or not, then it should be stated, since that would motivate Grace to do the training to avoid negative consequences.

"I think having like some sort of repercussion for not following this would be more motivating than, like, not" [Grace]

Perspective: Threats can Deter Compliance

Some participants viewed negative repercussion and threatening consequences for noncompliance as counterproductive to the intended message about cybersecurity. Participant responses reflecting this theme reported that they might feel negative emotions such as anger or resentment when motivated using negative extrinsic motivation. These negative emotions then would either interfere or distract from the intended message of the cybersecurity training document.

While a lot of pro-enforcement sentiment did appear in the interviews, participants like Sarah commented how threats can detract from the task being motivated. The threats for noncompliance can appear extreme and thus detract from the messages about cybersecurity that an organization is trying to communicate. The threat can make it harder for people like Sarah to learn through the training.

"Because once if I'm threatened to be fired these thoughts disrupt my own being, I mean, I'm no longer myself so I think I wouldn't even be in the right frame to, you know, go through a training and assimilate what they are telling me in the training because I'll just be thinking about (sic) I'll feel bad" [Sarah]

Participants are divided in their opinions on negative extrinsic motivation such as threats and repercussions. Some participants strongly prefer repercussions as motivation while other participants consider repercussions as detrimental to their compliance.

Between Group Results – Theme III

Theme III perspectives are not exclusive, and some interviews demonstrate both perspectives. The themes and perspectives of theme III present similarly in the responses of participants for the groups. Group does not appear to impact how this theme presents or the frequency it appears. Participant responses described in Table 11: Between Group Results - Theme III.

Participant responses demonstrate the Theme III perspective that repercussions are necessary appears in four autonomy framed interview transcripts and eight non-autonomy framed interview transcripts. Barbara in the autonomy group believes that the organization should have repercussions and enforce them. Quintin in the non-autonomy group indicates he may not comply with cybersecurity best practices without some threat or repercussion for noncompliance.

Participant responses demonstrate the Theme III perspective that threats can deter compliance appears in four autonomy framed interview transcripts and five non-autonomy framed interview transcripts. Hope in the autonomy group describes how she believes some people will be angry about being threatened. John in the non-autonomy group indicates he would feel negatively about how the organization chose to communicate about cybersecurity.

Whether the participants initially received the autonomy cybersecurity training document, or the non-autonomy training document does not appear to impact the view of negative extrinsic motivation the participant expresses. Users come to cybersecurity training with pre-existing views on the appropriateness of negative extrinsic motivation.

Participant	Group	Perspective	Illustration
Barbara	Autonomy	Repercussions are Necessary.	*"The company Alpha Corp has to enforce this. Especially if you are working on something particularly sensitive or private thing Alpha corporations should not only decide whether this person has to go through these bad practices, but also enforce them."*
Quintin	Non-Autonomy	Repercussions are Necessary.	*"But like, I would personally do everything you told me to cover my own butt. But obviously I'm doing that out of fear because this was probably presented to me in a way that threatened my job or you know, the company so knowing that ahead of time and then reading what I should do, would probably be more effective. Would I rather be told the more gentle way Yeah, but I know that if I'm told a more gentle way, I might shy away or maybe perhaps not take it as seriously."*
Hope	Autonomy	Threats can Deter Compliance.	*And I think that that's probably why, but I think that threatening is not a good way because I think that that would make a lot of people much more angry.*
John	Non-Autonomy	Threats can Deter Compliance.	*"I mean, it might motivate me but I but in like the back of my mind, I'm going to be feeling kind of resentful about the way that they're like, sort of, sorry, about the way that they're sort of approaching it and being a jerk about it, I guess."*

Table 11:Between Group Results - Theme III

Theme III-B: Participants Perceive Negative Extrinsic Motivation When None is Used

Some participants (5/19 of the participants) indicated the threat of repercussions, while not stating within the training content, was implied. Some participants indicated that receiving cybersecurity training content implies negative consequences for noncompliance. Participants in both the autonomy and non-autonomy groups reported that compliance is mandatory and that not following the best practices means they will face negative consequences from their employer. Participants reported this regardless of the strength of the language in the training document they received.

Michelle indicated that whether the repercussions are stated explicitly or not, noncompliance will be met with repercussions. It is understood because of the work context that failure to comply will be punished.

"So, if it's like required, it's somewhat implied that a serious repercussion will occur if you don't do it, right. It's not spelled out what will occur, but it's understood that you know, if you don't do this, there will be consequences and I would prefer that too." [Michelle]

Some participants assume negative consequences for non-compliance with cybersecurity training document best practices.

Between Group Results - Theme III-B

Theme III-B appears in two autonomy framed interview transcripts and three non-autonomy framed interview transcripts. This theme occurs in both groups at a similar frequency and presents the same. Participants from both groups each indicate they believe that they will be punished for noncompliance. They each believe that negative extrinsic motivation will be used despite the version of the training they received and that neither version included any language that would indicate this. Participant responses described in Table 12: Between Group Results - Theme III-B.

Receiving autonomy or non-autonomy language in the cybersecurity training document did not appear to impact whether a participant assumed negative consequences for noncompliance with cybersecurity training document best practices.

Participant	Group	Illustration
Trista	Autonomy	*“Because they were telling you that you have to do these things, these steps and I guess they weren't really giving you a choice.”*
David	Autonomy	*“it's not like you aren't going to like you get in trouble for necessarily not doing them”*
Kate	Non-Autonomy	*“Not understanding what was in the document could have repercussions, negative repercussions on me”*
Michelle	Non-Autonomy	*“The document didn't really spell it out. But I assume based on previous experience, that if you don't take you know, these guidelines and rule seriously that there would be repercussions.”*

Table 12: Between Group Results - Theme III-B

Theme IV: Participant Recognize Others' Communication Preferences

Participants (6/19 of the participants) indicated they understand that others within the organization might have different needs and preferences regarding communication. Of those participants (4/19 of the participants) indicated that they preferred more autonomy supportive language but understood not everyone prefers this kind of language, while others (2/19 of the participants) indicated they wanted to be motivated with more concrete controlling language and that others might prefer different language. This theme represents acknowledgements by participants that their preferences are not universal. Participants realize that organizations communicate to a broad audience with various needs and preferences for communication.

Trista highlights her preference for the autonomy version but comments that this is a personal preference for autonomy rather than a universal need.

"I feel like when I'm like offered a little more autonomy and like personal choice in like pursuing something for my own best interest and well, I feel like more motivated by that. So, it could just be my personality…personality drives the fact that I'm more drawn to version one. Like different people are motivated in different ways. And like some people might be more motivated to like make changes in their habits, if they're like very directly and firmly told what to do, which is more what version two is doing. Um, whereas like, I think other people like appreciate more of that autonomy and like choice and like (sic), creating habits." [Trista]

Quintin indicates a preference for controlling language and comments that he views this as a personal orientation. Quintin refers to his communication preferences as "personal orientation" which acknowledges the preference for controlling language would not be right for everyone.

"I will say version two is more appropriate because I'm just more oriented that way." [Quintin]

Participants give the organization the benefit of the doubt and know their communication preferences are not universal. They often recognize they prefer controlling language or autonomy language but that this is connected to them and there is not a right or wrong way to communicate.

Between Group Results - Theme IV

Theme IV appears in four autonomy framed interview transcripts and two non-autonomy framed interview transcripts. This theme appears often in more of the autonomy framed interviews. Each participant response indicates an underlying belief that there is no universal best way to communicate in this context. Participants recognize either 1) the existence of other preferences or 2) that their preferences are specific to them. Theme IV present similarly in both groups. David in the autonomy group and Lita in the non-autonomy group mention how others might have different preferences directly. Grace in the autonomy group and Quintin in the non-autonomy group both mention their preferences as part of their nature or personality. Participant responses described in Table 13: Between Group Results - Theme IV

Participants recognize other people have different communication preferences whether they received the autonomy language in their cybersecurity training document or not.

Participant	Group	Illustration
Grace	Autonomy	*“I always like to know the reason why I'm doing something instead of just do this. If I think that's just part of my nature.”*
David	Autonomy	*“So, I guess the first one could be slightly more comforting. For some people, I don't know if it's more completely necessary.” (sic)*
Lita	Non-Autonomy	*“An employer should motivate you in a gentle way. And well, I can see both sides…It might be effective for some people.”*
Quintin	Non-Autonomy	*“fear's a good motivator so I was in the military and 90% of everything ran on fear. So yeah, I would say she was like very specific to me.”*

Table 13: Between Group Results - Theme IV

Theme V: Participant Believe Engaging in Cybersecurity Best Practices is a Personal Responsibility but Recognize that Employers are Mandating the Behavior

Participants in this study indicated they consider implementing cybersecurity best practices as their personal responsibility. Participants (14/19 of the participants) indicated or implied a responsibility to implement cybersecurity best practices. Some of those participants (9/19 of the participants) indicated they felt personal responsibility for implementing cybersecurity best practices, while at the same time acknowledging that employers mandate these practices.

When asked who decides whether they implement the cybersecurity best practices David, Barbara, Emma, Grace, and Chloe each attribute the responsibility to themselves. The participant indicate that the responsibility for deciding to implement cybersecurity best practices lies with them.

"you're the one that's in control of whether or not those practices get adopted." [David]

"I do it because I think it's the responsible thing to do. Personally, I've always been somebody who is precautious about cybersecurity, given how much time I spend on the internet, and everything else I've heard and read about privacy invasion and what I know about tracking." [Barbara]

"It [the training content] reminded me to make these decisions like it related to cybersecurity. So, reminding that made me feel better about my choices because it's like, okay, I'm doing these things." [Emma]

It [implementing cybersecurity best practices] is up to the individual. [Grace]

Chloe talks about her personal responsibility by referencing a question from the Self-Regulation Scale. The previous question asked about why she would follow cybersecurity training suggestions. The question asked if she would follow the training suggestions because "wants to do well at this”. Chloe state that she doesn’t “want to do well at this” but rather she “need(s) to do well at this” to prevent negative outcomes.

“I do that's … not because I want to do well at this it's because I need to do well at this in order to prevent anything from going wrong.” [Chloe]

Quintin states that implementing cybersecurity best practices is up to him but also that it is a mandated task and part of his role at work. He acknowledges it is up to each person in the organization to adopt best practices but that his employer leverages employment to mandate compliance.

“It's my job…It's up to the individual, whether I want to keep my job or not.” [Quintin]

While Abby recognizes she is personally responsible, she also recognizes that receiving cybersecurity best practices from her employer means the employer can punish her for not engaging in these practices.

“It would be up to me, but then I feel like if I didn't do the best practices, and I were caught, I feel like I would probably get in trouble. So, kind of me, but there's also kind of a higher power.” [Abby]

When asked about whose responsibility cybersecurity is, Kate recognizes she is the responsible party. Like Abby, Kate acknowledges her employer may be able to see what she does depending on the circumstances.

“I would think ultimately me if I'm the one in the driver's seat on a daily basis in front of a computer, but I guess that depends on whether how and to what extent they have oversight of my if it's a work computer, for instance, or using work affiliated software programs.” [Kate]

Michelle responded to the question of "who is responsible for implementing cybersecurity best practices" with a recognition of personal responsibility while also noting that repercussions exist even when not directly stated in the training document.

"it's ultimately you, but I assume well, I'd be. The document didn't really spell it out. But I assume based on previous experience, that if you don't take you know, these guidelines and rule seriously that there would be repercussions." [Michelle]

Rei implies she is in control of whether to implement cybersecurity best practices and that she should engage in those practices because she is a paid employee.

"they're paying me so I probably should listen to them and do them." [Rei]

Trista states that while she doesn't know whether the training content was written in a way that implied, she was responsible or whether the organization was mandating it. Regardless of not recalling how the document stated it, Trista acknowledges that these best practices rely on her to either adopt them or not.

"I also recognize like, that the habits that I have that are successful for the realm of cybersecurity, are because I've either adopted it myself, or I haven't adopted it by myself. So, I think just like from past experience, I recognize that ultimately, it's not going to be adopted unless I choose to adopt it. But I don't know if the document was written in a way that like, made it seem like it was my decision." [Trista]

Participants feel responsible for cybersecurity and recognize the role of an employer in promoting and enforcing cybersecurity practice.

Between Group Results - Theme V

Theme V appears in two autonomy framed interview transcripts and seven non-autonomy framed interview transcripts. This theme appears in more often in the non-autonomy framed interviews. Personal Responsibility for cybersecurity appeared in nearly every interview however the recognition of the mandate from the employer came across more often in non-autonomy group interviews. The theme present similarly across the groups. Participants from each group indicated they make the decision when it comes to cybersecurity best practices while also acknowledging their employer may require them to do so through various means. Participant responses described in Table 14: Between Group Results - Theme V

Participants were more likely to acknowledge their responsibility and that employers mandate adopting cybersecurity best practices if they received the non-autonomy training document.

Participant	Group	Illustration
Abby	Autonomy	*"I guess it would be up to me, but then I feel like if I didn't do the best practices, and I were caught, I feel like I would probably get in trouble"*
Barbara	Autonomy	*I think especially if I think the responsibility of it is the responsibility of the employee to safeguard and take care of "these of these private and sensitive information. But at the same time, I feel like if it's very important for it to happen, it has to be a two-way street to because my experience is not a lot of people would be willing to jump through these hoops that is made mandatory. And I think that's when the authority was to offer cooperation to enforce that. So that it becomes more clear (sic) that it is an instruction and is a requirement and is not a suggestion."*
Chloe	Non-Autonomy	*"I can make that decision for myself personally. My employer may make that decision for me as part of a group, you know, or as an employee at that place at this institution. But in the end, it's up to me to adopt the best practices."*
Vanessa	Non-Autonomy	*"That can kind of be enforced, but ultimately, it kind of just comes down to like the individual."*

Table 14: Between Group Results - Theme V

Theme VI: Some Participants View Autonomy Language Positively While Others Do Not

Participants indicated a variety of opinions regarding the autonomy language and control language in the training documents they were presented. Participants (15/19 of the participants) made comments that indicated a positive perception of autonomy language, while participants (5/19 of the participants) indicated autonomy language produced negative perceptions of the cybersecurity training document. Some participants expressed both positive and negative perceptions about the autonomy language in the autonomy cybersecurity training document.

Perspective: Autonomy Language Creates Positive Perceptions

Participants indicated they had positive perceptions of autonomy language in the cybersecurity training document. Barbara describes how being given more alternatives might mean more opportunities to not engage in secure behaviors.

"I think you give people a lot of leeway and a lot of alternatives and like you can like bypass certain things or you can -might choose not to do certain things." [Barbara]

Rei describes the autonomy version as offering options regarding cybersecurity rather than issuing commands. She also felt it was more inviting.

"Yeah, so I guess the first one is just less do this. Do this, do this. It's like giving you the option to do it… It's like, I still it's still up to me. No one's making me do it... But so I guess this one's like even more, not making you do it. (sic) Well, I guess maybe it's more inviting." [Rei]

Michelle highlights how the standard document gives too many instructions. The sentiment Michelle expresses here is that multiple instructions are unfavorable. Michelle comments how the autonomy version feels like it is engaging in a conversation with the employee and is approachable.

"When you have to read like a lot of text and you know, these guidelines to make it feel more like a conversation and more you know, not to say use simpler words on this one necessarily, but the

tone was definitely like more conversational and more approachable. Whereas version two is just like, do this and do that." [Michelle]

Sarah felt that the way the autonomy version was written gave her confidence in her ability to accomplish the tasks.

"But the first version makes me feel like okay, something I should be able to do awesome." [Sarah]

Trista expresses directly how the autonomy in the autonomy version is more motivating than the alternatives.

"I feel like when I'm like offered a little more autonomy and like personal choice in like pursuing something for my own best interest and well, I feel like more motivated by that." [Trista]

Emma indicates that the autonomy version serves as a reminder of what she needs to do to maintain her cybersecurity. She specifically remarks how the autonomy training document does not make her feel bad. In this instance she indicates she expects a training document to make her feel bad or guilty but this one doesn't. She viewed the training document positively.

"And it was more of a reminder than(sic), like yelling at me like making me feel bad." [Emma]

Perspective: Autonomy Language is Bad for Cybersecurity

Participants indicated that they perceived the autonomy language in ways that are the opposite of other participants. Autonomy language came across to some participants as unappealing and lacking authority. For these participants autonomy language produced negative perceptions.

Barbara interpreted the training document with the autonomy language as suggestions and she viewed this negatively. Barbara strongly preferred to receive cybersecurity training information as direct orders.

"I saw the language and the document does not seem commanding...and if I was an employee, looking at this document, I would take these as suggestions, not instructions." [Barbara]

The language in the autonomy training document came across negatively for Quintin. He remarks how the autonomy training document sounds as if it is blaming him rather than encouraging him. The language that intends to encourage feelings of autonomy creates a sense of blame for Quintin.

"...when I'm reading these strong passwords, it almost seems like the blame is put more on me." [Quintin]

Some participants prefer autonomy language while other participants do not. Autonomy language does not appear to be universally popular with users for cybersecurity compliance efforts.

Between Group Results - Theme VI

Participant responses demonstrate the Theme VI perspective that autonomy language creates positive perceptions appears in seven autonomy framed interview transcripts and eight non-autonomy framed interview transcripts. The theme appears at roughly the same frequency in both groups. The perspectives of this theme are not exclusive, and some interviews demonstrate both perspectives. Participant responses described in Table 15: Between Group Results - Theme VI.

Seven of the autonomy framed interview transcripts demonstrate the perspective that autonomy language creates positive perceptions while two demonstrate that perspective autonomy language is bad for cybersecurity. This perspective presented similarly across both groups. Michelle in the non-autonomy group and Emma of the autonomy group both indicated they held a favorable opinion toward the autonomy version of the training document when comparing them.
Participant responses demonstrate the Theme III perspective, that autonomy language is bad for cybersecurity, appears in two autonomy framed interview transcripts and three non-autonomy

framed interview transcripts. This perspective presented similarly across both groups. Vanessa in the non-autonomy group indicated she preferred the stronger language of the non-autonomy version because of her strong feelings about identity theft. Trista in the autonomy group could not recall how the training document communicated the information and whether it made her feel as if it was her decision. She stated that in the end it was her decision to adopt the best practices or not rather than through being prompted by the training document. Trista's statement did not indicate a direct dislike for autonomy language in cybersecurity, but she indicated she didn't think it mattered.

Participants possess pre-existing preferences for autonomy language, whether they received the autonomy language in their cybersecurity training document or not.

Participant	Group	Perspective	Illustration
Emma	Autonomy	Autonomy Language Creates Positive Perceptions	*"I like the first version because it seems a little nicer. It's more like it the author is looking at me as a person you know, it's more personalized."*
Michelle	Non-Autonomy	Autonomy Language Creates Positive Perceptions	*"I did appreciate how the documents sort of spelled out it was written in a more conversational tone"*
Trista	Autonomy	Autonomy Language is Bad for Cybersecurity	*"I don't know if like the document was written in a way that like made me feel like it was my decision. But I also recognize like, that, like the, the, like, habits that I have that are successful for the realm of cybersecurity, are because I've either adopted it myself, or adopted it myself or I haven't adopted it by myself."*
Vanessa	Non-Autonomy	Autonomy Language is Bad for Cybersecurity	*"Like here's things that you would need to do in order to protect yourself and other ones like if you're wanting to here's some suggestions. So, I personally like the second one (the non-autonomy version), but that's because I know I don't like when people's identities get stolen"*

Table 15: Between Group Results - Theme VI

Theme VII: Participants were Familiar with the Training Content and Indicated That This Increases Their Confidence

Participants (15/19 of the participants) in this study indicated they were familiar with the content of the cybersecurity training documents. Participants often recognized the content of the cybersecurity training document. Of those participants who were familiar with the content of the training document some participants (10/19 of the total participants) indicated seeing familiar content was confidence boosting. When asked about how they felt about seeing familiar content, these participants described feeling more confidence and capable in cybersecurity. Seeing cybersecurity best practices that they knew, communicated to these participants that they were knowledgeable in this area.

Kate identifies the training content as being standard cybersecurity training language. Kate expresses that seeing familiar content made her feel good. She relates how seeing training content that she knew made her feel confident in her own preexisting knowledge and that she was not "a grandma" or someone whose knowledge was outdated.

"I feel like that's pretty standard onboarding, cybersecurity training language. I felt pretty good. That I had at least heard of all of them…[I] Didn't feel like a grandma basically, I was aware of things that I'm already doing and so I felt like it made me feel like I'm well protected, but perhaps I could be better protected in some ways." [Kate]

Sarah also indicated that seeing familiar content made her feel confident in her knowledge while also feeling she needed to be more active in protecting her cybersecurity. Her response indicates she felt she knew the content and that it both made her feel confident in her abilities but insecure about her cybersecurity behavior.

"It makes me feel like I know a little bit about cybersecurity… but it's also made me feel that I need to do more in protecting cybersecurity." [Sarah]

Providing familiar cybersecurity best practices demonstrated a boost in participant confidence.

Between Group Results - Theme VII

Theme VII appears in four autonomy framed interview transcripts and six non-autonomy framed interview transcripts. This theme appears at a similar frequency in both groups. Theme VII presents similarly in both groups. Barbara, in the autonomy group, indicates she felt the document made sense and that she had seen the content before. Her indications were that she felt confident seeing information she already knew. Emma, in the autonomy group, indicated seeing familiar content empowered her and Kate, in the non-autonomy group, indicated she felt good seeing familiar content. Quintin, in the non-autonomy group directly states seeing familiar content helps him to feel more confident in cybersecurity. Participant responses described in Table 16: Between Group Results - Theme VII.

Familiar cybersecurity best practices are associated with reported feelings of confidence whether participants received the autonomy or non-autonomy cybersecurity training document.

Participant	Group	Illustration
Barbara	Autonomy	*"A lot of the document information that was reiterated in the document is permission that I have come across at some point prior to this. So, a lot of this is kind of like yes, I've seen all this before, and I've seen the guidelines for this before. Yes, this makes sense."*
Emma	Autonomy	*"It's more just like a reminder to act this way. It wasn't like, negative towards me. Didn't seem like it was. I don't know. Like looking down on me for not being cyber safe or something like that. I think that it, I guess is a little bit empowering."*
Kate	Non-autonomy	*"I felt pretty good. That I had at least heard of all of them. And I was aware of things like the multifactor authentication."*
Quintin	Non-autonomy	*"So, and also like reaffirms my suspicions like why am I doing this? So just having a little bit background knowledge, even if it's just saying something as simple as like, because it is zero attack exploits, actually, like makes me feel a lot more confident. So, the document helps with that."*

Table 16: Between Group Results - Theme VII

Chapter 6: Discussion

Introduction

The dissertation's findings make noteworthy contributions to multiple discussions in the field of cybersecurity. Specifically, the research sheds light on various areas of inquiry, including users' autonomy perception, the role of organizations in promoting user well-being in cybersecurity, the effectiveness of autonomy-based motivation in encouraging cybersecurity compliance, the dynamics between users and organizational cybersecurity communication, users' preferences for cybersecurity communication, the utility of autonomy framing in mitigating autonomy loss, and the divergence among users in terms of internalization. These contributions are elaborated upon through the incorporation of themes and quotations presented in the results section, while the background and literature review sections provide the context for the sources utilized in this research.

Do Users Feel Autonomy in Cybersecurity?

Several previous studies have demonstrated using autonomy language to motivate cybersecurity behavior (A. Johnston, 2020; Lee, 2015; Menard et al., 2017; Wall et al., 2013). That work focused on measuring behavioral intentions to comply rather than exploring the experiences of autonomy of participants (A. Johnston, 2020; Menard et al., 2017). This dissertation shows how users perceive autonomy-based motivation in cybersecurity training. Interview responses provide insight into how participants experience aspects of autonomy in cybersecurity. This dissertation uses the definition that autonomy is freedom from undue influence and is characterized by feelings of ownership, responsibility, and an authentic connection to behavior.

As depicted in the findings chapter, Theme V indicates that participants experience autonomy in relation to the cybersecurity training texts through both expressions of personal responsibility for cybersecurity and openness to influence. For example, Vanessa expressed she knew adopting cybersecurity practices is her decision but that she can be forced by her employer (as previously included in the results section). She indicates both a responsibility to adopt the best practices and an openness to influence from her employer. Vanessa said that adopting cybersecurity best practices "*can kind of be enforced, but ultimately, it kind of just comes down to like the individual*." Likewise, Abby expresses responsibility and acceptance toward repercussions for not adopting cybersecurity best practices. Abby states this saying *"I guess it would be up to me, but then I feel like if I didn't do the best practices, and I were caught, I feel like I would probably get in trouble."* These expressions of personal responsibility for implementing cybersecurity best practices appear across both the autonomy language and non-autonomy language group. Participants reported they were responsible, and they felt they could act. Agency, a requirement for autonomy, means a person must feel they are able to act (Mackenzie & Stoljar, 2000; Parfit, 2011; Pettit, 1999; Rubel et al., 2020). Participants reported they feel they can act and therefore they appear to be experiencing agency in their cybersecurity practice. While participants reported they were aware they were or could be mandated to adopt cybersecurity best practices, participants did not indicate that it was improper for their employer to influence them to adopt cybersecurity. In fact, there were indications from some participants that they prefer more direct influence such as evidenced in the perspective that repercussions are necessary within Theme III. For Example, Quintin expressed that being motivated gently was nice but that more direct extrinsic motivation would be more effective and that was his preference. Quintin said, "*Would I rather be told the more gentle way Yeah, but I know that if I'm told a more gentle way, I might shy away or maybe perhaps not take it as seriously*." Participant responses support that the influence an employer uses in motivating cybersecurity behavior appears to them as legitimate and not undue.

The literature shows that users care about their privacy and security (Kokolakis, 2017). The participants of this dissertation showed they cared about security by expressing authentic intentions regarding cybersecurity. For example, the results chapter describes how Vanessa explains a personal dislike for identity theft. Vanessa states "*I know I don't like when people's identities get stolen.*" Chloe expressed a deep commitment to cybersecurity. Chloe explains, "*I do that's ... not because I want to do well at this it's because I need to do well at this in order to prevent anything from going wrong.*" Barbara indicated she had done previous reading regarding digital tracking and privacy and that she felt like a person with a privacy and security mindset. Barbara says, *"I've always been somebody who is precautious about cybersecurity, given how much time I spend on the internet, and everything else I've heard and read about privacy invasion and what I know about tracking."*

This dissertation's results complements prior research on autonomy and behavioral intentions to comply. Participant responses demonstrate that autonomy is being experienced regarding cybersecurity as they express the ability to adopt cybersecurity practices, responsibility, or ownership for adopting those best practices positive attitudes toward being influenced by employers, and authentic connections to security concerns. The responses demonstrating autonomy by the participants occur across the autonomy and non-autonomy groups. The inclusion or exclusion of autonomy framing elements from the cybersecurity training document the participants received, did not appear to encourage, or discourage responses indicating participant autonomy. This dissertation raises questions regarding whether autonomy language in cybersecurity motivation encourages users to feel autonomy in cybersecurity. Autonomy language may make users feel better but not impact their preexisting sense of autonomy. Future work may consider exploring autonomy perceptions in cybersecurity and their impact on cybersecurity compliance intentions.

How Do We Support Wellbeing in Cybersecurity?

Using Self-Determination Theory (SDT)-based motivation leads to higher reported wellbeing in education, therapy, health, and other fields (Deci et al., 1989; Pelletier et al., 1997; Vansteenkiste et al., 2004; Williams et al., 1996). Previous studies have used SDT in cybersecurity motivation but haven't focused on wellbeing, which is the intended benefit of using SDT motivation (A. Johnston, 2020; Lee, 2015; Menard et al., 2017; Wall et al., 2013). The benefit of using SDT and autonomy support is that motivation can be applied while still supporting basic psychological needs and producing a higher sense of wellbeing. This dissertation adds to this area of inquiry by measuring well-being and providing user accounts of how cybersecurity efforts can influence wellbeing. This dissertation provides an important first look at wellbeing in cybersecurity training.

As outlined in the results chapter, the results of the Learning Self-Regulation Questionnaire indicate differences in wellbeing through differences in self-regulation. As outlined in the literature review the self-regulation of an individual represents the level of self-determined vs controlled functioning (*Metrics & Methods*, 2021).The results of this questionnaire show:

- little difference between the two groups in participant reports of perceived autonomous regulation, regulation that is identified or integrated.
- There is a larger yet insignificant (p=.051) difference in reports of perceived controlled regulation, regulation that is external or introjected. The non-autonomy group had higher self-regulation scores.

- The relative self-regulation index shows a significant difference (p=.03) between the two groups. Relative self-regulation is defined as the difference between autonomous and controlled regulation. The autonomy group shows more relative self-regulation than the non-autonomy group.

Autonomous regulation:

Of note, the results indicate that autonomy supportive language did not increase perceived autonomous regulation as one might have expected.

Controlled regulation

The larger, yet not statistically significant, difference between the controlled regulation sub-scores has two possible explanations. 1) The autonomy training document decreased the controlled regulation for the autonomy group or 2) the non-autonomy document increased the controlled regulation for the non-autonomy group.

Relative self-regulation

The difference between the groups in relative self-regulation appears to come from the larger difference in perceived controlled regulation from the training document. The language in the non-autonomy document directly told the reader to engage in cybersecurity best practices whereas the autonomy training document phrased the best practices as a choice. Offering participants the choice to engage in best practices appears to lead to lower reported controlled regulation, while autonomous regulation remained at similar levels between the groups. The change in the language changed the amount of controlled regulation the autonomy language group experienced which precipitated a higher level of relative self-regulation.

The primary, but not only mechanism for impacting reported relative self-regulation is through the impact of controlled regulation. This aligns with Theme V results that indicated that most 73.68% of participants indicated a sense of personal responsibility for cybersecurity. Of the 47.37% of participants indicating that they felt mandated to engage in cybersecurity most were part of the non-autonomy group (7 out of the 9 interviews that demonstrated the theme). Receiving the non-autonomy document made the participant more likely to report they perceived cybersecurity as a mandate. Participant responses suggest autonomous regulation remains more constant despite alterations to the cybersecurity training. The non-significant differences between the groups suggests that controlled regulation could be impacted by alterations to the training document with autonomy but more research with larger sample size is necessary.

If our results hold true in larger studies, it could indicate that cybersecurity training can support the wellbeing of users through autonomy framing. Autonomy framing may not increase the autonomous regulation users perceive but the autonomy framing will reduce the amount of perceived controlled regulation. With lower perceived controlled regulation, users have a higher relative self-regulation. Higher self-regulation is associated with wellbeing. Autonomy framing reduces user perceptions of controlled regulation, which leads to higher relative self-regulation therefore autonomy framing supports the wellbeing of users.

Theme VI revealed that some participants report positive perceptions, such as reports of self-regulation, when presented with autonomy language. Participant interviews indicate higher relative self-regulation and describe the document as having lower controlled regulation. For example, Rei indicated that she liked that the autonomy version of the training document and that it came across less demanding and controlling. For Rei, the autonomy language appeared to facilitate self-regulation. Rei described this saying *”It’s like giving you the option to do it.”*

In Theme II, participant responses indicated how their wellness can be supported beyond self-regulation; for example, they felt they could be best supported by being treated like ‘human beings’ and they desired less-controlling language. Participants within this theme are indicating a need for relatedness with their organization. For example, Abby indicated she prefers the autonomy version because it sounded like it cared for her. Abby indicates that she wants to feel cared for by the organization when receiving cybersecurity communication. Abby reports that the version of the training she prefers *“sounds a bit nicer, it sounds like it kind of cares about the employee more.”*

Lita describes how the autonomy language version lowered the perceived power differential between her and the sender of the message. Furthermore, she indicates that the language of the autonomy version came across as both inviting and less scary. Lita describes her experience of the autonomy version of the training document, “*it seem(s) like the author is trying to be more like personable about the content and like it makes it more like we're on the same level than not like having these like scary concepts like projected onto me and like. Like it feels more like welcoming and encouraging to learn by inviting to like to get it to these practices definitely noticed.”*

It seems that the use of autonomy language has a positive effect on the well-being of certain participants, which is consistent with our initial predictions. Specifically, one group of participants responded favorably to the document presented with an autonomy framing, while another group did not. Surprisingly, we also discovered that participants feel a sense of responsibility towards their cybersecurity practices regardless of the type of training document they received. This suggests that participants may already have a sense of autonomy when it comes to their cybersecurity.

Should we use Autonomy in Cybersecurity?

Previous work has shown that behavioral intentions are positively affected by autonomy appeals (A. Johnston, 2020; Lee, 2015; Menard et al., 2017; Wall et al., 2013). This dissertation explores how individuals feel about autonomy language in cybersecurity contexts rather than their compliance intentions. As shown in the results in Theme VI, the participants did not agree on whether autonomy language helps or hurts the mission of cybersecurity training. Some participant responses supported the perspective that autonomy language creates positive perceptions as seen in the results of previous studies (A. Johnston, 2020; Lee, 2015; Menard et al., 2017; Wall et al., 2013). Participant Trista expressed this view clearly by stating *"I feel like when I'm like offered a little more autonomy and like personal choice in like pursuing something for my own best interest and well, I feel like more motivated by that."* For other participants though the autonomy language undermined the message. Barbara explains that autonomy supportive language makes the cybersecurity best practices being promoted by an organization appear more like suggestions than directions. Barbara comments that "*I saw the language and the document does not seem commanding…and if I was an employee, looking at this document, I would take these as suggestions, not instructions."* Other participants reported that the non-autonomy language version was preferable because they view cybersecurity as important. Vanessa's indicated "*I personally like the second one (the non-autonomy version), but that's because I know I don't like when people's identities get stolen.*" Previous studies have sought to show that compliance intentions are successfully motivated using autonomy language, but the results of this dissertation suggests some concerns with this approach (A. Johnston, 2020; Lee, 2015; Menard et al., 2017; Wall et al., 2013). Some users prefer more controlling language because of the gravity of the problem and find the autonomy language less authoritative. If autonomy language makes the cybersecurity information passed onto organizational users less authoritative to some individuals, then compliance efforts may suffer.

This research set out to uncover support for either using autonomy supporting language in cybersecurity motivation or contrary evidence that would cast doubt on using autonomy supporting language in cybersecurity training. Our results include perspectives supporting both. Some participants like autonomy and some users dislike autonomy. I believe this suggests that autonomy while motivating for some is demotivating for others The results show that autonomy supporting language does not make all users feel motivated raising doubts about its utility in all cybersecurity contexts. Future studies should explore whether users know their preferences for autonomy language or control language and assess outcomes when users can choose their preferred mode. Such a study could explore whether choosing their own training language will generate positive perceptions and intention to comply in users.

The Organizational User's Relationship with Cybersecurity Communication

Professionals know cybersecurity is important for organizations. Participants indicate this across several themes in the results chapter. As described in Theme III, some participants favor negative extrinsic motivational methods to push themselves and others to comply. As demonstrated in Theme III-B, some saw the mandate implied in just receiving a cybersecurity communication.

Participants feel responsible for their cybersecurity behaviors despite knowing the organizations mandate certain cybersecurity behaviors, as described in Theme V, participants feel responsible for their cybersecurity practices. This could indicate a move over recent years and given several widely publicized security breaches in large companies, from users seeing cybersecurity as an externally regulated behavior to increasing internalized motivation. Previous work showed users lament about cybersecurity getting in the way of their work (Albrechtsen, 2007). Previous work indicated users care about their security but won't align their behavior with their concerns (Kokolakis, 2017). Organizational efficiency concerns often trumped security concerns (Albrechtsen, 2007).

The results indicate that the study participants do feel responsible. This may explain why the autonomy version of the training document resonated with participants' desires for context in Theme I and caring language as described in Theme II. This could also explain why as a previous study showed, using "your" instead of "our" increased cybersecurity compliance intentions (A. C. Johnston et al., 2019). The ownership implied with the word "your" may resonate with users and improve compliance intentions.

When participants were asked about what they wanted from cybersecurity training document language many recognized that the organization is communicating to many different people. Some participants went out of their way to recognize and acknowledge their communication preferences were not universal and that other people have different preferences.

This study's participant responses suggest that organizational users know the importance of cybersecurity to the organization, they feel responsible for their part of cybersecurity efforts, and they can acknowledge that their communication preferences in cybersecurity are not universal.

User Communication Preferences

Several communication preferences findings emerged from the data. For example, Theme III indicates some participants want to see negative extrinsic motivation to feel motivated and comply. This finding suggest that some organizational users want to see repercussions. This fits with results from the literature that showed that individual-loss-framed messages were effective at motivating cybersecurity compliance (Burns et al., 2019). Individual loss-framed messages emphasize the potential negative outcomes of noncompliance. Individual loss-framed messages use negative extrinsic motivation to drive behavior change. Theme I indicates that some participants wanted context to cybersecurity communication messages. This suggests that additional context may allow users to feel persuaded to adopt cybersecurity best practices rather than coerced because of the power employers wield over them (Susser et al., 2018). Users want to feel they have a choice and can freely and rationally make decisions about cybersecurity. Theme II indicates that the study participants want to be treated ‘like people’. Cybersecurity communications that come across as “conversational”, “approachable”, “welcoming”, and “nicer” were well received by participants while participants described communication that came across “inhumane”, as “negative reinforcement”, or not producing a “sense that someone truly wants to dialogue” produced negative sentiment. Participants want to feel connected to their organization when they receive cybersecurity mass communications. Theme III indicates some participants see threats and negative extrinsic motivation as deterring their compliance and adoption of cybersecurity best practices. This suggests that a focus on repercussions could deter users from compliance. This fits with existing literature from other fields that negative feelings interfere with motivation (Perugini & Bagozzi, 2001).

Autonomy Framing Prevents Autonomy Loss

This dissertation chose to using framing as theoretical framework for supporting autonomy in this study. Previous work had used autonomy appeals or autonomy support in a general sense. Using framing allowed the dissertation to consider the role of language in supporting autonomy and wellbeing. Framing intends to alter the reception of a message to emphasize one aspect over another. The framing we employed in this study sought to encourage users to feel they have autonomy in cybersecurity. The results of the study are mixed as to whether the framing produced autonomy or not. The difference in relative self-regulation indices between the autonomy and non-autonomy group may suggest that autonomy framing did produce a difference in self-regulation, or experienced autonomy. Conversely, neither the vitality score not the perceived autonomy support scores differed between the groups. Furthermore, participants from both groups reported feeling personally responsible for implementing cybersecurity best practices regardless of group. These results appear to indicate that the framing did make participants feel autonomous in cybersecurity. However, some participants exhibit preexisting autonomy regarding cybersecurity practice. In short, it could be that autonomy framing did not alter participants to believe they have autonomy in cybersecurity practice, because they already felt autonomous. However, the autonomy framing appears to support participant wellbeing. A possible mechanism for this may be that autonomy framing reduces perceptions of external regulation. The autonomy framing may not be operating as anticipated by enhancing perceptions of autonomy. Rather, it could be preserving pre-existing autonomy by preventing its loss. The aim of the autonomy framing was to encourage participants to view cybersecurity as an area where they have control. Rather than instilling new beliefs, the framing reinforced pre-existing ones and prevented the loss of autonomy that would have resulted from controlling language.

Framing did not change how participants viewed cybersecurity; thus, it does not appear to have been any more or less effective than autonomy support or appeals. The framing supported participants wellbeing but did not change how participants thought about the material.

The Internalization Divide

The fact that participants react differently to the same communication suggests that there is no one-size-fits-all approach to communicating cybersecurity effectively. Theme III indicates a divide among the participants: those who perceive negative extrinsic motivation as constructive, while others consider it undesirable. This divide could indicate that the participants are experiencing different forms of regulation in cybersecurity.

Participants who seek extrinsic motivation are aware that the organization expects them to engage in cybersecurity practices, but they feel that they require external incentives to follow through. This group of participants may be expressing their need for external regulation, suggesting that they have not yet fully internalized the importance of cybersecurity and require external incentives to comply.

Participants who have a negative view of extrinsic motivation may have already internalized cybersecurity values. There are different levels of internalization, ranging from introjected regulation to identified regulation and integrated regulation, each reflecting varying degrees of internalization of a particular value or behavior (Ryan, 2017). Those who dislike negative extrinsic motivation seem to exhibit internalization. Our findings reveal a divide between those with internalization and those without, but the divide may be more nuanced. It is unclear which specific form of internalized regulation each participant is experiencing and what type of regulation is involved in cybersecurity practices. Different communication strategies may benefit users differently based on the level of internalization of cybersecurity practices, whether users are in an introjected, identified, or integrated state.

As shown in the results chapter, we see two groups in their approach to negative extrinsic motivation. To compare the two groups' perspectives on negative extrinsic motivation, let's examine the differences between Quintin and Sarah. Quintin demonstrates external regulation and favors negative extrinsic motivation. Quintin talks about how he would adopt cybersecurity best practices to protect himself from consequences. He says *"I would personally do everything you told me to cover my own butt. But obviously I'm doing that out of fear because this was probably* *presented to me in a way that threatened my job."* Sarah dislikes negative extrinsic motivation and described that it would make her feel bad and distracted. She describes *"Because once if I'm threatened to be fired these thoughts disrupt my own being, I mean, I'm no longer myself so I think I wouldn't even be in the right frame to, you know, go through a training and assimilate what they are telling me in the training because I'll just be thinking about (that)I'll feel bad."* Sarah describes fear and negative feelings interfering with her motivation rather than driving it. Her internalized regulation is disrupted by threats and repercussions. Negative extrinsic motivation is motivational for those in an externally regulated stage, but for those whose regulation is now internalized negative extrinsic motivation appears to produce negative perceptions from being threatened unnecessarily. These participants already feel internal pressure to adopt cybersecurity best practices and external pressure may be overwhelming. Studies have shown similar phenomena, that threats of punishment and negative extrinsic motivation undermine autonomy and intrinsic motivation (E. L. Deci & W. F. Casio, 1972).

If the division on negative extrinsic motivation observed in the participants is representative of the wider population, it could imply that there are two distinct groups of organizational users with varying levels of internalization of cybersecurity practices. These groups would have different communication preferences, depending on whether cybersecurity practices have been fully integrated into their behavior. Therefore, cybersecurity training and communication should cater to both groups to effectively promote best practices. Conducting further research to classify users based on their level of regulation and the differences between these groups would provide more insight into how to support users at different stages of regulation.

Implications for Research

This dissertation makes several contributions to the SDT cybersecurity literature. The results of my study indicate participants feel they have autonomy in cybersecurity whether presented with autonomy language or with control language. Participant responses provide the field with indications of how autonomy supportive language impacts their wellbeing in cybersecurity by increasing relative self-regulation and appealing to the user need for caring language. Participants do not however report a universal preference for autonomy language with some users feeling positive about the autonomy language while others preferred the non-autonomy version of the document. This suggests that autonomy language will not always benefit cybersecurity compliance efforts.

Previous studies using SDT in cybersecurity used quantitative methods to show SDT supported compliance intentions (A. Johnston, 2020; Lee, 2015; Menard et al., 2017; Wall et al., 2013). Previous studies suggested using mixed method or qualitative studies to examine how to predict compliant behavior in cybersecurity. This dissertation does this, and the results demonstrate the complexities of the user relationship with organization cybersecurity efforts. The nuanced results the qualitative aspect of this dissertation offers to the field suggests that more qualitative work would be beneficial. Future work where researchers work closely with end-user participants may refine the results of this dissertation or reveal additional phenomena. Participants in our study indicated more contextual information was desirable and future studies could expand this area of inquiry to find out what information is most often desired, how it should be presented, and why particular information is wanted.

This dissertation demonstrates the use of the Subjective Vitality Scale, the Learning Self-Regulation Questionnaire, and the Perceived Autonomy Support Questionnaire – Work Climate Questionnaire in cybersecurity. These scales were not previously adapted for cybersecurity and our results indicate the Learning Self-Regulation Questionnaire could be useful for future research. Our small sample produced a significant difference between relative self-regulation between the groups which suggests that this scale works in this context. Future work using the Learning Self-Regulation Questionnaire with a larger number of participants could provide evidence to support the indication that users experience autonomy in cybersecurity described earlier.

Implications for Practice

This dissertation offers insight for how organizations should promote cybersecurity. Organizations communicate to their users about cybersecurity often and this dissertation indicates a few ways that benefit users. Users want context in cybersecurity. When providing users with cybersecurity information organizations should strive to inform users about the commitment of the organization to cybersecurity, the benefits and drawbacks of cybersecurity practices, trends in cybersecurity attacks, and what the consequences of noncompliance are. To motivate users, provide users with clear but not overly emphasized consequences to motivate compliance while balancing the needs of users who prefer extrinsic motivation and those who do not. Users appreciate caring language like seen in the autonomy training document in this dissertation. Caring language should encourage positive perceptions for users that want that kind of treatment. Familiar content can also be used by organizations to build confidence in their userbase when appropriate.

Users have feelings about cybersecurity and organizational cybersecurity efforts benefit from knowing more about users' feelings. Some users will disapprove of how cybersecurity is communicated whether autonomy supporting language is used. Other users do understand that communication preferences are not universal and will give the organization leeway when the organization communicates cybersecurity. Users feel responsible for implementing cybersecurity best practices, but some users need the organization to motivate them to implement them.

This study sheds light on autonomy and communication in cybersecurity. Previous work shows autonomy support can produce positive cybersecurity behavioral intentions, this work offers more context to that (Menard et al., 2017). Cybersecurity professionals looking to implement autonomy into their cybersecurity awareness programs should consider that some of our participants did not approve of autonomy for cybersecurity. This dissertation indicates that while some will benefit from autonomy, others will not. Autonomy support while promising in terms of behavioral intentions and the preferences of some of our participants, it is not a universal best practice for cybersecurity communications.

Limitations

There are several limitations relevant to interpreting the results of this dissertation. This dissertation does not attempt to establish causal relationships or correlations. Its scope is limited to a small sample of participants who have shared their subjective experiences with cybersecurity. Therefore, the findings cannot be extrapolated to a larger population. This dissertation prioritized collecting qualitative data over acquiring a larger number of participants. With a usable n of 19, the sample size if not large enough for a full quantitative study and thus the quantitative results should not be interpreted as more than a pilot study. Another significant limitation is that the themes generated through thematic analysis were done by an individual coder thus are less reliable than coding corroborated by additional coders. This limits the validity of themes generated in this dissertation as there is no other researcher who has evaluated the interview transcripts for the themes. As a post-positivist researcher, I believe that the identity and biases of the researcher impacts the conclusions found but do not believe this diminishes the value of the conclusions themselves.

The fact that the study employed fictionalized training scenarios (i.e., not real mandated cybersecurity training) could mean that overall participants felt more autonomy than they would have under a real required training scenario. A future study could apply the same interview questions to real-world required training situation. The sample is self-selected and drawn from the students and staff of a large midwestern research university. Participants role as students and staff at a university limit the generalizability of their experiences and the results of the dissertation. Demographically the participants were majority white, 75% female, and 45% were between 18-24 years old (see the demographics section of the results chapter for complete demographic information collected). A larger and more diverse sample would generate more generalizable results. The Subjective Vitality Scale, the Learning Self-Regulation Questionnaire, and the Perceived Autonomy Support Questionnaire – Work Climate Questionnaire was each adapted to the cybersecurity training context for this dissertation and this adaptation introduce an opportunity for error. The Learning Self-Regulation Questionnaire was modified from a classroom context to a cybersecurity training context and the Perceived Autonomy Support Questionnaire – Work Climate Questionnaire was modified from a management context. These modifications for the cybersecurity context limit the results of these scales.

Chapter 7: Conclusion

This dissertation explores supporting wellbeing and autonomy through organizational cybersecurity communication. Organizations can suffer millions of dollars in damages due to cyberattacks. However, technical measures alone are insufficient to prevent cyberattacks, and human factors must also be considered. Thus, organizations engage in cybersecurity advocacy to prevent cybersecurity incidents. Cybersecurity awareness training seeks to influence and educate organizational users on cybersecurity concepts and best practices.

Research in cybersecurity motivation demonstrates that autonomy-based motivation using Self-Determination Theory (SDT) positively impacts cybersecurity compliance intentions. Motivation using SDT relies on supporting the three key psychological needs of autonomy, competence, and relatedness to generate intrinsic motivation. SDT posits that supporting basic psychological needs benefits wellbeing. Previous work concentrated on the compliance intentions of users when supported with SDT, this dissertation examines user experiences for elements of autonomy and wellbeing, the theoretical benefit of SDT-based motivation.

This dissertation moves beyond human factors to promote cybersecurity compliance by utilizing values-in-design. It modifies cybersecurity awareness training to encourage autonomy and wellbeing, aiming for users to view cybersecurity practices as a positive aspect of their lives rather than coercing them into compliance through heavy-handed tactics. Framing is employed to prevent participants from experiencing autonomy loss and to promote their wellbeing, as studies have revealed that cybersecurity is often linked with negative emotions for users.

We divided the participants into two groups where one group received an autonomy framed cybersecurity training document and the other group received a similar document without autonomy framing. To measure autonomy and wellbeing we administered the Subjective Vitality

Scale, the Learning Self-Regulation Questionnaire, and the Perceived Autonomy Support Questionnaire – Work Climate Questionnaire. Participants also answered open ended questions on their preferences around autonomy and how organizations could support their wellbeing in cybersecurity efforts. The interview allowed participants to review and compare both the autonomy framed cybersecurity document and non-autonomy document so they could offer their preferences.

Results of the Learning Self-Regulation Questionnaire suggest self-regulation may be impacted by autonomy framing in cybersecurity training documents; however, future studies require full statistical power to provide evidence of this. Participant responses to the open-ended interview questions do offer insight into the relationship between autonomy framing, cybersecurity, and wellbeing. Participants responses indicated the following themes:

1. Theme I: Participants Indicated Cybersecurity Training Should Include Contextual Information
2. Theme II: Participants Indicated Cybersecurity Training Should Treat Users in a Caring Manner
3. Theme III: Participants hold a Variety of Views on Negative Extrinsic Motivation
    a. Perspective: Repercussions are Necessary
    b. Perspective: Threats can Deter Compliance
4. Theme III-B: Participants Perceive Negative Extrinsic Motivation When None is Used
5. Theme IV: Participant Recognize Others' Communication Preferences
6. Theme V: Participant Believe Engaging in Cybersecurity Best Practices is a Personal Responsibility but Recognize that Employers are Mandating the Behavior
7. Theme VI: Some Participants View Autonomy Language Positively While Others Do Not

   a. Perspective: Autonomy Language Creates Positive Perceptions

   b. Perspective: Autonomy Language is Bad for Cybersecurity

8. Theme VII: Participants were Familiar with the Training Content and Indicated That This Increases Their Confidence

This dissertation's findings add substantial value to the current body of research on cybersecurity. Autonomy framing appears to support self-regulation and wellbeing among participants in some cases. Furthermore, participants value caring language Yet, this study indicates that autonomy framing does not produce autonomy in participants and instead prevents loss of autonomy. These results suggest participants feel autonomy in cybersecurity but not all prefer autonomy framing. There may be a divide around users who have internalized cybersecurity practice and those who have not.

Furthermore, our results offer insight into how the participants view communication in cybersecurity and how organizations can support their wellbeing. Providing contextual information and communicating in a compassionate manner could be advantageous for users. It's acknowledged by participants that organizational communication may not always align with their preferences as they recognize that their preferences are not universal. This indicates that users may be understanding when they receive cybersecurity communication.

Future studies using quantitative approaches should examine self-regulation while future qualitative studies should expand to larger demographics to gain more insights into cybersecurity communication and wellbeing. Further studies can explore what types of information users prefer, how it is presented, and why that information is useful. Studies can also identify users’ levels of internalization and explore how internalization of cybersecurity intersects with self-regulation and attitudes toward negative extrinsic motivation.

Works Cited

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248. https://doi.org/10/gfz22x

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). A phishing Mitigation Solution using Human Behaviour and Emotions that Influence the Success of Phishing Attacks. *Adjunct Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization*, 345–350. https://doi.org/10.1145/3450614.3464472

Actions Taken by Equifax And Federal Agencies in Response to The 2017 Breach. (2018). US Government Accountability Office. https://www.gao.gov/assets/gao-18-559.pdf

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, *26*(4), 276–289. https://doi.org/10/cjbt8x

Al-Hamdani, W. A. (2006). Assessment of need and method of delivery for information security awareness program. *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development - InfoSecCD '06*, 102. https://doi.org/10/dmtjwk

Almuqrin, A. (2019). *Examining the influence of technology acceptance, self-efficacy, and locus of control on information security behavior of social media users* (2019-23494-039). ProQuest Information & Learning.

Bandura, A. (1977). Self-efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review*, *84*(2), 25.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers and Security*, *39*, 145–159. https://doi.org/10/f5mx6h

Boss, S. R., Galletta, D. F., Benjamin Lowry, P., Moody, G. D., & Polak, P. (2015). What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors. *MIS Quarterly*, *39*(4), 837–864.

Bostic, T. J., McGartland Rubio, D., & Hood, M. (2000). A Validation of the Subjective Vitality Scale Using Structural Equation Modeling. *Social Indicators Research*, *52*(3), 313–324. https://doi.org/10.1023/A:1007136110218

Braun, V., & Clarke, V. (2012). Thematic analysis. In H. Cooper (Ed.), *Research designs* (Vol. 2, pp. 57–71). APA books.

Burns, A. J., Johnson, M. E., & Caputo, D. D. (2019). Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing & Electronic Commerce*, *29*(1), 24–39. https://doi.org/10/ggqpj5

Cacciatore, M. A., Scheufele, D. A., & Iyengar, S. (2016). The End of Framing as we Know it … and the Future of Media Effects. *Mass Communication and Society*, *19*(1), 7–23. https://doi.org/10.1080/15205436.2015.1068811

Camp, L. J. (2004). Mental Models of Computer Security. In A. Juels (Ed.), *Financial Cryptography* (Vol. 3110, pp. 106–111). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-27809-2_12

Chen, J., Gates, C. S., Li, N., & Proctor, R. W. (2015). Influence of risk/safety information framing on android app-installation decisions. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 149–168. https://doi.org/10/ggwmhd

Chen, J., Tian, Z., Cui, X., Yin, L., & Wang, X. (2019). Trust architecture and reputation evaluation for internet of things. *Journal of Ambient Intelligence and Humanized Computing*, *10*(8), 3099–3107. https://doi.org/10.1007/s12652-018-0887-z

Creswell, J. W., & Creswell, J. W. (2007). *Qualitative inquiry & research design: Choosing among five approaches* (2nd ed). Sage Publications.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Das, S., Kramer, A. D. I., Dabbish, L. A., & Hong, J. I. (2014). Increasing Security Sensitivity With Social Proof: A Large-Scale Experimental Confirmation. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 739–749. https://doi.org/10/ggwmdd

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

De Keukelaere, F., Yoshihama, S., Trent, S., Zhang, Y., Luo, L., & Zurko, M. E. (2009). Adaptive Security Dialogs for Improved Security Behavior of Users. In T. Gross, J. Gulliksen, P. Kotze, L. Oestreicher, P. Palanque, & R. O. Prates (Eds.), *Human-Computer Interaction—Interact 2009, Pt I* (Vol. 5726, pp. 510-+). Springer-Verlag Berlin.

Deci, E. L., Connell, J. P., & Ryan, R. M. (1989). Self-Determination in a Work Organization. *Journal of Applied Psychology*, *74*(4), 580. https://doi.org/10.1037/0021-9010.74.4.580

Dennis, A. R., & Minas, R. K. (2018). Security on Autopilot: Why Current Security Theories Hijack our Thinking and Lead Us Astray. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *49*(SI), 15–38. https://doi.org/10/gdg2q3

E. L. Deci & W. F. Casio. (1972, June). *Changes in intrinisc motivation as a function of negative feedback and threats.* Eastern Psychological Association, Boston, MA, USA.

Entman, R. M. (1993). Framing: Toward Clarification of a Fractured Paradigm. *Journal of Communication*, *43*(4), 51–58. https://doi.org/10.1111/j.1460-2466.1993.tb01304.x

Faizi, S. M., & Rahman, S. S. M. (2020). Effect of Fear on Behavioral Intention to Comply. *Proceedings of the 2020 the 4th International Conference on Information System and Data Mining*, 65–70. https://doi.org/10.1145/3404663.3404685

Gomm, R., Hammersley, M., & Foster, P. (2009). *Case Study Method*. SAGE Publications Ltd. https://doi.org/10.4135/9780857024367

Hancock, J. (2022). *Psychology of Human Error 2022 | Research Report*. tessian. https://www.tessian.com/resources/psychology-of-human-error-2022/

Huberman, A., & Miles, M. (2002). *The Qualitative Researcher's Companion*. SAGE Publications, Inc. https://doi.org/10.4135/9781412986274

Iyengar, S. (1994). *Is anyone responsible? How television frames political issues*. University of Chicago Press.

Jenkins, J. L., Anderson, B. B., Vance, A., Kirwan, C. B., & Eargle, D. (2016). More Harm Than Good? How Messages That Interrupt Can Make Us Vulnerable. *Information Systems Research*, *27*(4), 880–896. https://doi.org/10/f9jxgw

Johnston, A. (2020). A Replication Study of User Motivation in Protecting Information Security using Protection Motivation Theory and Self Determination Theory. *AIS Transactions on Replication Research*, *6*, 1–22. https://doi.org/10.17705/1atrr.00053

Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. (2019). Speak their Language: Designing Effective Messages to Improve Employees' Information Security Decision Making. *Decision Sciences; Atlanta*, *50*(2), 245–284. https://doi.org/10/ggvtk9

Kahneman, D. (2011). *Thinking fast and slow*. Farrar, Straus & Giroux.

Kam, H.-J., Menard, P., Ormond, D., & Crossler, R. E. (2020). Cultivating cybersecurity learning: An integration of self-determination and flow. *Computers & Security*, *96*, 101875. https://doi.org/10/ghz5vp

Kam, H.-J., Ormond, D. K., Menard, P., & Crossler, R. E. (2021). That's interesting: An examination of interest theory and self-determination in organisational cybersecurity training. *Information Systems Journal*, *n/a*(n/a). https://doi.org/10.1111/isj.12374

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Lee, V. C. (2015). *Examining the Relationship between Autonomy, Competence, and Relatedness and Security Policy Compliant Behavior* [Ph.D., Northcentral University]. http://search.proquest.com/docview/1746623306/abstract/D830B8CA778F4A70PQ/1

Levin, I. P., Schneider, S. L., & Gaeth, G. J. (1998). All Frames Are Not Created Equal: A Typology and Critical Analysis of Framing Effects. *Organizational Behavior and Human Decision Processes*, *76*(2), 149–188. https://doi.org/10.1006/obhd.1998.2804

Mackenzie, C. (2008). Relational Autonomy, Normative Authority and Perfectionism. *Journal of Social Philosophy*, *39*(4), 512–533. https://doi.org/10.1111/j.1467-9833.2008.00440.x

Mackenzie, C., & Stoljar, N. (2000). *Relational autonomy: Feminist perspectives on automony, agency, and the social self*. Oxford University Press. http://site.ebrary.com/id/10278562

McDermott, R. (2012). Privacy and Security: Emotion and Security. *Association for Computing Machinery. Communications of the ACM; New York*, *55*(2), 35. https://doi.org/10/fzwx2s

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems*, *34*(4), 1203. https://doi.org/10.1080/07421222.2017.1394083

Metrics & Methods: Questionnaires. (2021). Self-Determination Theory. https://selfdeterminationtheory.org/questionnaires/

O'Connor, C., & Joffe, H. (2020). Intercoder Reliability in Qualitative Research: Debates and Practical Guidelines. *International Journal of Qualitative Methods*, *19*, 1609406919899220. https://doi.org/10.1177/1609406919899220

Pagliery, C. R. and J. (2015, March 19). *Target will pay hack victims $10 million*. CNNMoney. https://money.cnn.com/2015/03/19/technology/security/target-data-hack-settlement/index.html

Parfit, D. (2011). *On What Matters: Volume One*. Oxford University Press. https://doi.org/10.1093/acprof:osobl/9780199572809.001.0001

Pelletier, L. G., Tuson, K. M., & Haddad, N. K. (1997). Client Motivation for Therapy Scale: A Measure of Intrinsic Motivation, Extrinsic Motivation, and Amotivation for Therapy. *J. Pers. Assess*, *68*(2), 414-435,. https://doi.org/10.1207/s15327752jpa6802_11

Perugini, M., & Bagozzi, R. P. (2001). The role of desires and anticipated emotions in goal-directed behaviours: Broadening and deepening the theory of planned behaviour. *British Journal of Social Psychology*, *40*(1), 79–98. https://doi.org/10.1348/014466601164704

Pettit, P. (1999). *Republicanism*. Oxford University Press. https://doi.org/10.1093/0198296428.001.0001

Press, A. A. (2018, August 22). Melbourne student health records posted online in “appalling” privacy breach. *The Guardian*. https://www.theguardian.com/australia-news/2018/aug/22/melbourne-student-health-records-posted-online-in-appalling-privacy-breach

Proctor, R. W., & Chen, J. (2015). The role of human factors/ergonomics in the science of security: Decision making and action selection in cyberspace. *Human Factors*, *57*(5), 721–727. https://doi.org/10/f7kz7m

Reeves, A., Calic, D., & Delfabbro, P. (2021). “Get a red-hot poker and open up my eyes, it’s so boring”1: Employee perceptions of cybersecurity training. *Computers & Security*, 102281. https://doi.org/10.1016/j.cose.2021.102281

Renaud, K., Zimmermann, V., Schürmann, T., & Böhm, C. (2021). Exploring cybersecurity-related emotions and finding that they are challenging to measure. *Humanities and Social Sciences Communications*, *8*(1), 75. https://doi.org/10.1057/s41599-021-00746-5

Rosenberg, B. D., & Siegel, J. T. (2018). A 50-year review of psychological reactance theory: Do not read this article. *Motivation Science*, *4*(4), 281–300. https://doi.org/10.1037/mot0000091

Rubel, A., Castro, C., & Pham, A. (2020). *Algorithms & Autonomy: The Ethics of Automated Decision Systems*. Cambridge University Press.

Ryan, R. M., author. (2017). *Self-determination theory: Basic psychological needs in motivation, development, and wellness*. The Guilford Press, [2017]. https://search.library.wisc.edu/catalog/9912336946102121

Ryan, R. M., & Frederick, C. (1997). On Energy, Personality, and Health: Subjective Vitality as a Dynamic Reflection of Well-Being. *Journal of Personality*, *65*(3), 529–565. https://doi.org/10.1111/j.1467-6494.1997.tb00326.x

Saldana, J. (2015). *The Coding Manual for Qualitative Researchers* (3rd ed.). Sage Publications.

Scheufele, B. T., & Scheufele, D. A. (2009). Of Spreading Activation, Applicability, and Schemas. In *Doing News Framing Analysis Empirical and Theoretial Perspectives* (p. 25). Routledge.

Scheufele, D. (1999). Framing As a Theory of Media Effects. *The Journal of Communication*, *49*, 103–122. https://doi.org/10.1111/j.1460-2466.1999.tb02784.x

Scheufele, D. A., & Iyengar, S. (2014). *The State of Framing Research* (K. Kenski & K. H. Jamieson, Eds.; Vol. 1). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199793471.013.47

Scheufele, D. A., & Tewksbury, D. (2007). Framing, Agenda Setting, and Priming: The Evolution of Three Media Effects Models: Models of Media Effects. *Journal of Communication*, *57*(1), 9–20. https://doi.org/10.1111/j.0021-9916.2007.00326.x

Sobers, R. (2019, November 20). *110 Must-Know Cybersecurity Statistics for 2020 | Varonis*. Inside Out Security. https://www.varonis.com/blog/cybersecurity-statistics/

Spring, T. (2021, May 8). *Major U.S. Pipeline Crippled in Ransomware Attack*. Threatpost; Newstex. http://www.proquest.com/docview/2523191730/citation/296F785C41064FDCPQ/1

Strempfl, J., Wutzl, T., Ün, D., Greber-Platzer, S., Keilani, M., Crevenna, R., & Thajer, A. (2022). Impact of self-determination theory in a physiotherapeutic training: A pilot-study on motivation for movement of obese adolescents. *Wiener Klinische Wochenschrift*, *134*(5–6), 208–214. https://doi.org/10.1007/s00508-021-01849-4

Susser, D., Roessler, B., & Nissenbaum, H. F. (2018). Online Manipulation: Hidden Influences in a Digital World. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3306006

Tafvelin, S., & Stenling, A. (2021). A Self-Determination Theory Perspective on Transfer of Leadership Training: The Role of Leader Motivation. *Journal of Leadership & Organizational Studies*, *28*(1), 60–75. https://doi.org/10.1177/1548051820962504

The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. (n.d.). https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. *Computers & Security*, *79*, 68–79. https://doi.org/10/gfh9xn

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science*, *211*(4481), 453–458. https://doi.org/10.1126/science.7455683

Usability & human factors. (2016). In *NIST*. https://www.nist.gov/topics/usability-human-factors

van der Vossen, B. (2019). Libertarianism. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Spring 2019). Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/spr2019/entries/libertarianism/

Vansteenkiste, M., Simons, J., Lens, W., Sheldon, K. M., & Deci, E. L. (2004). Motivating Learning, Performance, and Persistence: The Synergistic Effects of Intrinsic Goal Contents and Autonomy-Supportive Contexts. *J. Pers. Soc. Psychol*, *87*(2), 246-260,. https://doi.org/10.1037/0022-3514.87.2.246

Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-Related Motivations and Information Security Policy Compliance: The Role of Autonomy and Efficacy. *Journal of Information Privacy & Security*, *9*(4), 52–79. https://doi.org/10.1080/15536548.2013.10845690

What is Cybersecurity? (2019). [Government Website]. Cybersecurity & Infrastructure Security Agenecy. https://www.cisa.gov/stopthinkconnect-toolkit

Williams, G. C., Cox, E. M., Kouides, R., & Deci, E. L. (1999). Presenting the facts about smoking to adolescents: Effects of an autonomy-supportive style. *Archives of Pediatrics & Adolescent Medicine*, *153*(9), 959–964. https://doi.org/10.1001/archpedi.153.9.959

Williams, G. C., Grow, V. M., Freedman, Z. R., Ryan, R. M., & Deci, E. L. (1996). *Motivational Predictors of Weight Loss and Weight-Loss Maintenance*. 12. https://doi.org/10.1037//0022-3514.70.1.115

Yaokumah, W., Walker, D. O., & Kumah, P. (2019). SETA and Security Behavior: Mediating Role of Employee Relations, Monitoring, and Accountability. *Journal of Global Information Management*, *27*(2), 102–121. https://doi.org/10/ggh85d

Appendices

Scales

Vitality Scale

Please respond to each of the following statements in terms of how you are feeling right now. Indicate how true each statement is for you at this time, using the following scale:

1 2 3 4 5 6 7
not at all true somewhat true very
true

1. At this moment, I feel alive and vital.
2. I don't feel very energetic right now.
3. Currently I feel so alive I just want to burst.
4. At this time, I have energy and spirit.
5. I am looking forward to each new day.
6. At this moment, I feel alert and awake.
7. I feel energized right now.

Self-Regulation Questionnaire

The following statements are about your perception of cybersecurity training. For each of the following statements, please indicate your agreement/disagreement, using the following scale:

1 2 3 4 5 6

7

not at all true somewhat true very true

A. I will participate actively in the Cybersecurity Training:

1. Because I feel like it's a good way to improve my skills and my understanding of cybersecurity.
2. Because others would think badly of me if I didn't.
3. Because learning to protecting against cyberthreats is an important part of being a professional.
4. Because I would feel bad about myself if I didn’t read this information.

B. I am likely to follow the cybersecurity training’s suggestions for cybersecurity:

5. Because I will get a reward if I do what the cybersecurity training suggests.
6. Because I believe the cybersecurity training’s suggestions will help me protect against cyberthreats.
7. Because I want others to think that I have good cybersecurity habits.
8. Because it's easier to do what I'm told than to think about it.
9. Because it's important to me to do well at this.
10. Because I would probably feel guilty if I didn't comply with the cybersecurity training’s suggestions

C. The reason that I will continue to broaden my cybersecurity skills is:

11. Because it's exciting to try new ways to protect against cyberthreats.
12. Because I would feel proud if I did continue to improve my cybersecurity skills.
13. Because it's a challenge to really understand how to protect against cyberthreats.
14. Because it’s interesting

Autonomy Support Questionnaire

The following statements are about your perception of the training content you have been provided. For each of the following statements, please indicate your agreement/disagreement, using the following scale:

1 2 3 4 5 6 7
strongly disagree neutral strongly agree

1) I feel that the document provides me choices and options.
2) I feel understood by the document.
3) I feel I am able to be open with the document's author.
4) The document conveyed confidence in my ability to do well at managing my cybersecurity.
5) I feel that the document's author accepts me.
6) The document made sure I really understood the goals of my role in cybersecurity and what I need to do.
7) The document encouraged me to ask questions.
8) I feel a lot of trust in the document's author.
9) The document answers my questions fully and carefully.
10) The document's author listens to how I would like to do things.
11) The document handles people's emotions very well.
12) I feel that the document's author cares about me as a person.
13) I don't feel very good about the way the document talks to me.
14) The document tries to understand how I see things before suggesting a new way to do things.
15) I feel able to share my feelings with the document's author.

Notes

Note regarding results: A technical issue caused the recording of one participant to record only silence thus all results reflect the results of the 19 interviews that were recorded, transcribed, and analyzed. The interviewer reports that the missing interview did not notably deviate from the other interviews and the interview was in the non-autonomy group.

Note regarding results: Means and p-values included in this document are rounded to two decimal places.

Statistical Test Results for Scales

Vitality Score

t-Test: Two-Sample Assuming Unequal Variances

	Autonomy	*Non-Autonomy*
Mean	5.55357143	4.83116883
Variance	0.76639942	1.20742115
Observations	8	11
Hypothesized Mean Difference	0	
df	17	
t Stat	1.59332437	
P(T<=t) one-tail	0.06475471	
t Critical one-tail	1.73960673	
P(T<=t) two-tail	0.12950942	
t Critical two-tail	2.10981558	

Regulation-Autonomous

t-Test: Two-Sample Assuming Unequal Variances

	Autonomy	*Non-Autonomy*
Mean	5.35	5.03030303
Variance	1.40539683	1.00454545
Observations	8	11
Hypothesized Mean Difference	0	
df	14	
t Stat	0.61870752	
P(T<=t) one-tail	0.27302243	
t Critical one-tail	1.76131014	
P(T<=t) two-tail	0.54604486	
t Critical two-tail	2.14478669	

Regulation-Controlled

t-Test: Two-Sample Assuming Unequal Variances

	Autonomy	*Non-Autonomy*
Mean	3.33928571	4.4025974
Variance	1.24161808	1.01150278
Observations	8	11
Hypothesized Mean Difference	0	
df	14	
t Stat	-2.1388192	
P(T<=t) one-tail	0.02527912	
t Critical one-tail	1.76131014	
P(T<=t) two-tail	0.05055824	
t Critical two-tail	2.14478669	

Self-Regulation-Relative

Index

t-Test: Two-Sample Assuming Unequal Variances

	Autonomy	*Non-Autonomy*
Mean	2.01071429	0.62770563
Variance	1.7715047	1.15241187
Observations	8	11
Hypothesized Mean Difference	0	
df	13	
t Stat	2.42148094	
P(T<=t) one-tail	0.01540972	
t Critical one-tail	1.7709334	
P(T<=t) two-tail	0.03081944	
t Critical two-tail	2.16036866	

Perceived Autonomy

t-Test: Two-Sample Assuming Unequal Variances

	Autonomy	*Non-autonomy*
Mean	4.48333333	4.05333333
Variance	2.67015873	0.56079012
Observations	8	10
Hypothesized Mean Difference	0	
df	9	
t Stat	0.68868453	
P(T<=t) one-tail	0.25419196	
t Critical one-tail	1.83311293	
P(T<=t) two-tail	0.50838392	
t Critical two-tail	2.26215716	

*One participant removed from non-autonomy group analysis because of data collection error

Training documents

*Differences between documents are highlighted

Non-Autonomy Document

What is Cybersecurity?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. How much of your personal information is stored either on your own computer, smartphone, tablet or on someone else's system?

To minimize the risks of cyberattacks, follow basic cybersecurity best practices:

- **Keep software up to date**. Install software patches so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.

- **Run up-to-date antivirus software**. A reputable antivirus software application is an important protective measure against known malicious threats. It can automatically detect, quarantine, and remove various types of malware. Be sure to enable automatic virus definition updates to ensure maximum protection against the latest threats. Note: Because detection relies on signatures—known patterns that can identify code as malware—even the best antivirus will not provide adequate protections against new and advanced threats, such as zero-day exploits and polymorphic viruses.

- **Use strong passwords**. Select passwords that will be difficult for attackers to guess, and use different passwords for different programs and devices. It is best to use long, strong passphrases or passwords that consist of at least 16 characters.

- **Change default usernames and passwords**. Default usernames and passwords are readily available to malicious actors. Change default passwords, as soon as possible, to a sufficiently strong and unique password.

- **Implement multi-factor authentication (MFA)**. Authentication is a process used to validate a user's identity. Attackers commonly exploit weak authentication processes. MFA uses at least two identity components to authenticate a user's identity, minimizing the risk of a cyberattacker gaining access to an account if they know the username and password.

- **Install a firewall.** Firewalls may be able to prevent some types of attack vectors by blocking malicious traffic before it can enter a computer system, and by restricting unnecessary outbound communications. Some device operating systems include a firewall. Enable and properly configure the firewall as specified in the device or system owner's manual.

- **Be suspicious of unexpected emails**. Phishing emails are currently one of the most prevalent risks to the average user. The goal of a phishing email is to gain information about you, steal money from you, or install malware on your device. Be suspicious of all unexpected emails.

If you have any questions email: cyber@alpha.com

Autonomy Document

What is your role in Cybersecurity?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use. Cybersecurity relies on the decisions you make every day. You contribute to the cybersecurity of our organization, and your choices make a difference.

As you review some cybersecurity best practices, consider how you support the cybersecurity of the organization:

- **Keep software up to date.** You can install software patches so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates and enabling this option gives you control over your cybersecurity with less effort.

- **Run up-to-date antivirus software**. A reputable antivirus software application is an important protective measure against known malicious threats. It can automatically detect, quarantine, and remove various types of malware. You can enable automatic virus definition updates to maximize your protection against the latest threats. Note: Because detection relies on signatures—known patterns that can identify code as malware—even the best antivirus will not provide adequate protections against new and advanced threats, such as zero-day exploits and polymorphic viruses.

- **Use strong passwords.** If you select passwords that will be difficult for attackers to guess and use different passwords for different programs and devices, you are controlling how easy or hard it is for your information to be accessed by attackers. You can choose how to build your password, such as:
  - Use special characters, capital, and lowercase letters
  - Use a passphrase of at least 16 characters

- **Change default usernames and passwords** Default usernames and passwords are readily available to malicious actors. Changing default passwords, as soon as possible with a sufficiently strong and unique password lets you prevent others from getting into your account.

- **Implement multi-factor authentication (MFA).** Authentication is a process used to validate a user's identity. Attackers commonly exploit weak authentication processes. MFA lets you require at least two identity components to authenticate your identity, minimizing the risk of a cyberattacker gaining access to an account if they know the username and password.

- **Install a firewall.** Firewalls may be able to prevent some types of attacks. Firewalls let you control what connections are allowed to your computer. Some device operating systems include a firewall. You can enable and properly configure the firewall by referring to the device or system owner's manual.

- **Be suspicious of unexpected emails.** Unexpected emails are often attackers trying to trick you. Phishing emails are currently one of the most prevalent risks to the average user. The goal of a phishing email is to gain information about you, steal money from you, or install malware on your device. Being suspicious of all unexpected emails lets you minimize the likelihood of being tricked.

If you have any questions or anything to share about, the Office of Cybersecurity can be reached at the following email: cyber@alpha.com

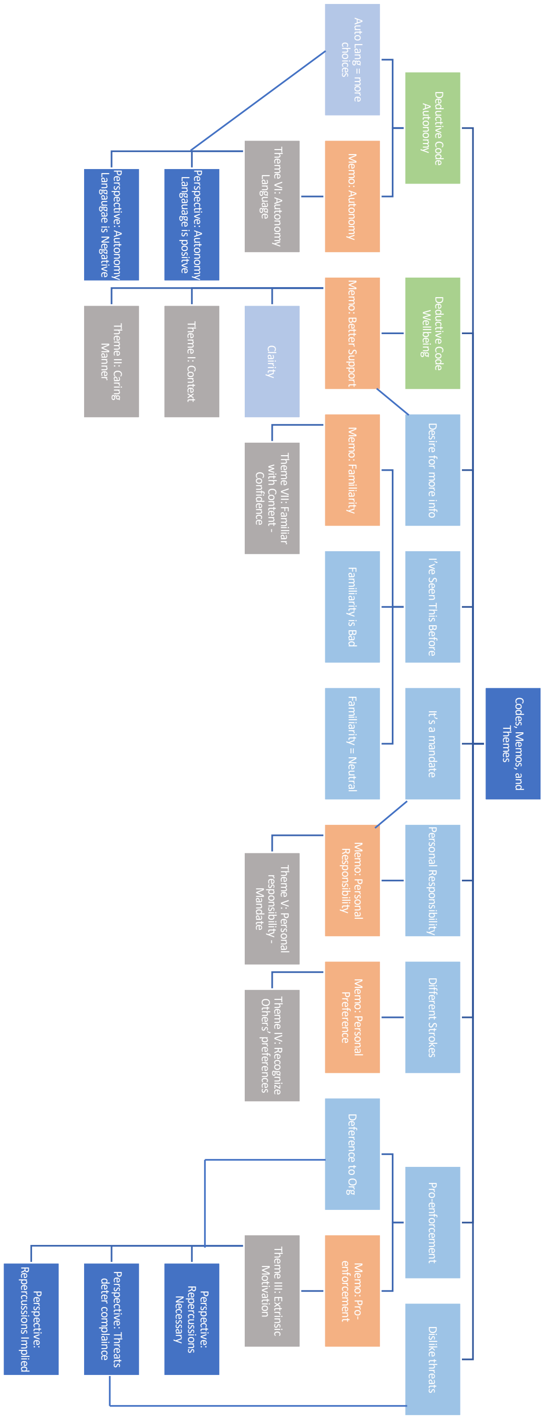
Codes, Memos, and Themes
Deductive Code Autonomy
Auto Lang = more choices
Memo: Autonomy
Theme VI: Autonomy Language
Perspective: Autonomy Langauage is positve
Perspective: Autonomy Langaugae is Negative
Deductive Code Wellbeing
Memo: Better Support
Clairity
Theme I: Context
Theme II: Caring Manner
Desire for more info
Memo: Familiarity
Theme VII: Familiar with Content - Confidence
I've Seen This Before
Familiarity is Bad
It's a mandate
Familiarity = Neutral
Personal Responsibility
Memo: Personal Responsibility
Theme V: Personal responsibility - Mandate
Different Strokes
Memo: Personal Preference
Theme IV: Recognize Others' preferences
Deference to Org
Pro-enforcement
Memo: Pro-enforcement
Theme III: Extrinsic Motivation
Perspective: Repercussions Necessary
Perspective: Threats deter complaince
Perspective: Repercussions Implied
Dislike threats

Figure 2: Code, Memo, and Theme Hierarchical Relationships and Theme Development

Glossary

Autonomy – A perception that one is in control of their behavior and governing their own life.

Autonomous Regulation- a measure of identified and integrated regulation

Framing – The alteration of words and emphasis to alter the reception of a piece of media.

CAT – **Cybersecurity Awareness Training** – a training program aimed to increase cybersecurity behavior in organizational users to prevent security incidents.

Controlled Regulation- a measure of external and introjected regulation

Competence – a perception that one is capable of accomplishing tasks.

Cybersecurity Behavior – Behaviors, actions, and decisions that supports the cybersecurity goals of an individual or organization.

Cybersecurity Incident – A negative event where the cybersecurity of an entity is compromised.

Cybersecurity Practice – The routine decisions users make to maintain the security of information and information systems.

External Regulation- regulation that occurs when the perception of an external contingency motivates behavior.

Identified Regulation - regulation that occurs when a person consciously endorses regulations or values.

Integrated Regulation - regulation that occurs when a person actively and in a transformative manner brings a value or regulation into congruence with other aspects of oneself.

Introjected Regulation - regulation that occurs when a person adopts or takes in a regulation or value with incomplete assimilation.

OIT- Organismic Integration Theory - a mini-theory of SDT that provides a framework of extrinsic motivation.

Professional – A person who in a given activity receives payment for their efforts. Sometimes includes pre-professionals.

Pre-Professional - a person who will be seeking to receive payment for their efforts within 2 years.

Relatedness – A perception that one is connected to others, and they share experiences.

SDT - Self-Determination Theory - a theory that states the three basic psychological needs are autonomy, competence, and relatedness and that supporting these needs leads to wellness.

Self-Regulation- Experienced autonomy – An expression of autonomy with the locus of control coming from within a person.

Training Content – Content that is instructive in nature and provides information about a subject. Training content is an artifact found in a training.

Wellness – a positive state of being where a person is vital, energetic, and self-regulating. A fully functioning person.