The Human Reaction to Organizational Cyber Threats in a K-12 Institution

A Dissertation

Presented to the Faculty of

Millersville University and Shippensburg University

In Partial Fulfillment

of the Requirements for the Degree of

Doctor of Education

By

John-Paul Franzen

April 2024

Title of Dissertation:

The Human Reaction to Organizational Cyber Threats in a K-12 Institution

Candidate: **John-Paul Franzen**

__ Approved
__ Approved with Conditions
__ Not Approved

SHIPPENSBURG UNIVERSITY *

_____* _____
Committee Chair, Dr. Oliver Dreon, Millersville University

_____* _____
Committee Member, Dr. Wendy Kubasko, Shippensburg University

MILLERSVILLE UNIVERSITY

_____* _____
Committee Member, Dr. Theresa Russell-Loretz, Millersville University

**Signatures on file in the College of Graduate Studies and Adult Learning*

DATE: April 2024

Submitted in partial fulfillment of the requirements for the Degree of Doctor of Education.
***Indicates University of Admission**
Notes/Comments:

Dedication

K-12 schools are constantly under the threat of cyber attacks from outside threat actors, and the IT teams in these organizations are working diligently behind the scenes to ensure that schools continue to function. Digital technology permeates all aspects of modern K-12 institutions, and the IT teams make sure that schools' infrastructures can support a continuity of education so that all students can achieve their greatest potential. This study is dedicated to all of the K-12 IT teams that are providing the foundation for 21st century learning.

Acknowledgements

There are countless people who have made this journey possible- some overtly and some surreptitiously. Standing out in front of those who have shaped this experience, I would like to express my sincerest gratitude to Dr. Oliver Dreon. His guidance and feedback pushed me to think about the research in new ways, and his commitment to excellence elevated my study to higher levels. I would also like to thank my committee members, Dr. Wendy Kubasko of Shippensburg University, and Dr. Theresa Russell-Loretz of Millersville University for dedicating their time and expertise to help shape this academic endeavor. Furthermore, I would like to thank Charlie Reisinger of the Penn Manor School District for sharing his knowledge as a content expert during this study.

Sharing a common experience with others helps to carry us through the times when we doubt ourselves, and I cannot thank Cohort 8 of the Millersville University and Shippensburg University doctoral program in Educational Leadership enough for applying that gentle pressure to keep me moving forward. I want to express the same thanks to my professional colleagues who offered their understanding, words of encouragement, and their insights. A special thanks to Dr. Katie Kennedy-Reilly who has functioned as a role model in my professional career and has encouraged me to grow as both a leader and an academic.

Finally, I would like to thank my family for being accepting of the times when I wasn't present mentally because my mind was focused on the dissertation, and especially my wife Brandi, who navigated the emotional twists and turns of the process with me. Without your support, I would not have been able to see this through to the end.

Abstract

The use of digital technology continues to expand in K-12 public schools, creating potential security vulnerabilities for district networks. As technology use grows, K-12 institutions have seen an increase in cyber attacks, which can have a profound impact on stakeholders in the organization. The purpose of this study was to examine how K-12 Information Technology (IT) administrators, those closest to the attack, experienced a cyber attack and how it impacted their security processes and policies. A case study methodology, including interviews and artifact collection, was used to understand the lived experience of the participants, and themes emerged from inductive coding of the data. Regarding how K-12 IT administrators experienced a cyber attack, data revealed the themes of "Nobody's Seen Something Like This Before," and "The End". Participants described their experience during the cyber attack as unlike anything they had encountered before, and all participants had different perspectives on when they considered the attack over. Relating to how experiencing a cyber attack impacted the cybersecurity policies and processes of the IT administrators, the themes of "Finding a Voice" and "Trust Nothing" emerged from the data. Participants shared that after experiencing a cyber attack they found a voice both internally within the department and externally with other departments in the school district. Participants also expressed that after the attack, they did not trust that they were ever safe from potential cyber threats. This study has implications for K-12 IT administrators, as well as other K-12 district leaders. Implications for K-12 administrators include fostering effective communication with IT administrators during a cyber attack, and proactively promoting communication between IT administrators, between IT administrators and other departments in the school district, and between school districts that have experienced an attack and those that have not. In addition, the study highlights the need to

support the mental health of K-12 IT administrators after an attack, maintaining robust cybersecurity measures to protect school districts, and the potential importance of collective efficacy in core IT team decision making after a cyber attack. This study adds to the limited research on how K-12 IT administrators experience a cyber attack, and additional research is needed to further understand how IT administrators, district leaders, staff, and students experience a cyber threat.

TABLE OF CONTENTS

Chapter 1: Introduction

It was four days into the start of school, and students and staff were home enjoying the Labor Day weekend. The Fern Valley School District had already distributed all the student laptops, but due to a shipping delay, the new teacher devices had not arrived yet. The technology director had resigned the prior December, and up to this point, the District was unable to find a suitable replacement, so the position remained vacant. Saturday morning was the first indication something was wrong. A staff member submitted a help desk ticket because they were unable to access a document on their desktop, and it appeared all their files now had an unusual extension added to the file name. It wasn't until Sunday afternoon that the network administrator realized that this issue wasn't confined to a single laptop, and the unusual extension appeared on most district devices. This included not just staff and student-issued devices, but also all the servers that housed everything from student information to HVAC controls. Nothing housed on a district device was accessible. It was on Sunday night, with three other members of the IT team watching helplessly through the large glass window that separated the rooms, that the network administrator removed any connections from the District to outside networks. In a large room, tucked into a dark corner of one of the middle schools that few in the district even knew existed, the District's technology center was isolated and silent, held captive by an outside threat actor. Students would return to buildings in less than 36 hours, and the District could not trust any of the digital systems that supported the day-to-day operations of learning.

With an increase of digital devices and digital systems to support public education in the United States, cyber attacks on schools are becoming more prevalent, taxing the resources of school districts, and impacting the education of students (Castelo, 2020). While K-12 institutions have expanded the use of digital devices since the early 1980s, the COVID-19 pandemic

accelerated the adoption of 1:1 programs and also changed how educators view education. In March of 2020, the COVID-19 pandemic forced many students into virtual or distance learning for the conclusion of the 2019-20 school year (United Nations, 2020). As schools moved into the 2020-21 school year, many students still participated in some form of virtual instruction where students would access instruction either synchronously or asynchronously from locations outside a school district's network. While education transitioned to online environments, many teachers had little to no experience teaching virtually or supporting students through digital mediums (Gudmundsdottir & Hathaway, 2020). In addition to potential security vulnerabilities that existed before the COVID-19 pandemic, the increase in devices and virtual learning during the pandemic expanded cybersecurity threats. The increase in threats was related to more students who lacked cybersecurity knowledge had access to devices, more students used school devices on under-protected home networks, and more students used new digital programs for virtual instruction that were un-vetted for safety (Saleous et al., 2022).

Prior to the COVID-19 pandemic, cyber-related crime on organizations was already on the rise; however, the large-scale adoption of 1:1 programs, unsecured home networks, unvetted apps, and a lack of cybersecurity knowledge provided additional opportunities for threat actors. Given these potential vulnerabilities, cyber attacks on organizations, including K-12 institutions, became more prevalent during the pandemic (Castelo, 2020). The increase in attacks prompted the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and the UK's National cybersecurity Centre to issue a warning in 2020 stating that "malicious cyber actors are adjusting their tactics to exploit the COVID-19 pandemic" and "it is expected that the frequency and severity of COVID-19 related cyber attacks will increase over the coming weeks and months" (CISA, 2021b, para. 17). Despite this announcement, the FBI estimated that

the total losses due to cyber crime increased from $4.2 billion in 2020 to $6.9 billion in 2021, and $10.2 billion in 2022 (FBI, 2022a).

While threat actors target digital devices for cyber crime, human beings are the biggest vulnerability to any organization's cybersecurity (McMahon, 2020; Proctor & Chen, 2015). Despite this vulnerability, institutions often do not address the indirect impacts on stakeholders after a cyber attack, even though there can be profound psychological and behavioral implications because of an attack (Bada & Nurse, 2018; Gross et al., 2017; Minei & Matusitz, 2011). The experience of an attack and the ongoing cybersecurity behaviors of individuals can have serious implications on the future safety of a school district's technology infrastructure, and it is important that schools understand how stakeholders, specifically technology-related staff, experience a cyber attack.

Statement of the Problem and Purpose of the Study

As K-12 organizations expand the number of low-cost digital devices that access their networks, they offer additional vulnerabilities for potential hackers to exploit the network for personal gain. This proliferation of vulnerabilities, coupled with the increase in number of hackers, has created a scenario where "security experts are locked in a deadly race with these malicious hackers that at the moment looks like a losing battle with the security community" (Kizza, 2012, p. 67). Even though there is a continual escalation of attacks on organizations, there is minimal research on how security experts experience cyber events and even less that examine how K-12 Information Technology (IT) professionals experience a cyber attack.

The purpose of this study was to examine the experiences of public school IT administrators after going through a cyber attack to help promote the overall cyber safety of a school district. By exploring their experiences, this study contributes to an understanding of how

IT administrators navigate challenges in the K-12 public school setting after an attack and can help inform strategies to enhance cyber safety measures. Each member of an IT administrative team is unique and "every stakeholder may perceive or experience harm differently, and the consequences of cyber attacks should be assessed based on their views, resulting in the existence of different 'lenses' to examine cyber harm" (Agrafiotis et al., 2018, p.13). Understanding the context, practices, and experiences of individuals in a specific school district in the aftermath of a cyber attack can provide valuable insights for school leaders and learning communities as they encounter similar situations and make informed decisions to protect their school communities.

Significance of the Problem

Public schools continue to become more reliant on digital devices. From 1981 to 1991, the number of schools that utilized computers for education went from 18% to 98%, and the number of students per computer went from 125 students per computer to 18 students per computer (Cuban, 1993). The adoption of computers in K-12 education continued to grow at a steady pace during the 1990s and 2000s; however, the COVID-19 pandemic in 2020 accelerated the adoption of 1:1 computer programs in schools. In 2022, 90% of school districts reported that they were providing a device for every middle school and high school student, and 84% reported they were providing a device for every elementary student (Bushweller, 2022). Given the limited budgets of school districts, districts will often purchase low-cost devices over business-class laptops to minimize costs and maximize the number of devices in the classroom (Topper & Lancaster, 2013). In addition to the adoption of 1:1 devices in public education, schools have also increased the use of the Internet for instruction since it went public in 1993 (Ring, 2023).

To maximize the impact of the Internet and educational technology, schools "must find ways to design, fund, acquire, and maintain the infrastructure that will make connectivity a

reality for every teacher and student in every learning environment" (U.S. Department of Education, 2017, p.3). To accomplish connectivity across different environments, organizations, including K-12 institutions, design computer networks where multiple computers are connected either by cables or Wi-Fi for the purpose of sharing data (IBM, n.d.-a). While a network allows students and teachers to share information across devices, it can also allow outside threat actors to access devices connected to the larger network.

Threat actors can access organizational networks through different methods including malware, which includes viruses, spyware, ransomware, and any other software installed secretly on a user's device (Federal Trade Commission, 2022) or using malware-free methods like stolen usernames and passwords. In 2022, malware-free attacks accounted for 71% of all cyber crime activity, and once a device was compromised, it took an average of 84 minutes for a threat actor to infect other devices on the same network (Crowdstrike, 2023). An increase of non-malware credential-based attacks highlights how humans are the greatest vulnerability to an organizational network (McMahon, 2020). As more individuals have access to devices in an organization, there is a greater potential for security failures.

Even though the number of reported cyber-related incidents continues to increase (Castelo, 2020), the number of reported attacks potentially does not represent the true number and severity of cyber attacks since cyber events are often under-reported by organizations (Cashell et al., 2004). Even when cyber events are reported, communication can contain ambiguous information given the difficulties in relating the comprehensive impact of an attack (van Zedlhoff, 2016; Watkins, 2014; Zhang et al. 2018). Downtime, organizational reputation, employee retention, and stakeholder morale are all indirect impacts of a cyber attack that make it difficult for organizations to quantify the true impact of a cyber attack beyond direct fiscal

expenditures (Furnell et al., 2015). Often institutions do not accurately address indirect impacts, which can lead to future issues related to cybersecurity and increased vulnerabilities to future cyber crime.

When an individual is a victim of traditional crime such as assault or burglary, it can negatively impact occupational functioning, social functioning, life satisfaction, and well-being (Hanson et al., 2010). In addition, crime can also lead to posttraumatic stress disorder (PTSD), increased levels of vulnerability and fear, and lower levels of self-efficacy (Kilpatrick et al., 1987; Lurigio, 1987). Although researchers have examined the negative lasting effects of traditional crime on individuals, there is a lack of research regarding the human impact of cyber crime, even though the prevalence of cyber attacks continues to increase every year. Also, the potential impact of crime on an individual's perceived vulnerability and self-efficacy could influence an individual's cybersecurity decisions (Liang and Xue, 2009). Since humans are the greatest vulnerability to a school district's network, all stakeholders, especially IT team members, need to make effective decisions regarding cybersecurity.

In any organization, only a limited number of people have a comprehensive understanding of a cybersecurity incident (Stacey et al., 2021) and in the K-12 environment, this is often the IT administrators for the school district. In addition to IT administrators having the greatest knowledge of a cyber event, recovery efforts and the long-term cybersecurity of the school district after an attack are also directly tied to their decisions. With the successful implementation of cybersecurity measures at stake, it is imperative that school districts understand how their IT administrators are impacted by a cyber event and how it influences their security decisions.

Theoretical Framework

This study utilized the Technology Threat Avoidance Theory (TTAT) (Liang and Xue, 2009). TTAT is rooted in cybernetic theory (Weiner, 2019) where individuals undertake actions to distance themselves from a negative end-state to minimize potential harm. In the case of TTAT, Liang and Xue identified two initial processes that interact to determine how individuals cope with cyber threats. The first process includes a threat appraisal where an individual analyzes how susceptible they are to a cyber threat and the potential severity of the cyber threat. The second process includes a coping appraisal where an individual analyzes the potential that they have to avoid a cyber threat based on the perceived effectiveness of available countermeasures, the perceived cost of implementing countermeasures, and one's self-efficacy, or perception that they have the ability to avoid or address the cyber threat. In addition to a threat appraisal and coping appraisal, individuals' decisions are also impacted by their risk tolerance and social influences. Based on one's threat appraisal, coping appraisal, risk tolerance, and social influence, an individual will either utilize problem-focused coping, and implement actions to address the cyber threat or implement maladaptive coping responses that include denial, fatalism, wishful thinking, and hopelessness (Milne et al. 2000). TTAT offered a researched based framework for this study regarding how individuals perceive cybersecurity threats and implement actions to mediate their impact. Given that TTAT provides a framework that outlines decision-based actions that are influenced by individual perceptions and experiences, I used the components of the framework to aid in the development of interview questions to understand the experience of IT administrators who have experienced a cyber attack, and their decision-making processes. In addition, TTAT provided a broad framework for interpreting results during data analysis.

Research Questions

While there are numerous studies that focus on the impact cyber attacks have on larger private institutions and college-aged groups, there is a lack of research in the public K-12 setting. Furthermore, outside of Stacey et al. (2021), research does not address the personal impact on IT administrators, let alone K-12 IT administrators. This study adds to the research on the impact of cyber threats in the K-12 setting and the impact on K-12 IT administrators by addressing the following questions:

- How do K-12 IT administrators describe their experiences with a cyber attack within their district?
- How do K-12 IT administrators see a cyber attack as influencing current practices and policies?

Overview of the Study

This qualitative case study took place in the Fern Valley School District (FVSD), a pseudonym. FVSD is a mid-sized K-12 suburban school district that serves approximately 6,200 students in kindergarten through twelfth grade. This study was limited to the timeframe from September 2019, when a district-wide cyber event occurred, until the time of data collection in late 2023/early 2024. The study utilized purposive sampling to focus specifically on the personal impact the district-wide cyber event had on IT administrators in the District. The participants of this study were six of the core IT team of administrators. I selected these participants since they were employed by FVSD at the time of the study and were also employed by FVSD during the cyber attack that occurred in 2019. This sample included the director of technology, technology supervisor, network administrator, digital media specialist, web/communication specialist, device

manager, and technical support specialist. The mix of positions, all Act 93 administrative positions, provided input from all areas of a school district's technology infrastructure.

After IRB approval, I asked all participants to voluntarily participate in two semi-structured interviews that each took approximately 45 minutes. I recorded and transcribed all interviews, as well as took notes during each meeting. In addition to interviews, I collected news articles and other documents related to the cyber attack. During data collection, I kept a reflective journal as a means of bracketing, which helped me identify my own preconceived perspectives related to the research (Ahern, 1999; Chan et al., 2013; Tufford & Newman, 2012). After completing data collection, I began coding the interview transcripts to inductively identify themes that emerged from the responses. Concurrently, I utilized Atlas.ti, an artificial intelligence-based software, to identify themes to act as a comparison to manually identified themes.

Limitations of the Study

There are several limitations regarding the study that are of importance. Given the site-specific qualitative data collection in a medium-sized suburban school, there are limitations to transferability since the findings are the unique experiences of specific individuals in a set location. In addition, I was an administrator in the district where the study took place. While none of the participants reported directly to me, and all worked at the same employee contract level or higher, I collaborated with the participants on projects to achieve district goals. This professional relationship could have impacted the extent and detail of interview responses and limited the overall understanding of the cyber attack experience.

Furthermore, while this study examined the reaction of school-district IT administrators after experiencing a cyber attack, there were several years between the attack and data collection,

which might have impacted responses. Also, concurrent with the cyber attack remediation, the COVID-19 pandemic interrupted the continuity of education in the district. While the district only engaged in virtual instruction for all students for three months in 2020, the presence of the pandemic could potentially have affected the reactions and decision making of the IT staff.

Definition of Relevant Terms

Cyber attack/Event/Threat: "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information" (NIST, n.d.-a, para. 2)

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." (CISA, 2021a, para. 1)

District (also known as Local Education agency [LEA]): "a board of education or other legally constituted local school authority having administrative control and direction of public elementary or secondary schools in a city, county, township, school district, or political subdivision in a state, or any other public educational institution" (PA DOE, 2022, para. 35)

Endpoint: "Physical devices that connect to and exchange information with a computer network. Some examples of endpoints are mobile devices, desktop computers, virtual machines, embedded devices, and servers" (Microsoft, 2023, para. 1)

Malware: "A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim." (NIST, n.d.-b, para. 3)

Network: "A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications." (JavaTpoint, 2021, para. 1) Types of computer networks include Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), and Personal Area Network (PAN).

Ransomware: "Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return." (FBI, 2002b, para. 1)

Self-efficacy: "Conviction that one can successfully execute the behavior required to produce the outcomes." (Bandura, 1977, p. 193)

Threat Actor: "Threat actors, also known as cyber threat actors or malicious actors, are individuals or groups that intentionally cause harm to digital devices or systems. Threat actors exploit vulnerabilities in computer systems, networks, and software to perpetuate a variety of cyber attacks, including phishing, ransomware, and malware attacks." (IBM, n.d.-b, para. 1)

Chapter 2: Literature Review

The Growth of Cyber Attacks

On January 1, 1983, the Advanced Research Projects Agency Network created what is considered the first modern Internet by adopting Transmission Control Protocol (TCP) and Internet Protocol (IP) (Andrews, 2019). Even before the Internet became publicly available on August 6, 1991 (Bryant, 2011), the first cyber disruption occurred. Three years prior to public access, Robert Morris created a "worm" to determine the extent of the internet; however, the worm ended up creating the first instance of a Distributed Denial of Service (Ddos) attack and shut down 10% of the internet at the time (Climer, 2018). While Morris's intentions were not malicious, individuals and groups have utilized cyber attacks since the initial disturbance in 1988 to "disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems" (Pratt, 2021, para. 1). As cyber attacks have grown in number and severity, it is estimated that they cost organizations over 1 trillion dollars in 2020 (Ballard, 2021). In addition to the negative financial impact of cyber attacks, there is also the possibility that members of an organization could experience reputational, emotional, and psychological harm as a result of cyberbreaches (Agrafiotis et al. 2018; McMahon, 2020). As the number of cyber events grows each year, so does the likelihood of adverse consequences for institutions that are attacked by external threat actors.

During 2019, cyber attacks accounted for 1,473 breaches of personal information and the exposure of over 164 million records in the United States alone (Purplesec, 2020). While most of these breaches affected private organizations, there were 348 publicly reported attacks on education institutions during this time period (Purplesec, 2020), which is almost three times the number reported by U.S. schools in 2018 (Castelo, 2020). As a result of the COVID-19

pandemic and the shift in education to online learning, schools increased their cyber vulnerabilities, and as a result, cyber events increased by over 30% from July to August in 2020 (Whitney, 2020). With the growing number of education-related cyber attacks, and the potential negative impact on stakeholders, it is important for organizational stakeholders to understand how members of the organization experience cyber threats and how to develop and apply best practices in cybersecurity to minimize the effect of future attacks. To help highlight the difficulties in managing and responding to cyber attacks on organizations, this literature review presents information about the current state of cybersecurity and factors that can shape an individual's reaction to organizational cyber threats.

The following review of literature presents multiple studies that focus on the impact of cyber attacks on institutional preparation, response, and remediation, as well as how individuals play a role in threat prevention and recovery. Given the limited research on the effects of cyber attacks on educational organizations, this review also includes articles on political and commercial entities; however, the non-school related research that I selected can have universal application to educational settings. Since cyber attacks are a constantly evolving form of terrorism (Colbaugh & Glass, 2011), this review focuses primarily on more recent research between 2010 and 2022 to demonstrate current trends in cybersecurity; however, I also selected articles prior to 2010 in specific cases to provide a historical foundation for the development of cyber attacks and related theories.

Four themes emerged from the research related to how organizations manage cyber threats. The first theme focuses on the current state of cyber crime and the organizational impact. This includes the variety of outcomes that can influence the economic, reputational, and emotional state of the organization and stakeholders, as well as the difficulty in quantifiably

measuring the comprehensive effects of a cyber event. The second theme focuses on cybersecurity behavior that includes stakeholder awareness of cybersecurity threats in relation to behavior, and the potential influences of socio-demographic and personality types on cybersecurity behavior. The third theme investigates how a technology user's self-efficacy influences cybersecurity behavior and how response-efficacy can affect security related decision making. The fourth theme examines the process of how individuals make cybersecurity related decisions, specifically focusing on the Technology Threat Avoidance Theory (TTAT). In this literature review, I defined a cyber attack, cyber crime, cyber event or cyberterrorism as any instance "via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information" (National Institute of Standards and Technology, n.d.-a, para. 2). While I used cyber attack, cyber crime, cyber event, and cyberterrorism synonymously to refer to an actual event, I used cyber threat to account for a potential event that has not yet occurred.

Current State of Cyber Crime and Organizational Impact

While cyber attacks were initially considered "weapons of mass annoyance" in the early 2000s (Lewis, 2002), instances of disruptions have continued to increase in frequency and severity despite increased spending to prevent attacks (Hiscox, 2022). By 2012, the worsening trend in cyber warfare prompted the Director of the Federal Bureau of Investigation to state that, "I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again" (Mueller, 2012, para. 63). With the growing risk of cyber

events, it is important for institutions, including K-12 organizations, to understand the types of cyber-related attacks and how stakeholders of the enterprise can react.

Types of Cyber Events

There are multiple proposed classifications of cyber events; however, the Home Office of the United Kingdom (2015) categorized cyber crime as either cyber-enabled or cyber-dependent. Cyber-enabled crimes are traditional forms of non-digital crime that can be heightened using technology, while cyber-dependent crimes refer to events that "can only be committed by using computers, computer networks or other forms of informational communication technology (ICT)" (p. 22). Through a review of literature, Das and Nayak (2013) expanded classifications of cyber-dependent crimes. These categories included data crime, network crime, access crime, and related crimes. Within these categories, the impact of the crimes can range from network disruptions to corruption or loss of large sets of private data.

Regardless of the type of cyber-dependent crime, threat actors need to gain access to a target's computer or network. One of the key ways threat actors gain access to a digital device or network is through phishing (Aleroud & Zhou, 2017). Phishing is when a threat actor utilizes social engineering, which involves collecting information about an individual, developing a relationship with the individual, and then using the available information to exploit the individual (Salahdine & Kaabouch, 2019). Traditionally, exploitation would involve getting a user to unknowingly download and install malware onto their device; however, in recent years, threat actors have utilized stolen usernames and passwords more frequently to gain access to an individual's device (Crowdstrike, 2023). Based on how the cyber crime is committed, and the type of cyber crime committed, there are different potential impacts on individuals and organizations that can include reputational, monetary, and emotional repercussions.

Reporting Cyber Attacks

In an analysis of cyber event related surveys and several vendor reports, Furnell et al. (2015) questioned the validity of reported impacts as a result of cyber events. Based on current methods of reporting, Furnell et al. contended that most reports documenting the impact of cyber attacks are subjective recollections and do not represent a true factual description of the organizational impacts. To better represent the danger of cyber attacks, reporting should place a greater emphasis on the "financial impact in terms of down-time, real or potential loss of stolen data and clean-up costs" (p.11). Furthermore, when organizations report the impact of cyber events, organizations must give specific context to the event so that future victims can apply the related details of the attack to their own situations.

In addition to questions surrounding the accuracy regarding reports on cyber attacks, Cashell et al. (2002), in a review of literature and articles related to cyber crime and impacts, found that cyber attacks that have a minimal monetary impact are reported by organizations more frequently than attacks that have the highest levels of fiscal impact. Despite the potential relationship between financial losses and the number of reported incidents, the trend of under-reporting cyber events and their details could affect this finding since the existing data might be unreliable. In the review, Cashell et al. (2004) cited potential reasons for the under-reporting of cyber-related events. First, there are strong incentives not to report incidents, which include a negative effect on organizational reputation, litigation, liability implications, publicly indicating weak cyber preparedness, and the potential loss of employment. The second reason organizations do not report cyber crime is an inability to quantify the damage caused to an organization. While determining direct costs associated with an attack can be more straightforward, the indirect costs associated with items such as lost revenue and downtime are hard to accurately determine.

In another review of literature including news articles, research studies, and database searches related to cyber events, Agrafiotis et al. (2018) supported the difficulty of measuring impact and concluded that "organizations lack sufficient models to estimate the harm, direct and indirect, from cyber attacks" (p. 13). Given an inadequate understanding of how a cyber attack can impact an organization, there is the potential that leaders will fail to implement controls that protect the organization and minimize the threat of an attack. Furthermore, without a comprehensive understanding of the impacts of a cyber attack, organizational leaders are prone to have a lower inclination to allocate resources and a diminished focus on enhancing security. With a failure to invest in effective security practices, organizations increase the likelihood of falling victim to threat actors. To address misunderstandings related to the impacts of cyber events, organizations should adopt threat impact models that examine stakeholder perceptions related to the physical or digital, economic, psychological, reputational, and societal harm that can result from a cyber attack. By adopting a comprehensive threat impact model, organizational leaders can more accurately assess the safeguards needed to minimize digital harm.

Research surrounding the impact of cyber events on organizations highlights multiple potential negative effects and indicates that the reporting of organizational impact often fails to encompass the true extent of the attack. Even though Furnell et al. (2015), Cashell et al. (2002) and Agrafiotis et al. (2018) support multiple impacts and ambiguous reporting, the research focuses on a review of current literature to draw conclusions. Given that one of the conclusions of the research is that cyber events are under-reported, it calls into question whether research relying on news articles and reviews of self-reported information can accurately inform generalizable findings. Furthermore, Agrafiotis et al. (2018) suggests that researchers should place cyber events into specific context so individuals and organizations can understand the full

extent of attacks in a given situation. Even though current research categorizes different effects of cyber crime, few studies examine specific attacks to fully understand how cyber events affect an organization or individuals within the organization. Regardless of research indicating a need for more context and specificity in reporting, this process may be complicated given the nature of cyber crime.

The Complexity of Sharing Information About Cyber Events

Even though a common perception is cyber attacks are carried out by individuals or small groups, it is estimated that up to 80% of cyber events are carried out by state-sponsored criminal organizations (Malby et al., 2013). Based on a review of current literature, Watkins (2014) concluded that "organizations are generally outmatched by the tools and resources of state-sponsored organizations" (p. 5) and this has increased the amount of money that public and private organizations spend on cybersecurity, and the way they communicate to stakeholders before and after cyber events. Given the potential tools and resources that state-sponsored threat actors might have available, institutions that are attempting to resolve a cyber event should consider the vulnerabilities and benefits before publicly communicating an attack and assigning blame within or outside of the institution (Edwards et al., 2017). When institutions communicate information regarding a cyber attack, they need to consider the possibility of escalation from the threat actor and the potential impacts on all stakeholder groups. Furthermore, Edwards points out that often threat actors can "spoof" different aspects of an attack which affects an organization's ability to accurately identify the real attacker. This can make it difficult for organizations to properly assign responsibility, which can lead to further escalation of the event or miscommunication to stakeholders.

Difficulties surrounding communication related to a cyber event could lead to a limited number of employees having extensive knowledge of a particular cyber event and also create ongoing confusion for those trying to mediate the attack. With a potential imbalance of information regarding an attack, institutions should consider internal and external reputational implications when communicating about cyber events (Coombs, 2007). While cyber events impact digital networks, internal human capacity is the largest vulnerability to digital systems (McMahon, 2020), and ultimately organizational employees are the weakest link in preventing cyber attacks (Proctor & Chen, 2015). When organizations do not address the human side of cybersecurity, employees are left to make security related decisions based on personal values, which often lack accurate content knowledge and perceptions of virtual threats (van Zedlhoff, 2016). When organizations fail to adequately relay information regarding a cyber event, it can leave internal vulnerabilities through employees who are underinformed, and also impact internal and external reputation that can leave lasting impressions on the organization (Coombs, 2007). The human element of cyber events can add a layer of vulnerability and complication when preventing and remediating cyber threats, so organizations should consider effective ways to work with all stakeholders.

Communication During and After a Cyber Event

Researchers often apply the Situational Crisis Communication Theory (SCCT) (Coombs, 2007) to cyber attack related communication, which allows entities to examine communication through the strategies of deny, diminish and rebuild (Knight & Nurse, 2021; Kuipers & Schonheit, 2021; Wang & Park, 2017). While not the theoretical framework I will utilize in this study, SCCT provides a framework for organizations to assess the best way to preserve a positive reputation with stakeholders and can help minimize the emotional stress caused by a cyber

attack. Utilizing text analysis, Wang and Park (2017) applied the SCCT models of deny, diminish, and rebuild on post-crisis communications from Yahoo data breaches to analyze how post-attack communications can affect stakeholder's perceptions. While the analysis indicated components of transparency, understanding, and respect in post-crisis communication, ultimately a delay in initiating post-crisis messages had an impact on the company's reputation. Even though delayed communication can impact reputation, Richardson et al. (2020) concluded that stakeholders should prepare for ambiguous cyber event communication since there is an ongoing threat of escalation and complexities related to cyber attacks, and correct information is not always available. In addition, stakeholders often do not understand their role in the remediation of an attack which can influence their expectation of communication.

Zhang et al. (2018) conducted a mixed-method study after a large-scale ransomware attack on a university by surveying 150 participants and conducting 30 interviews. Participants shared through surveys that post cyber attack communication did not effectively relay information, did not minimize confusion, did not address concerns, and did not offer reassurance. In addition, "the situation should have been made public immediately or as soon as possible, instead of masquerading as a 'network disruption'" (p.1066). Furthermore, participants reported that the lack of substantial and timely communication caused more frustration with stakeholders than the cyber attack itself. Overall, the general lack of substantial communication led to stakeholders feeling "stressed, frustrated, anxious, scared, and panicked" (p. 1068). Zhang et al's study highlights not only the importance of effective post-event communication but also the potential psychological impact communication can have on stakeholders.

Along with timing and level of detail with communication, organizations also need to consider the level of responsibility for the event they will assume when making the attack public.

In an analysis of 70 post-attack company responses, Bentley et al. (2017) found that companies rarely took responsibility for a cyber attack since there was usually an obvious outside threat actor. While organizations denying responsibility can seemingly have a positive reputational impact, an analysis of the post-attack communications demonstrated a higher level of empathy for organizations that accepted responsibility for the event. This finding shows that there are potentially different benefits related to organization and stakeholder well-being based on how an organization chooses to communicate a cyber attack.

In a study that examined the responses from 2014 to 2019 of 64 companies to cyber attacks through SCCT, Kuipers and Schonheit (2021) identified that companies that admitted responsibility, offered an apology, and provided compensation, had stronger positive reputation perceptions from stakeholders. Furthermore, organizations could minimize reputational damage by communicating early after the attack and providing detailed information. Knight and Nurse (2020) supported these findings in a review of American companies' post cyber event communication focused on multiple themes including stock market reaction, legal requirements, message framing, not disclosing, protecting reputation, negative emotions, word of mouth, and complexities with outsourced functions. Based on communications, Knight and Nurse concluded that it is more beneficial for organizations to accept responsibility for cyber attacks rather than place blame on an outside threat actor.

Even though organizations can gain empathy, and potentially minimize reputational impact by taking responsibility for an attack, Chen and Jai (2019) found that as stakeholder perceptions of responsibility increased, the perceptions of trust in the organization decreased. Participants provided situational feedback based on four different conditions that varied in message delivery (news or directly from the hotel) and culpability of the organization (victim or

non-victim). In addition to finding a link between responsibility and trust, Chen and Jai also found that the source of post-crisis communication can impact stakeholder perceptions. When stakeholders receive information directly from the institution that was attacked and not media sources, the perception of organizational responsibility goes down. Based on stakeholder reactions and the thoroughness of the communication, the research shows the situational complexity of communicating a cyber event.

Through a social media text mining approach to study stakeholder perceptions of companies, Confente et al. (2019) found that user-generated content (UGC) demonstrated the presence of five important dimensions related to post-attack stakeholder perceptions including perceived quality, employer, corporate performance, customer orientation, and social responsibility of the organization. In addition, negative reactions identified in the UGC showed the type of cyber attack had an influence on the level of negativity demonstrated by stakeholders. This indicates a need for organizations to analyze the specific type of cyber event that occurred to properly communicate with stakeholders.

Overall, research supports differing strategies regarding how organizations should approach post cyber attack communication, and based on the method of communication, strategies can have differing effects on stakeholder groups. While researchers have applied SCCT to cyber-related responses, studies vary on whether taking responsibility for an attack (Kuipers & Schonheit, 2021) or claiming victimization (Bentley et al. 2017) is the best way to preserve organizational reputation. Furthermore, research indicates there are many complexities in cyber attacks that can influence the most effective response strategy (Confente et al. 2019; Edwards et al., 2017). With the number of complexities that can influence communication and

stakeholder reactions, it is important that organizations examine each cyber event based on its unique characteristics.

Regardless of the type of attack and the communication strategies implemented after an event, a common theme regarding communications is that it should be clear, prompt, and direct from the organization after an attack to provide information to stakeholders (Bentley et al., 2017; Chen & Jai, 2019; Zhang et al., 2018). While organizations can have a goal of clear communication, given the presence of threat actors and ongoing retaliation, clear communication is not always possible. Also, while there is limited research that explores how organizations can approach cyber response communication, research focusing specifically on educational institutions is lacking even more. While all institutions need to address the reputational and economic perceptions when communicating about a cyber event, they also need to consider the emotional impact that can develop after a cyber attack on stakeholders, including staff and students. With the potential of unclear communication, stakeholders' feelings of victimization, and the threat of ongoing escalation, there is the possibility that individuals will have negative psychological reactions to cyber events. Furthermore, when organizations employ communication strategies, intentional or not, that elicit negative reactions from large stakeholder groups, there is further potential for emotional and psychological stress on the members of the organization who are closest to remediating the attack.

The Psychological Impact of a Cyber Attack

Between 2015 and 2016, Gross et al. (2017) conducted three studies using both experimental manipulation and self-reported data to investigate the impact of lethal and non-lethal cyber events on the population. These studies revealed key insights into how people respond to such events. First, when a cyber attack results in loss of life, it increases the anxiety of

the victims. Additionally, when an attack doesn't result in loss of life, participants experienced the highest anxiety when the personal data of stakeholders was compromised. Secondly, the perception of the threat posed by a cyber event influences participants' anxiety as significantly as direct exposure to an attack, suggesting that the fear of an attack has similar effects to experiencing one. As a result of the findings, Gross et al. recommended that organizations should enhance their resilience through communication regarding cyberterrorism, conveying potential threats, and promoting the adoption of effective security protocols.

Bada and Nurse (2019) expanded their focus beyond the psychological impact in the pre-attack phase to encompass the aftermath of cyber crime incidents. Individuals affected by cyber crime may experience conditions such as depression or Acute Stress Disorder (ASD). Moreover, the unclear identity of attackers can intensify feelings of victimization, fostering a sense of personal culpability. Consequently, this may lead to isolation and a tendency to underreport cyber attacks. Given the range of negative psychological reactions to cyber events, there is the potential for not only short-term impacts but long-term impacts to stakeholder groups.

In a qualitative study with law enforcement representatives on cyber attacks, one participant highlighted the emotional impact on stakeholders by stating that often the immediate damage of a cyber event is not the most profound impact and “in most cases the fear, the reaction, and the uncertainty is more damaging than the actual damage wrought by the cyber attack” (Minei & Matusitz, 2011, p. 1007). This demonstrates the lasting impression a cyber event can have on an organization’s employees and stakeholders. Minei and Matusitz also emphasized the importance of human reactions by stating “it has been established that what is most human—the interpretation, the beliefs, the culture that forms thereafter— cannot be subjected to the process of being dehumanized” (p. 1014). When examining the effects of a

cyber event, it is imperative that organizations acknowledge the personal experiences of their stakeholders and the lasting effects on the institution.

Focusing on the personal experiences of a smaller stakeholder group in cyber events, Stacey et al. (2021) interviewed 8 administrators, including IT members, and collected artifacts from an organization that had experienced a cyber attack. The interviews highlighted the emotional and psychological impact that a cyber event can have on administration, specifically those working in IT. Since IT members work closer with the remediation and communication of a cyber event, the emotional and psychological repercussions can be more profound than other stakeholder groups. As a result of the study, Stacey et al. indicated three propositions that management can use to help in "transforming the emotional and coping capabilities of employees" (p. 1). First, senior management should display empathy, to support the emotional health of IT members. Second, management should proactively promote empathy at all levels of an organization; and finally, leadership should create a positive "supportive organizational culture" around cybersecurity.

In a review of literature, Triplett (2022), also recognized the importance of creating a culture around cybersecurity and highlighted the importance of strong leadership in developing that culture. Leadership in organizations can set an example of how members utilize technology in the institution, and ignorance of cyber threats at the leadership level can promote ignorance of security practices among employees. Sometimes leaders become complacent in their security practices, which can impact the level of stakeholder engagement to promote the best cybersecurity measures. Overall, leadership promotes the culture of the organization that can lead to a change in actual cybersecurity related behaviors.

Given the potential for a prolonged impact to an individual's emotional and psychological state (Bada & Nurse, 2019; Gross et al., 2017; Minei & Matusitz, 2011), it is important for organizations to consider the emotional state of stakeholders, especially IT members, before a cyber event, and after a cyber event. Additional research on the personal reactions of individuals who experience cyber attacks could help organizations determine best practices to address their emotional needs to promote the mental health of all groups involved, and also plan future training and supports to minimize the potential risk of future events. In addition to the emotional and psychological reaction to cybersecurity, it is also important for institutions to understand how other demographics impact how individuals react to cybersecurity.

Cybersecurity Behavior

While cyber-related communication is important to minimize negative impacts to reputation and the economic stability of an organization, McMahon (2020) indicated that there are important psychological factors to consider since there is the potential to create victimization when emphasizing individuals' actions regarding cybersecurity. Whether it is pre-attack or post-attack, how stakeholders respond and internalize their role in cybersecurity can have a profound impact on individuals and the larger organization (Bada et al., 2019; McCrohan, 2010). Furthermore, "organizations remain oblivious to the harms their employees and consumers experience" (Agrafiotis et al., 2018, p. 13) during a cyber event which leads to the possibility the organization will fail to address stakeholder needs before and after a cyber attack. To increase the preventative human actions to avoid a cyber event and address the individual responses to going through a cyber event, organizations should understand how people internalize the threat of cyber crime.

Cybersecurity Behavior: Awareness

While promoting cybersecurity awareness for organizational employees is a critical element of keeping institutions safe, McCrohan et al. (2010) argued that past security training has been ineffective since it focused on procedural aspects of how users can remain safe online, such as how to create a strong password. This type of procedural training lacked an explanation of specific cyber threats and how specific actions can overcome those threats. In a study of 396 undergraduate students, the researchers conducted an experimental study where students were assigned to high or low information groups regarding cybersecurity practices and cyber attack examples. Participants were told the experiment was part of a larger study to analyze the difference between online and paper/pencil assessments, and an online profile requiring a password was needed for participation in the two sessions. An analysis of password robustness after each session showed that participants in the high information group had more complex passwords after the second session when compared to the low information group, indicating that increased knowledge of the importance of cybersecurity, and awareness of potential attacks, can increase security behaviors. While these findings can offer insight into developing security education programs, McCrohan et al. acknowledged that the undergraduate sample may have lacked generalization to a larger workforce demographic. Furthermore, the study examined security behavior in a supervised setting and did not address long-term changes in behavior.

Despite a lack of generalization, Bada et al. (2019), through an examination of two case studies, supported the concept that the threat of harm through training is not enough to change behavior and that training should address multiple elements of human behavior. Bada et al. cited that often the concepts of cybersecurity are too difficult for the average consumer to implement and training on cybersecurity uses fear to invoke change. While organizations can feel that fear

can increase awareness, the presence of fear can lead to stress, and ultimately the avoidance of cyber threats. Furthermore, training often focuses on just building knowledge and awareness, which while a prerequisite to changing behavior, does not fully prepare individuals to develop effective cyber etiquette. Bada et al. suggested that in addition to building knowledge and awareness, organizations need to make training targeted, actionable, and doable. In addition, organizations should pair training with consistent feedback to reinforce positive changes in behavior. If training fails to address all these items, there is the possibility that stakeholders will acknowledge the threat of cyber attacks; however, they will make no changes to their online behavior, which will still leave the group susceptible to failures.

While the perception of harm prior to an attack has little effect on user behavior, it is also possible that experiencing a cyber attack also does little to change behavior. Utilizing an experimental study of 479 participants between the ages of 18 and 58, Kostyuk and Wayne (2019) administered surveys to assess participants' perceptions regarding cyber attacks and how experiencing an attack can influence security behavior. The researchers conducted the study because, “to date, most academic work on cybersecurity has focused on the macro-security dynamics of cyber warfare rather than the bottom-up perspective investigating attitudes of individual citizens” (Kostyuk & Wayne, 2019, p. 6). Findings from the study indicated that for the average user, there is limited understanding of basic knowledge and best practices when it comes to cybersecurity; however, experiencing a cyber event “heightens risk perception and increases willingness to engage in safer online practices” (p. 1). This finding contradicts Bada et al. (2019); however, while it is promising that individuals have an increased desire to change post-attack, Kostyuk, and Wayne found that despite a willingness to adopt best practices due to a heightened risk perception, there is little evidence that people changed their behaviors. This is

troubling because if stakeholders understand the potential threat, yet do not change behavior, it creates the possibility that a negative event will occur again. This also indicates that to change human security behavior, organizations should consider a comprehensive view of security that addresses multiple elements including awareness, knowledge, and realistic expectations. It is in the best interest of an organization to minimize the possibility of an attack to decrease the negative effects on the economic and reputational status of the organization, and more importantly, decrease the negative impact on the emotional state of employees and stakeholders (McMahon, 2020).

Cybersecurity Behavior: Personality and Socio-Demographics

Going beyond organizational practices that are implemented to promote a change in cyber-related behavior, studies show that personality types and socio-demographics could influence components of digital safety. In the development of the Security Behaviors Intention Scale (SeBIS), Engelman and Peers (2015) identified personality traits that can lead to more secure online behavior including device securement, password generation, proactive awareness, and updating software. Through a survey of 479 participants that ranged in gender, age, education level, and household income, individuals that demonstrated inquisitiveness, had a high level of reflection and consideration of future consequences, low impulsivity, and low dependence on others, all demonstrated significantly higher positive security behaviors. In addition, while individuals that had a high level of risk taking had a strong correlation with negative behaviors, researchers only observed this finding in regard to proactive awareness and keeping devices updated.

Gratian et al. (2018) expanded on the work of Egelman and Peers and used multiple online surveys to assess 389 higher-education staff and students. The surveys focused on

personality traits, risk-taking preferences, and decision-making styles in relation to cybersecurity behaviors. While the sample size was smaller and more limiting than previous studies, there were key findings related to personality and demographic information compared to various elements of cybersecurity best practices. First, research demonstrated a strong positive correlation between securing a device, using PINs or passwords to lock a device when not in use, and extroverted and rational decision-making personalities. Second, gender and age were strong predictors of password strength with women and younger participants showing a negative correlation to strong password generation. Furthermore, individuals that displayed avoidant decision-making traits had a higher likelihood of creating strong passwords; however, rational decision makers did not show a positive or negative correlation, indicating that different personality types could be better suited to different areas of cybersecurity. Like password generation, gender and age were potential predictors of proactive security awareness with women and younger participants having weaker proactive habits. The trend of gender and age continued in regard to updating devices for security reasons. In addition to gender and age, the researchers found a positive correlation between updating and risk-aversion, rational, avoidant, and spontaneous decision-making styles.

Alqahtani et al. (2020) further examined the impact on decision-making styles on cybersecurity related behaviors through the implementation of an augmented reality application game that taught key security concepts and allowed participants to enact situational security measures with immediate feedback on their effectiveness. As with certain aspects of cybersecurity in Gratian et al. (2018), rational decision makers demonstrated significantly higher positive online behaviors. In addition, avoidant and dependent decision-making personalities showed a small to medium effect on safe online practice. While this study had a small sample

size and a limited participant demographic that consisted of only students, the findings support that certain decision-making styles can have an impact on how individuals act online.

Even though several studies indicated correlations between socio-demographics on cybersecurity behavior (Bada et al., 2019; Egelman & Peers, 2015; Gratian et al., 2018), Kovačević et al. (2020) found "that the effects of cybersecurity perceptions, knowledge, and experiences are stronger than the effects of socio-demographics" (p. 125147) on cybersecurity related behavior. In a study of 147 students at a post-secondary institution, Kovačević et al. examined the cybersecurity related behaviors of individuals. Even though responses indicated potential relationships between security knowledge and socio-demographics, such as gender and education level, the strongest indicators of behavior were related to an individual's perceptions, knowledge, and experiences related to cybersecurity. Although increased knowledge and experience could presumably lead to improved behavior, survey responses also showed that individuals who experienced more data breaches had the least secure password behavior. In addition, individuals that had the most knowledge related to cybersecurity were the most frequent victims of cyber crimes. This finding supports previous research that awareness alone does not change behavior, and this could pose issues for organizations since increased experience and knowledge related to cyber events could have minimal impact on positive security behaviors.

Zwilling et al. (2022) expanded on the relationship between knowledge and cybersecurity in a quantitative study of 459 undergraduate and graduate students across multiple countries. Results showed that increased knowledge about cybersecurity increased an awareness of best practices and potential threats; however, changes in actual behavior were mixed. Individuals with increased knowledge and awareness are more likely to implement "simple and familiar" defense tools, but as prevention becomes more difficult and complex, people are less likely to act. The

researchers attributed this shift in behavior to the level of self-efficacy and controllability, and "people may be aware of a hazard and want to protect their devices but feel insecure about the appropriate measures, and this can reduce motivation to explore additional options" (Zwilling et al., 2022, p. 91).

When examining how individuals react to cybersecurity, research shows training, knowledge, personality, and personal demographics could impact an individual's behavior. Organizations should consider how their current training programs and awareness campaigns are marketed to different groups of individuals to make sure that security practices are actionable, and that training does not promote additional stress on stakeholders (Bada et al., 2019). In addition, given negative correlations related to age and gender, organizations should consider their stakeholder demographics and adjust training programs and awareness campaigns accordingly. Furthermore, organizations must consider how personality types can impact behavior not only through training but also how personality types are represented in technology leadership within the institution since rationale and risk-aversion personalities have a stronger likelihood of implementing multiple areas of cybersecurity (Gratian et al., 2018). Research shows that there are many different aspects of how individuals process cybersecurity related behaviors, and while there are correlations between personality types, socio-demographics, and knowledge, research also shows that technology users need to have trust in their ability to prevent a cyber attack to initiate positive behavior.

Self-Efficacy and Cybersecurity Behavior

Based on research, there are potential differences in cybersecurity knowledge and experience related to socio-demographics (Bada et al., 2019; Egelman & Peers, 2015; Gratian et al., 2018), and knowledge has a potential relation to security related behavior; however,

increased knowledge does not necessarily have a positive impact on actions (Kovačević et al., 2020). Zwilling et al. (2022) attributed the failure of increased knowledge to positively change behavior to an individual's negative perception of their ability to successfully implement tools and actions that will prevent an attack. Bandura (1994), in a discussion of self-efficacy, or a person's perception of their ability to produce an effect, states when people have a negative view of their capabilities they will "shy away from difficult tasks which they view as personal threats" (p. 2). In contrast, people with positive self-efficacy will "approach threatening situations with assurance they can exercise control over them" (p. 1). With the potential of a cyber attack, there is a possibility that a technology user's self-efficacy could play a role in their implementation of strong security practices.

Technology Related Self-Efficacy

Halevi et al. (2016) conducted a survey involving 621 college-level students from various countries to investigate cultural and psychological factors in shaping a framework for studying cybersecurity-related human behavior. Through binary logistic regression analysis, the researchers identified several key findings. First, they found that culture was a predictor of privacy behaviors but had a limited impact on security-related behavior and self-efficacy. Gender did have an impact on self-efficacy where males demonstrated higher confidence in being able to prevent a cyber breach; however, despite higher self-efficacy, there was no difference in actual security behaviors based on gender. This indicates that even though an individual perceives their ability to prevent an attack as high, their security related actions are no different than someone with a low perception of self-efficacy. While this finding can help organizations plan for training and monitoring of cybersecurity best practices, the number of demographic variables combined

with the limited age range of participants calls into question the generalization of the findings to larger mature organizations.

In a review of literature, Bada and Nurse (2019) synthesized previous findings to explore psychological reactions related to cybersecurity. They examined various established concepts and theories that pertained to how individuals perceive cybersecurity, including self-efficacy, risk perception, Protection Motivation Theory, locus of control, the Extended Parallel Process Model, and Culture of Fear. The analysis yielded crucial insights into how people perceive and respond to cyber attacks. First, an individual's perception of a cyber threat is closely tied to how they perceive its impact on themselves and their belief in their ability (self-efficacy) to effectively address the threat. This suggests that IT users weigh their self-efficacy against the potential impact of the threat on themselves or their organization. When stakeholders feel ill-equipped to handle a threat, they tend to downplay its significance or even deny its existence (Bada & Nurse, 2019).

Cheng et al. (2020) further examined the impact of self-efficacy on cybersecurity behavior through another larger study that consisted of a random sample of 1018 participants that responded to a phone-based survey. Participants ranged in demographics and had an average age of 42 years old. Using a correlational analysis, the researchers found a relationship between high self-efficacy towards preventing cyber threats, high technology usage, and an increased susceptibility to falling victim to cyber crime. The researchers attributed this finding to individuals having overconfidence in their ability to prevent cyber crime, and due to overconfidence, they do not implement best practices to protect themselves. In addition to overconfidence and an increased susceptibility to cyber-related failures, Wang et el. (2012) found that individuals who are more confident in their ability to detect phishing emails spend

less time processing potential red flags in emails. For organizations, these findings present potential difficulties since it implies that the users who use tech the most and are most confident in their ability to remain safe online, are potentially the biggest threat to the organization. At the same time, this finding does not account for the effect of knowledge on a user's decision making. Just because someone is a frequent technology user, it does not mean they have developed a strong understanding of positive security behaviors.

While confidence can influence security practices, confidence levels could vary between security experts and novices. In a quantitative study of 55 novices and 20 security professionals, Ben-Asher and Gonzalez (2015) analyzed participants' reactions and ability to identify malicious attacks in 20 different network scenarios. Findings showed that even though experts were able to identify components more accurately in a larger sequence of events that indicated an attack, there was no significant difference between experts and novices in determining whether the overall scenario was malicious. Even though this demonstrates that the ability to detect a cyber attack is similar regardless of experience, the authors point out that the potential for early detection in a larger sequence of events could have a profound impact on early detection and overall impact on the organization. Ben-Asher and Gonzalez also highlighted a limitation of the study as experts navigating an unfamiliar network set-up. There is the potential that experts would have higher detection results if the researchers conducted the study in a familiar network system. In addition to attack detection, responses also showed that experts and novices had similar confidence levels in their ability to detect an attack; however, novices also had a higher level of confidence in labeling a scenario as benign. This potentially indicates "that cybersecurity analysts adopt cautious behaviors when monitoring a network" (Ben-Asher & Gonzalez, 2015, p. 59) and understand that potential threats are not always easy to detect. If experts approach all cyber

situations as a potential threat, this could indicate a lower self-efficacy to identify a potentially harmful situation. If personal perceptions of threats are unreliable, then experts might also rely on external tools to help identify and mediate threats.

Response Efficacy

In addition to a user's perceived self-efficacy to address a cyber threat, Johnston and Warkentin (2010) examined the link between response-efficacy, the belief that an action can mitigate a threat, and self-efficacy, a user's belief in their ability to implement an action to address the threat. In an experimental study that included 275 college level students and staff, found that behavior is directly influenced by both response-efficacy and self-efficacy; however, "while both response efficacy and self-efficacy appear to have strong predictive ability, social influence has slightly more of an effect on behavioral intent" (p. 560). Zahedi and Chen (2015) also showed a strong relationship between response-efficacy and self-efficacy in a controlled experimental study that included 865 college level participants. Results from the study indicated that response-efficacy is positively influenced by the accuracy and speed of the tool, and users "may view protective IT artifacts as an extension of their selves" (p. 473). These findings demonstrate the need for a positive perception of security tools within organizations and their psychological impact on stakeholders.

Jansen and van Schaik (2017) continued work that links response-efficacy to strong online security behavior. This finding was the result of a questionnaire completed by 1200 online banking participants that ranged in gender, age, education, working status, and internet usage. Like Johnston and Warkentin (2010) and Zahedi and Chen (2015), findings indicated knowledge of others using security measures, or social influences, could positively impact online behaviors and that a positive perception of security measures can increase positive security behaviors.

While the findings of the study supported previous research, the wider range of demographics in Jansen and van Schaik's sample size could increase the generalization of the findings.

Overall, research shows that a user's perception of their ability to address a cyber threat can have a positive (Bada & Nurse, 2019) or negative (Cheng et al., 2020; Wang et al., 2012) impact on user intentions and behavior. In addition, a user's own perception of self-efficacy is potentially related to the positive perception of the tools utilized to address the cyber threat (Jansen & van Schaik, 2017; Johnston & Warkentin, 2010). These findings can help organizations determine policies and procedures to help increase stakeholder confidence in both themselves as well as the tools utilized to prevent cyber events; however, research also indicates complicated interactions that shape stakeholder's intentions and behavior including factors such as social influences (Johnston & Warkentin, 2010). To fully understand how stakeholders will implement positive and negative cyber behaviors, organizations need to examine a more comprehensive interaction of elements that include self-efficacy, response efficacy and social influence.

Making Cyber-Related Security Decisions

Human beings are the weakest link in preventing cyber attacks (Proctor & Chen, 2015) and have strong emotional reactions to cybersecurity (Bada & Nurse, 2019; Gross et al., 2017); yet organizations will often attempt to address behavioral related risks with technological tools rather than responding directly to human decision making (Metalidou, 2014). When considering how individuals make security related decisions, positive cybersecurity behaviors have varied relationships with different demographic groups, personality types, and decision-making styles, making it hard for organizations to understand the best ways to prevent cyber attacks (Bada et al., 2019; Egelman & Peers, 2015; Gratian et al., 2018). Furthermore, experience and knowledge

of best practices related to security do not appear to influence actual changes in behavior on their own (Kostyuk & Wayne, 2019; Kovačević et al., 2020). The lack of consistent findings regarding influences on cybersecurity related decisions indicates the possibility that the decision-making process related to cyber behavior is more complicated than isolated variables.

Protection Motivation Theory (PMT)

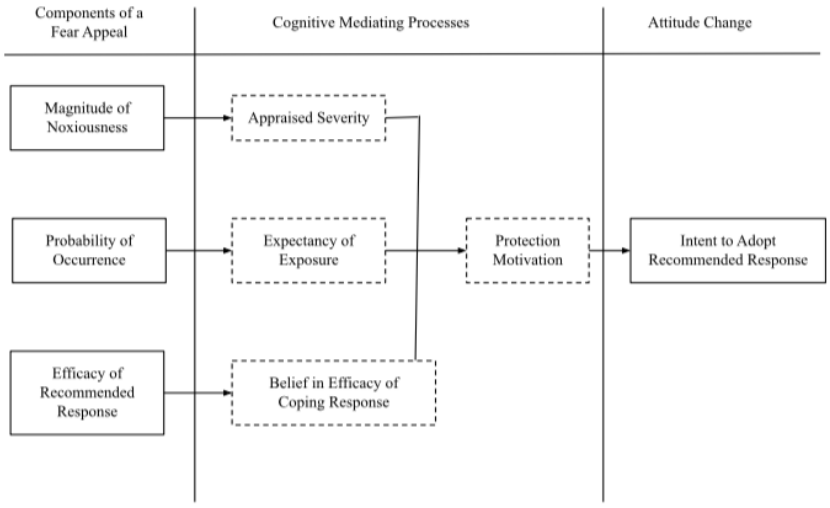
To examine decision making related to cyber crime prevention, and how individuals initiate cyber-related security behaviors, researchers have applied Protection Motivation Theory (PMT) (Chenoweth et al., 2009; Mwagwabi, 2015; Woon et al., 2005) to gain a better understanding of how people process cybersecurity related practices. PMT is rooted in the concept of positive feedback loops in cybernetic theory where individuals recognize an anti-goal, an undesired resolution, and enact behavior to increase their distance from the negative end state (Carver, 2006; Wiener, 2019). In cybernetics, a cyber threat would be the anti-goal, and the IT user would implement actions to increase their distance from the threat. PMT expands on positive feedback loops and outlines a more comprehensive process of how individuals decide to implement threat avoidance decisions based on multiple factors. Developed in 1975, PMT proposed stimuli associated with change related to fear appeals, or "the contents of communication describing unfavorable consequences that may result from failure to adopt the communicator's recommendations" (Rogers, 1975, p.94). Rogers indicated a fear appeal is made up of three components including the magnitude of noxiousness, the probability of occurrence, and the efficiency of the recommended response (see Figure 1). From an analysis of the initial components, individuals enter a "cognitive mediating process" of appraised severity, expectancy of exposure, and belief in the efficacy of the coping response that would result in initiating "protection motivation," or the level of desire to implement a communicator's recommendations.

Based on the arousal of protection motivation, a user would potentially implement a change in behavior. Maddux and Rogers (1983) later added "self-efficacy expectancy" as a fourth component in PMT that influences an individual's protection motivation.

In an experimental study of 153 college level students utilizing smoking dangers as a fear appeal, Maddux and Rogers identified self-efficacy as the "most powerful predictor of behavior intentions" (p. 476) and self-efficacy also had a strong influence on the probability of a threat's occurrence and coping response efficacy. While PMT's analysis of fear appeals has a direct relation to the potential fear of a cyber-related incident, initial studies on PMT focused primarily on health-related fear appeals and did not address specific attributes of cyber-related incidents. To fully understand behavior and intentions related to cyber threats, an additional model could provide a more thorough analysis of stimuli and thought processes.

Figure 1

Schema of the Protection Motivation Theory (Rogers, 1975, p.99)



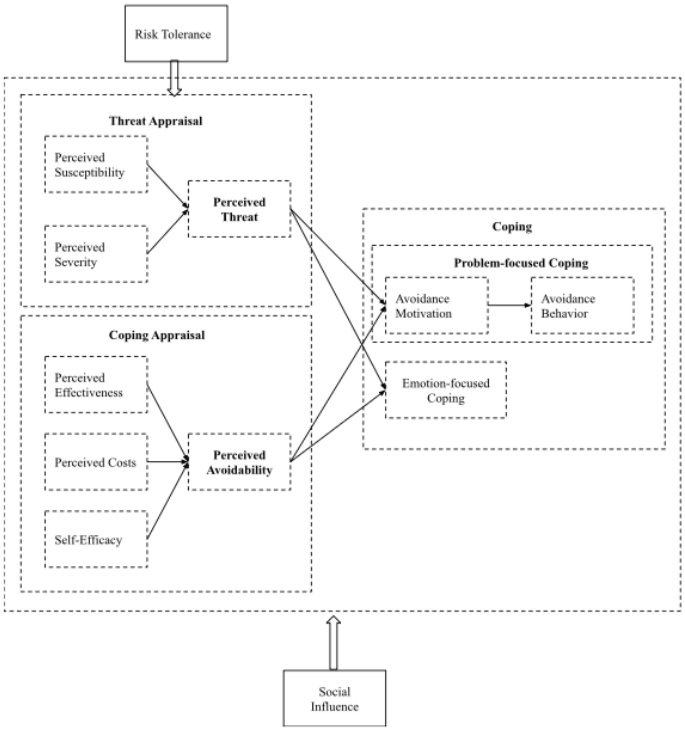
Note: Adapted from "A Protection Motivation Theory of Fear Appeals and Attitude Change" by R.W. Rogers, 1975. *The Journal of Psychology*, 91(1), 99.

Development of Technology Threat Avoidance Theory (TTAT)

To provide a more comprehensive way to analyze the process related specifically to technology related security decisions, Liang and Xue (2009) developed the Technology Threat Avoidance Theory (TTAT). TTAT is based on the tenets of PMT where a user identifies a threat and then appraises the likelihood of exposure, the potential severity, and their perceived ability to address the situation before determining a response. Liang and Xue believed a new model related to technology was needed since existing models focused primarily on human decisions related to "programs designed to provide communicational, computational, or decisional aids to users to increase their performance" (p. 73), and did not account for reactions to malicious IT, or programs that cause disruptions and impact the security of networks. Once a user has accepted that a potential online threat exists, the first process related to TTAT involves an individual conducting a threat appraisal and coping appraisal. During the threat appraisal, individuals assess their perceived susceptibility, the probability of a negative digital impact, and the perceived severity of the impact. In addition to the threat appraisal, individuals undergo a coping appraisal that analyzes the perceived effectiveness, perceived cost of the actions, and their self-efficacy to avoid a negative impact. Based on the threat appraisal and coping appraisal, individuals determine the perceived threat and their perceived ability to avoid the threat.

FIGURE 2

Schema of Technology Threat Avoidance Theory



Note: Adapted from "Avoidance of Information Technology Threats: A Theoretical Perspective," by H. Liang and Y. Xue, 2009. *MIS Quarterly,* 33(1), 79.

Based on an individual's analysis of a perceived threat and the ability to avoid a cyber threat, users will approach the situation through either problem-focused coping, emotion-focused coping, or a combination of the two. Problem-focused coping consists of implementing safeguards that can prevent or minimize a negative impact, while emotion-focused coping "is oriented toward creating a false perception of the environment without actually changing it or adjusting one's desires or importance of desires so that negative emotions related to threat are mitigated" (Liang and Xue, 2009, p. 78). Users that feel that a situation is preventable, regardless of perceived severity, will more than likely enact problem-focused coping strategies to avoid

negative consequences. If an individual perceives that there are no measures to avoid the threat, that measures cost too much, or they are unable to perform the measures, they will use emotion-coping to deal with the negative threat. Since not all cyber risks are preventable with safeguards, individuals might use a combination of problem and emotion focused strategies to minimize the negative impacts and regulate emotional stability.

In addition to the individual cognitive perceptions, TTAT also accounts for personality and social influences that impact cybersecurity decision making. First, a user's risk tolerance can have a profound impact on the perceived threat. Since different people have varying tolerance for uncertainty and severity of specific events, risk perception can affect the type of actions utilized to minimize a threat and when a user implements those actions. Secondly, social influence can shape a user's reactions through informational and normative means. If an organization promotes cybersecurity training and focuses on multiple ways to prevent cyber harm, an individual is more likely to implement positive behavior in reaction to a threat. Organizational structures can also impact actions through normative influences including security compliance, internalization of the group's shared values, and perceived identification with the larger group.

To measure the interaction of the TTAT components, Liang and Xue (2010) developed a two-part questionnaire that contained items related to perceived susceptibility, severity, and threat, safeguard effectiveness, safeguard cost, self-efficacy, avoidance motivation, and avoidance behavior. The researchers administered the questionnaire to 166 college students at a single university. Using Partial Least Squares, Liang and Xue examined whether there were positive impacts between each decision component in the TTAT model. While most of the researchers' hypotheses regarding TTAT component interactions were supported, there was a weak correlation between perceived severity and perceived susceptibility, showing that both

constructs are largely independent of each other. Since the study demonstrated a positive interaction between both perceived susceptibility and perceived threat and perceived severity and perceived threat, it indicated that "both constructs are necessary antecedents of perceived threat" (p. 404).

Carpenter et al. (2019) further examined the interaction of perceived susceptibility and perceived severity through a survey of 152 college students, with most respondents being male. As with Liang and Xue (2010), findings showed no interaction between perceived susceptibility and perceived severity; however, both were indicators of perceived threat. Carpenter et al. (2019) proposed three potential explanations for the lack of interaction. First, since Liang and Xue and Carpenter et al. both utilized purposeful sampling, the study did not represent the larger IT using population. Second, the scale used to assess susceptibility and severity on the questionnaire could have been ineffective in accurately measuring a user's perspective, and finally, given the small sample size, there were not enough respondents to determine a small moderation effect.

In addition to a lack of correlation between susceptibility and severity, Carpenter et al. (2019) identified a negative interaction between perceived threat and safeguard effectiveness, indicating as either of the constructs increased, the other would go down. This was an unexpected finding and could indicate that if a user views a threat as too severe and too likely, the individual will engage in emotional coping over problem-focused coping. Carpenter et al. (2019) suggested that due to this finding, organizations should not overemphasize how disastrous cyber attacks can be since it can cause stakeholders to avoid cyber threats. While a unique finding, Carpenter et al. only focused on spyware during the study, and given the potential for varying reactions based on the type of cyber threat (Confente et al., 2019), additional research is needed to show whether this finding is generalizable to different populations and scenarios.

Young et al. (2016) replicated Liang and Xue's original study with a larger sample size utilizing three different sample groups. The first group consisted of 271 students from a large university, group two consisted of 196 students from a small university, and group three was composed of 45 students from a large university. While the replication expanded the total sample size, the demographics were still limited to college level students and limited the generalization of the findings. Young et al.'s findings largely supported the hypotheses of the original study except for a correlation between susceptibility and perceived threat. Additional research could confirm whether this interaction, or lack thereof, is significant, but Young et al. theorized that in the time from the initial study in 2010 and the replication in 2016, the number of cyber attacks increased significantly and could have impacted perceived susceptibility. If an individual assumes a cyber attack is a certainty, perceived susceptibility has little effect on perceived threat, and focus shifts to perceived severity of an unavoidable event.

Even though Young et al. observed a difference in the interaction of perceived susceptibility and perceived threat, the study still replicated the lack of correlation between perceived susceptibility and perceived severity. Given the weak interactions related to the threat appraisal variables in the TTAT, it calls into question whether additional research could help refine specific components to better understand how individuals assess perceived threat. Young et al. hypothesized that there is a potential discord from the evolution of TTAT since research in threat appraisals with PMT was initially grounded in medical related fear appeals, where "susceptibility is estimated based on known correlated factors such as lifestyle choices, proximity to risk vectors, and presence of related disease while perceived severity is based on previous patient data" (p. 6). Since cyber attacks are constantly changing and users are less likely to analyze a threat assessment based on previously correlated and historical data, users could rely

more heavily on emotional and social perceptions for a threat appraisal. While historical data might be missing from some users of technology's perception of susceptibility and severity, experiencing a cyber attack could impact the constructs that shape user perceptions.

Using a between groups experimental design, Mwagwabi (2015) surveyed 419 participants that ranged in gender and age, looking at how perceived vulnerability and susceptibility relate to password behavior. One key finding was prior exposure to hacking increases an individual's perception of vulnerability. While vulnerability perception increased post cyber event, it does not appear to predict actual intentions or behavior related to cybersecurity. Furthermore, there is no correlation between perceived severity and intentions or behavior; however, perceived threat, which is composed of perceived vulnerability and severity, does show a strong relation to security intentions and behavior. This supports Liang and Xue's (2010) findings that perceived vulnerability and susceptibility, although largely independent of each other, are essential constructs to assess perceived threat and impacts on security behaviors.

In addition to perceived vulnerability and susceptibility increasing after a cyber event, through a study involving 62 participants, Vance et al. (2014) found that self-reporting regarding risk, vulnerability, and susceptibility perceptions is only accurate after an individual experiences an attack. Comparing perceptions and responses through Electroencephalogram (EEG) and self-reporting surveys, Vance et al. placed participants in a controlled laboratory-based task in which they experienced a simulated cyber attack. The researchers hypothesized that perceptions of cyber risk are addressed by individuals subconsciously prior to an attack, and it is only through the experience of an attack that participants are consciously aware of their risk perceptions. Given the small sample size of the study, it does limit the generalization of the results and further replication could strengthen the findings. Regardless of the lack of generalization, the study does

imply that research that utilizes self-report measures after experiencing a cyber attack could offer a more accurate representation of an individual's perceptions and behavior.

Along with the experience of going through an attack, culture, and economic status might also impact a user's threat appraisal and coping process. In a survey of American and Chinese tech users, Chen and Zahedi (2016) found that Chinese users have a higher perception of susceptibility and severity, as well as stronger tendencies to adopt avoidance behavior to address a threat. Chen and Zahedi attributed these differences to the cultural constructs of the countries as well as a potential economic impact resulting from availability of resources to prevent cyber attacks. While the impact of individual demographics on the TTAT appraisal process is potentially important for the application of the theory in different settings, there are limitations to the study that could indicate the need for further research. Even though the study contained a range of demographics, the response rate in America was 70.3%, compared to a response rate of 27.8% in China. Given the variation in response rate, both samples might not be representative of the population and have limited generalization.

While there are limitations with TTAT that include mixed findings regarding how perceived susceptibility and severity impact a user's threat appraisal (Mwagwabi, 2015; Young et al., 2016), and the validity of quantitative studies that utilize self-reporting data (Vance et al. 2014), the theory offers a framework to analyze multiple components that impact technology-based security decisions. Current research on TTAT is limited since most studies focus on college level students utilizing self-report survey data. Since cyber attacks continue to evolve, individual differences can impact threat appraisals and coping strategies, and the experience of going through an attack can increase the conscious awareness of security perceptions, rather than relying on survey data, which might fail to accurately assess user perceptions, future research

should seek to understand the lived experiences of technology users and look at how individuals apply the principles of TTAT post-attack.

Summary

The threat of cyber attacks and their impact on organizations continues to increase (Castelo, 2020) and with a strengthened reliance on technology during the COVID-19 pandemic, schools created additional digital vulnerabilities, which leave them more vulnerable to cyber events (Whitney 2020). Current research on how institutions manage cyber events is limited, and there is even less research that focuses specifically on the K-12 educational setting. In addition to a lack of research, studies also indicated that cyber attacks and their severity are underreported by organizations. In order to help inform a user's decision-making process, future research should focus on understanding cybersecurity in the context of K-12 organizations and emphasize accurate reporting of cyber events so IT users can make the most informed decisions. While quantitative studies can offer insight into how all the potential variables interact within the Technology Threat Avoidance Theory framework, qualitative work, such as case studies could provide deeper levels of human reaction and offer a greater context to a cyber event.

While much of the current research on cybersecurity behavior and reaction uses quantitative methods to provide overarching findings that are generalizable across situations, the research points to individual complexities such as personality-type, knowledgebase, and communication creating unique contextual situations for all stakeholders. Since widespread accurate communication is often hindered during a cyber event (Bentley et al., 2017; Zhang et al., 2018), there are potentially only a few members of the organization that have a comprehensive understanding of an actual event. As Stacey et al. (2021) points out, often IT professionals are the closest to the remediation process and communication after a cyber attack,

and will potentially have the greatest emotional and psychological reaction from experiencing an attack. Moving forward after an attack, it is imperative that organizations understand how their IT teams react to the traumatic experience of a cyber attack to ensure the continuing mental health of the team. With additional qualitative studies that focus on the lived experience of the individuals closest to a cyber event, K-12 organizations can develop a better understanding of the psychological and emotional reactions that stakeholders encounter, and work to refine support, training, and communication strategies to better meet the needs of different stakeholder groups.

Chapter 3: Methodology

This chapter outlines the methodological practices I utilized in this study. The first section focuses on the worldview, followed by the research methodology and design, theoretical framework, and research questions. Subsequent sections present an overview of the research context and participants. I have also included sections that contain information regarding the background, role, and perspective of the researcher, as well as the data collection methods and data analysis. The chapter concludes with an examination of the validity, limitations, ethical considerations of the study, and a summary.

The purpose of this study was to explore the experiences of one district's IT administrative staff after a cyber attack to gain a better understanding of how organizational cyber events in K-12 institutions shape the perspectives and decisions of IT leaders. This study contributes to the limited body of research that focuses on cybersecurity and cyber attacks on K-12 institutions, as well as the human experience of living through a cyber attack. In addition, this research provides considerations for schools on how to support IT staff and promote effective cybersecurity decisions before and after an attack.

Worldview, Methodology, and Research Design

A researcher's worldview provides the philosophical lens that acts as the foundation of the research process. As such, the worldview has a direct impact on how the researcher perceives how knowledge is constructed. The worldview also shapes the development of research questions, the methods utilized in collecting data, and the analysis of the findings (Butin, 2010; Creswell & Creswell, 2018). Since the worldview is the basis for how a researcher formulates a study, it is important to understand how the worldview influences the framework of the research.

The foundational underpinnings of this study are a social constructivist worldview. "Social constructivists believe that individuals seek understanding of the world in which they live and work" (Creswell & Creswell, 2018, p 8). With a social constructivist worldview, the researcher acknowledges that participants construct individual meaning based on their interactions with others and make sense of the world "based on their historical and social perspectives" (p.8). Furthermore, since individuals make sense of their world through their interactions, it is important for social constructivist researchers to seek to understand the specific context and setting in which participants interact. Since the purpose of this dissertation was to study the experiences of individual IT administrators in the K-12 setting after a cyber attack and their perceptions of ongoing security measures, the voices and lived experiences of the IT administrators were the primary focus of the research. In addition, since a social constructivist worldview highlights the importance of the setting and context in shaping an individual's experience, this study limits the scope of the research to one K-12 district.

The tenets of the social constructivist worldview are often associated with qualitative research since "qualitative research methodologies are oriented towards developing understanding of the meaning and experience dimensions of human lives and their social worlds" (Fossey et al., 2002, p. 730). This dissertation employed a case study methodology, a specific type of qualitative research that researchers utilize when they want to study a specific event or events (Yin, 2018). Researchers conduct case studies when they want to investigate "a contemporary phenomenon (the 'case') in depth and within real-world context, especially when the boundaries between the phenomenon and the context may not be clearly evident" (Yin, 2018, p. 15). Given the potential number of variables associated with the lived experiences of IT administrators after a cyber attack and their ongoing perceptions of decision making, this case

study relied on multiple sources of evidence, including interviews and artifacts, to triangulate themes related to the research case. I used interviews in this research since one of the goals of qualitative research is to get as close as possible to participants (Creswell, 2016), and interviews allowed me to develop rich descriptions of the participants' experiences. At the same time, social constructivist researchers acknowledge that their own experiences, including personal, cultural, and historical, shape their interpretation of the research (Creswell & Creswell, 2018) and it is important to consider how biases, preconceived perceptions, and relationships can impact data collection.

Theoretical Framework

While qualitative researchers do not test theories, the application of specific theories in qualitative research can help the researcher develop questions and can also help provide a framework for analyzing the results that are obtained (Creswell, 2016). To provide a framework to offer guidance with questions and data analysis, I utilized the Technology Threat Avoidance Theory (TTAT), which outlines aspects related to cybersecurity reactions and decision making. Based on TTAT, a technology user will initially conduct a threat appraisal and coping appraisal to assess the severity and likelihood of a cyber event, and the user's ability to prevent negative repercussions as a result of the cyber event. In addition to a threat and coping appraisal, a user's risk tolerance and social influences can also impact the decision-making process. Based on the interaction of the threat appraisal, coping appraisal, risk tolerance, and social influences, a technology user will either implement a problem-focused coping mechanism to minimize the negative impact of the threat or implement an emotional coping mechanism where the user creates a false perception of the event and does nothing to minimize the threat.

Even though the intention of this dissertation was not to test the components of TTAT in the decision-making processes of IT administrators after experiencing a cyber attack, the framework provided insights for developing questions in the semi-structured interview protocol that I utilized to gain a better understanding of IT administrators experiences (Appendix A and B). While interview questions did not directly address the components of TTAT, the concepts of TTAT helped form the basis for the interview questions such as perceptions of cyber threats and an individual's belief in their ability to minimize the impact of a threat. Furthermore, in conjunction with inductive coding, I used deductive coding to apply themes related to TTAT to interview responses. This can provide a deeper understanding of the decision-making process used by IT administrators after experiencing an attack. Research already highlights potential inconsistencies between the interaction of "perceived susceptibility" and "perceived severity" leading to the perception of a "perceived threat" (Carpenter et al., 2019; Liang & Xue, 2010; Young et al, 2016). The use of deductive coding regarding TTAT themes provided insight into how experiencing an attack shapes the perception of cyber threats through the eyes of K-12 IT administrators.

Research Questions

- How do K-12 IT administrators describe their experiences with a cyber attack within their district?
- How do K-12 IT administrators see a cyber-attack as influencing current practices and policies?

Research Context

The setting of this case study was Fern Valley School District (a pseudonym), a K-12 public school district located in southeast Pennsylvania. Fern Valley School District (FVSD) is a

suburban district that serves approximately 6,100 students and 1000 staff members across six elementary schools, two middle schools, and one centralized high school. In addition to the nine academic buildings, the District also has one administrative office building that houses the superintendent, assistant superintendent, and other administrators in business, facilities, curriculum, technology, pupil services, food services, and community education. Students in the FVSD were predominantly White (76.8%); however, the District was seeing an increase in the number of Asian (6.9%) and Hispanic students (10.5%), while the percentage of Black students remained consistent (5%). At the time of the study, FVSD was also seeing an increase in economically disadvantaged students (22.5%), English Language Learners (5.7%), and students receiving special education services (18.6%) (Commonwealth of Pennsylvania, 2023).

While classroom technology had increased in FVSD during the 1980s, 1990s, and early 2000s, beginning in 2014, the district began to pilot a 1:1 Chromebook program for students at the high school, focusing on specific classes. From its inception in 2014, the 1:1 program continued to grow in secondary buildings, and in 2016 with the retirement of the district's technology supervisor, the district created a director level position that oversaw all aspects of technology. Under the new director, the district continued to implement the 1:1 program but started the transition from Chromebooks to Windows based devices. Also, during this time, the district started to shift from Google Apps for Education to Microsoft Office 365. In addition to student and teacher endpoints, FVSD also maintained a single Network Operations Center (NOC) where the district housed all in-district servers related to daily operations including teacher storage drives and the student information system (SIS).

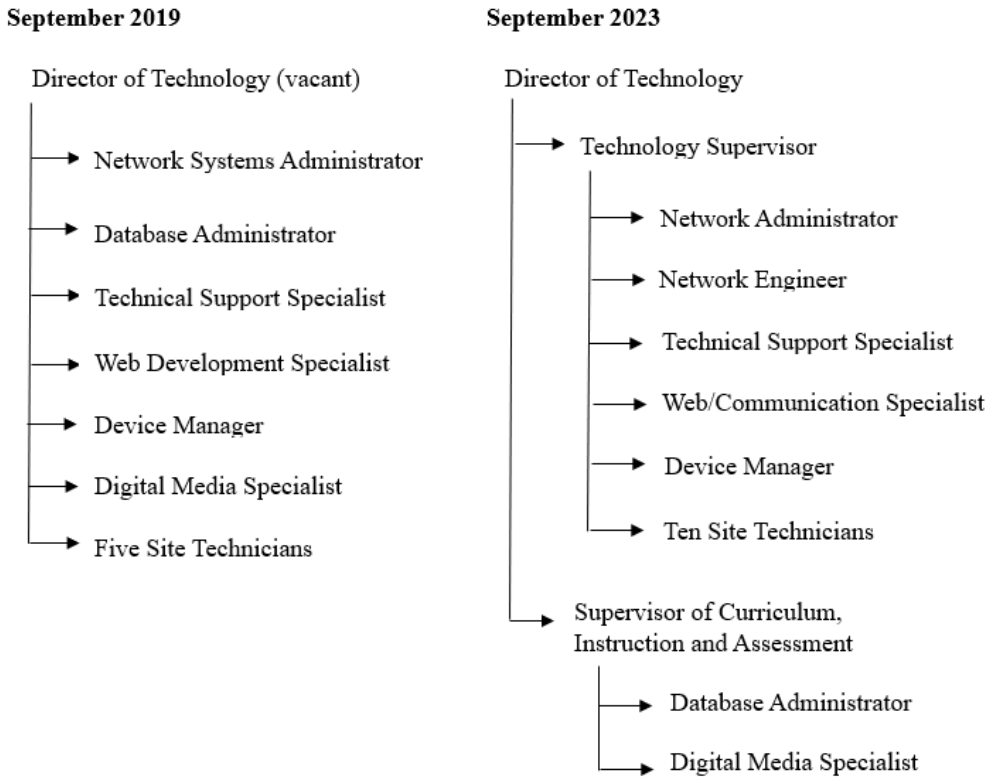
Then, in December of 2018, the technology director retired, and after several rounds of interviews, FVSD did not find a replacement for the position. The director position was still

vacant when the FVSD experienced a cyber attack over the Labor Day weekend in 2019. The cyber attack was a ransomware attack or an attack where threat actors encrypt a victim's personal data and demand a ransom to unlock the data (Mohurle & Patil, 2017). FVSD started remediation of the attack immediately on all impacted devices, which included any student, teacher, or computer lab devices that were turned on at the time of the attack, as well as domain controllers and onsite servers in the district's technology center. In addition to repairing systems impacted by the cyber attack, the District also upgraded safety measures to protect against future attacks. The District was still working to recover all impacted systems in March of 2020 when the COVID-19 pandemic forced a shutdown of all Pennsylvania schools.

As a result of the attack, and to support the increase of technology in the district, FVSD increased the number of technology staff since 2019 and restructured the organization of the department (Figure 3). As of September 2023, the department fell under a director of curriculum, instruction, assessment, and technology, referred to in this study as the director of technology. A direct report to the director, a technology supervisor oversees a technical support specialist, a network engineer, a network administrator, a web/communications specialist, and a device manager. In addition, a database administrator and digital media specialist report to a supervisor of curriculum, instruction, and assessment, who then also reports to a director of technology.

Figure 3

Technology Organizations Charts: September 2019 and September 2023



Participants

For this study, I used purposeful sampling to identify participants. When researchers use purposeful sampling, it is important for the researcher to select participants who have experienced the particular phenomenon being studied (Creswell, 2016). To ensure that selected participants had first-hand experience with the cyber attack, I included IT administrators in FVSD who were employed in the district at the time of the cyber attack in 2019. Site technicians who were present during the 2019 attack were excluded from the study since the District had removed the group from the administrative group in 2016. While site technicians played an

important role in recovering from the attack, they were not directly involved in the day-to-day planning and remediation at the district level.

Prior to the interviews, I sent all participants an email invitation describing the purpose and methodology of the research, as well as the anticipated time commitment for being part of the study. From the invitations, seven members of the IT administrative team (see Table 1) agreed to participate in the research study through two semi-structured interviews that each lasted approximately 45 minutes. All interviews occurred in person, and I used Otter.ai, a digital application, to transcribe all dialogue. To protect the identity of the participants, I reported all participants with pseudonyms. The participants included:

Table 1

Participants' Title, Years Experience in FVSD, and Responsibilities at the Time of the Interviews

Name	Title	Years	Responsibilities
George	Technical Support Specialist	23	Managed district help desk
Hilary	Web/Communication Specialist	23	Managed district website and communications
Andrew	Digital Media Specialist	17	Managed district filming
Tom	Device Manager	16	Managed all district devices
Haley	Director of Technology	11	Oversaw curriculum and technology departments
James	Network Administrator	22	Managed district network and Internet
Martin	Technology Supervisor	26	Oversaw daily operations of core IT team

Note: Experience is reported as the number of years from the original date of hire in FVSD and does not reflect the number of years in the current position

Technical Support Specialist George

Technical Support Specialist George started his career in K-12 IT in 1997 and moved into a FVSD site technician position in 2001. After several years as a building-level technician, George moved into a technical support specialist role where he was responsible for maintaining a district help desk that received technology-related problems from all FVSD buildings via phone or email. At the time of the attack, George was in the technical support specialist role.

Web/Communication Specialist Hilary

Web/Communication Specialist Hilary graduated from college and started her career in corporate business. After going back to college, Hilary studied desktop publishing and computer graphics, eventually moving into an advertising position, and then transitioned into a web development role in FVSD in 2001. Her position grew to include district communications, and at the time of the attack, her role was web/communication specialist.

Digital Media Specialist Andrew

Digital Media Specialist Andrew graduated college with a degree in communications and worked as a television producer for a large news network. Wanting a change of position, Andrew accepted a video production specialist position at FVSD in 2007. At the time, Andrew was in charge of filming and editing district video content; however, the position evolved to include all technology-based media. During his time at FVSD, Andrew earned a technology related master's degree. At the time of the attack, his title was digital media specialist.

Device Manager Tom

Device Manager Tom initially started his career in construction but moved into corporate technology support roles in the mid-1990s. Tom accepted a job as a FVSD site technician in 2008 and eventually moved into the device manager role where he was responsible for

maintaining all district digital devices. At the time of the cyber attack, Tom was the device manager.

Director of Technology Haley

Director of Technology Haley started her career as a teacher in 1996. In 2004 she transitioned to an independent contractor role for school districts requiring reading services and then moved into a professor role at the university level. During this time Haley completed several graduate programs and her doctorate in education. Haley then accepted a role in the FVSD curriculum department in 2013, moving to the K-12 director of curriculum position in 2016. At the time of the cyber attack, Haley was the director of curriculum, instruction, and assessment.

Network Administrator James

After graduating from college and earning a master's in information systems, Network Administrator Andrew started his career as a medical bill reviewer in the private sector before moving into an FVSD billing role in 2002. From the billing role, James moved into a building site technician position in the district, and then into a database administrator role. As the database administrator, James was responsible for managing all digital program integrations for the school district. James was in the database administrator role at the time of the cyber attack.

Technology Supervisor Martin

After completing two associate degrees, Technology Supervisor Martin started his IT career in the private sector during the late 1990s before moving to FVSD in 1998 as a building site technician. After three years as a site technician, Martin moved into an assistant network administrator position where he was responsible for managing the school district's network. At the time of the cyber attack, he was the network administrator.

Background, Role, and Perspective of Researcher

I started my education career in FVSD in 2003 as an instructional assistant and then moved into a 5th grade classroom position. During my time as an elementary teacher in FVSD, I was involved in the implementation of instructional technology including interactive boards and curriculum aligned technology implementation. In 2016 I moved out of the classroom into an administrative role in FVSD's curriculum department. During this time, I worked closely with federal funding and curriculum development. At the time of the cyber event in 2019, I worked with the technology department to coordinate the implementation of new district digital applications and devices related to curricular programs. As a member of the school district, I had first-hand experience of the cyber event and was involved in assisting in recovery efforts including collecting devices, reimaging endpoints, and vetting new digital and cloud-based solutions. Since 2020, the director of technology, which I report to, has overseen all aspects of the technology department. My experiences on the front end and back end of district technology provide me with a broad lens to capture the experiences of individuals who have lived through a cyber attack.

Data Collection

This qualitative case study includes data from multiple sources to examine how K-12 IT administrators experienced a cyber attack. There are multiple types of data sources that researchers can utilize in case studies (Yin, 2018); however, in this study, I focused on interviews and documentation to explore the feelings of IT staff members. "Interviewing is necessary when we cannot observe behavior, feelings, or how people interpret the world around them (Merriam & Tisdell, 2016, p. 108)" and documentation is helpful in case study research to "corroborate and augment evidence from other sources (Yin, 2018, p. 115). Since it is difficult to

observe the feelings of individuals, interviews allowed me to obtain a deeper understanding of how IT administrators experienced the cyber attack, and documents helped triangulate themes from the interviews.

In this study, I utilized semi-structured interviews, which typically provide a structured set of questions; however, it also provides flexibility in participants' answers and the ordering of questions (Merriam & Tisdell, 2016). In addition, it also allows the researcher to respond to the viewpoints of participants and explore new concepts that participants discuss during the interview process. I conducted two semi-structured interviews with each of the seven participants in person within FVSD implementing an interview protocol (Appendix A and Appendix B). I conducted two interviews to allow participants to reflect and process the purpose of the study in between meetings. It is beneficial to conduct qualitative interviews in the natural setting since it allows the interviewer to see the participants act and behave within the context of the area of research (Creswell & Creswell, 2018). I recorded all of the audio from the interviews using a digital recording device and transcribed the audio through Otter.ai. In conjunction with audio recording, I took handwritten notes in the event the audio recording failed, and to document notable physical reactions during the interviews.

Concurrently with interviews, I collected documents to provide further context for the post cyber attack phenomenon. This included news articles, planning documents, and web postings. All of these documents are considered primary sources, or sources that were recorded close to the time and location of the studied case by a qualified person and demonstrate a firsthand experience of the event (Merriam & Tisdell, 2016). To access out of date articles and archived website postings, I used the Wayback Machine (an internet archive library). The

collection of documents was systematic; however, I included additional resources outside the initial scope if they were relevant to the research.

To ensure the privacy of all data, I stored all data on an external drive that was not regularly connected to outside networks with pseudonyms recorded for all participants to protect individual identities. I also password protected all files on the external drive and stored the drive in a secure location when not in use. After five years from the conclusion of the research, I will permanently erase all files from the external drive and reformat the hardware.

Data Analysis

In case study research, data analysis begins during data collection to avoid unfocused and repetitious data (Merriam & Tisdell, 2016). As I conducted interviews, I reflected on each process and adjusted to promote better and more focused data collection. In addition, following each interview, I reviewed transcriptions and notes to inductively look for themes that might be emerging from the data. Since I also collected documents at the same time as conducting interviews, I began to organize my data during ongoing collection and analysis to promote more efficient retrieval once I collected all the needed data.

Upon finalization of data collection for the case study, I organized all interview transcripts, documents, and researcher notes into a single repository, or case study database, to allow easy retrieval for continuing analysis. By developing a case study database, it also increases the reliability of the study (Yin, 2018). With the development of the case study database, I began coding, which is going through the data and assigning a word or short text that summarizes an attribute of the data (Creswell, 2016; Merriam & Tisdell, 2016). From the coding, I started to inductively look for emerging themes in the data. Once all of the transcripts were coded, I grouped codes to identify a list of themes in the data. At the same time as manual

coding, I entered anonymized transcripts into Atlas.ti, an artificial intelligence (AI) powered thematic analysis tool, to generate themes based on the interview transcripts. Upon completion of manual and AI theme analysis, I compared the generated themes and looked for similarities and discrepancies. As I followed up to inductively look for themes in the data through manual and AI processes, I also used deductive processes to analyze the data for themes related to TTAT. At the conclusion of inductive and deductive theme development, I used documentation identified during data collection to triangulate identified themes and gain a better understanding of the context of the study.

Validity of Interpretation

Validity in qualitative research means that what the researcher is presenting is accurate (Creswell, 2016). A key element of establishing validity in qualitative research is understanding the biases and perceptions of the researcher (Creswell, 2016; Merriam & Tisdell, 2016). In the development of this study, I openly discussed how my own biases relate to the accurate collection and analysis of this case study. To further ensure that this research accurately represents the phenomena in this case study, I employed rigorous data collection and analysis techniques in the methodology (Merriam & Tisdell, 2016). I used multiple data sources, including interviews and document analysis, to triangulate findings and enhance the depth of understanding. Triangulation is using multiple points of data to confirm findings and the application of the process strengthens the construct validity of the case study (Creswell, 2016; Merriam & Tisdell, 2016; Yin, 2018).

In addition to using triangulation during data collection and analysis, when researchers use detailed descriptions to convey findings and present negative information that is contradictory to the themes, it can also help strengthen validity. “When qualitative researchers

provide detailed descriptions of the setting, for example, or offer many perspectives about the theme, the results can become more realistic and richer" (Creswell & Creswell, 2018, p. 200), which can support the validity of the findings. During data analysis and presentation of the findings, I made efforts to provide detailed descriptions to capture the lived experience of the participants. Furthermore, researchers can also make findings more realistic and valid by offering contradictions to the themes they have identified (Creswell & Creswell, 2018). During data analysis, I identified areas of negative or discrepant information to demonstrate that not all perspectives in the research were unified.

To further strengthen the validity of the research I utilized member checking and peer debriefing. Member checking is when a researcher returns broad summary statements to the interviewees to determine if the identified themes are accurate (Creswell, 2016; Merriam & Tisdell, 2016). Once the initial findings were completed, I selected participants to review the themes I identified as a researcher to ensure that they accurately represent what was covered in the interviews. In addition to member checking, I utilized peer debriefing, which is when someone who is knowledgeable about the research topic reviews the findings and provides feedback to help refine the study (Creswell, 2016).

Limitations

In case study research, a researcher will inadvertently bring preconceived positions into the research which can impact their ability to listen to and explore evidence that is contrary to their current positions (Yin, 2018). Any preconceived positions I had prior to research can influence the data I collected and the way I interpreted the data (Creswell, 2016). To compensate for preconceived positions, I have identified the background and perspectives of the researcher and made every effort methodologically to minimize the influence of my personal values,

assumptions, and biases in the reporting of the case study. One way to do this is through bracketing, which is a method intended "to mitigate the potential deleterious effects of unacknowledged preconceptions related to the research and thereby to increase the rigor of the project" (Tufford & Newman, 2012, p. 2). While there are different ways to implement bracketing, reflexivity is an important component of bracketing (Ahern, 1999). To increase my own reflexivity throughout this dissertation I maintained a research journal that included research related interests, personal value systems, potential role conflicts, feelings that could impact neutrality, and surprising findings in the research (Ahern, 1999; Chan et al., 2013).

In addition to potential biases in research, qualitative studies also lack generalizability to other settings since "in qualitative research, a single case or a small, nonrandom, purposeful sample is selected precisely because the researcher wishes to understand the particular in depth, not to find out what is generally true of the many" (Merriam & Tisdell, 2016, p. 254). Given the limited scope of qualitative research, it is important for researchers to remember that meaning from interview-based research is "a function if the participant's interaction with the interviewer" (Seidman, 2019), further limiting application to other settings.

Since meaning comes from interactions that are rooted in the participant/interviewer relationship, my relationship with the participants is a potential limitation. While I did not serve in an administrative role for any of the participants, we did work for the same district in the same department. This prior relationship had the potential to make participants feel more comfortable and they might have been willing to share more, or it could have had an adverse effect and could have limited what participants were willing to share. Either way, the meaning that I derived from interviews was potentially influenced by the working relationship I had with each of the participants.

Ethical Considerations

Qualitative research often involves collecting data from individuals that can include data regarding “emotional topics” that are sensitive to the participant (Creswell, 2016). As such, it is important for the researcher to protect the rights of participants and ensure that the study does not cause unintended emotional harm. Furthermore, since case study research is primarily focused on human affairs and involves interview interactions that may not be as structured as survey research, it is of the utmost importance that researchers protect the rights of the participants and minimize harm (Yin, 2016). Researchers need to address different ethical considerations at each step of the inquiry process, and the initial steps begin before the research is even started (Creswell & Creswell, 2018).

One way I protected the ethics and validity of this study before research began was through the IRB process. The IRB process is designed to ensure the protection of human participants and ensure researchers utilize sound methodological practices. One aspect of the IRB review process was having all participants sign a consent form that outlined the purpose of the research and participants' rights prior to participating in any aspect of research collection. In addition, before any interview, I read a statement that reiterated the purpose of the research, encouraged the participants to be honest while protecting their role as district leaders, and what to expect during the interview. During this statement, participants were also informed that free counseling was available if they experienced any negative emotional impact as a result of the study. To protect the participants’ identities and the data obtained in this study, all files were password protected and stored on a non-networked external hard drive. This decreased the chances of someone accessing the files remotely and gaining access to sensitive information.

Researchers also need to acknowledge ethical considerations regarding relationships with participants (Merriam & Tisdell, 2016). While I did not serve as an administrator for any of the participants, I did have a working relationship with the participants. This required me to consider how my relationships with participants could impact data collection. The first strategy I utilized to ethically account for relationships was participation in the research study was voluntary, so there was no pressure to participate. Next, in maintaining appropriate relationships it is important that I respected participants' relationships and ensured their stories were heard. One strategy utilized to maximize the participants' voices was to review transcripts to ensure that I was not dominating conversations and leading participants to predetermined themes (Siedman, 2019). In addition, since there were pre-existing relationships, I treated sensitive topics with respect and ensured that interview responses did not undermine the participants' role as an administrator or cause unnecessary discomfort. Finally, since researcher knowledge of a particular case and existing relationships can lead a researcher to focus on pre-existing perceptions during data analysis (Merriam & Tisdell, 2016), I used multiple rounds of coding in conjunction with theme development through artificial intelligence to minimize the possibility I failed to identify themes based on my existing knowledge and relationships.

Summary

This research aimed to explore K-12 IT administrators' experiences following a cyber event from a social constructivist perspective. Since the purpose of the research is to highlight individual experiences, I utilized qualitative methods to focus on the participants' voices. Given the specific context of this research in a single southeastern suburban Pennsylvania school district, I used a case study methodology to examine the phenomenon in a specific real-world

context. To offer further insight into the lived experiences of K-12 administrators, I used the Technology Threat Avoidance Theory to help frame questions and deductive analysis.

This case study occurred at a K-12 public school district in Pennsylvania, and while interviews were conducted in 2023 and 2024, document collection extend back to the time of the cyber attack in September of 2019. I used purposeful sampling to identify the seven participants who participated in two semi-structured interviews that each lasted approximately 45 minutes. In addition to interviews, I also collected documentation related to the cyber event including news articles and district communications regarding the attack. I used all documents to aid in the triangulation of themes as they were developed during analysis. Once all data was collected, I coded each of the interviews to inductively identify themes. In conjunction with manual coding, I also used AI driven software to generate inductive themes to provide an opportunity to compare and contrast results. Following inductive theme generation, I also used deductive processes to test themes related to TTAT that appear in the data.

It is important to the research that I acknowledge the limitations of this study, specifically the biases and preconceived perceptions that I brought to the research. Through the disclosure of biases and implementing a detailed and transparent methodology, I addressed limitations related to this study. While I implemented procedures to address the limitations in this study, qualitative research lacks generalization to other contexts. Regardless of the lack of generalization, there is a lack of research surrounding the lived experiences of K-12 IT administrators after a cyber attack, and this study offers insight into how IT administrators and school districts can plan for experiencing a cyber event, and how to mediate an attack once it has occurred.

Chapter 4: Findings

This qualitative case study examined how IT administrators in one Pennsylvania K-12 public school experienced a cyber attack. The purpose of the research was to gain insight into how a cyber attack impacts IT administrators and their perceptions of the school district's cyber environment during and after a cyber attack. Qualitative research, more specifically a case study, provided in-depth data regarding a particular cyber event that occurred in the Fern Valley School District (FVSD).

To explore how FVSD core IT administrators reflected on how they experienced the attack, and how they perceived the period after an attack; qualitative data was collected and analyzed to explore two research questions.

- How do K-12 IT administrators describe their experiences during a cyber-attack within their district?
- How do K-12 IT administrators see a cyber-attack as influencing current practices and policies?

To investigate the research questions, I utilized two semi-structured interviews with the seven participants. The semi-structured format provided open-ended possibilities to allow participants to share their experiences and perceptions as a result of experiencing a cyber attack (Merriam & Tisdell, 2016). A qualitative case study methodology is beneficial when a researcher is attempting to study a phenomenon in a real life context (Yin, 2018). Through inductive coding, four major themes emerged from the data.

For the first research question, the themes of "Nobody's Seen Something Like This Before" and "The End" emerged from the data and examined the IT team's experiences during the cyber attack. "Nobody's Seen Something Like This Before" explored how the team found

themselves in a situation unlike anything they had experienced in the past. The second theme from the first research question was “The End,” which examined when the team considered the cyber attack over in FVSD. Subthemes related to both “Nobody’s Seen Something Like This Before” and “The End,” further capture how the participants described their experience during a cyber attack. While participant responses showed that members of the team considered the cyber attack an unparalleled experience, and also had differing views of when the attack was over, experiencing the attack also impacted their cybersecurity related decisions and processes.

Related to the second research question of how experiencing the cyber attack impacted the core IT team’s current practices and policies, two themes emerged from the data. The first theme, “Finding a Voice” examined how communication within the department and outside the department changed after the attack. The final theme related to the second research question was “Trust Nothing” and explored how experiencing the cyber attack led to a lack of trust in anything cybersecurity related. Overall, participants expressed that the cyber attack changed the way they view and address ongoing security threats.

Question 1

The first research question explored how FVSD core IT team members described their experiences during a cyber attack. From the data, two themes emerged, each with sub-themes. The first theme from the data was “Nobody’s Seen Something Like This Before” and captured how the core IT team described their experiences as having to navigate and respond to a unique event that none of the members had encountered in the past. Since this experience was unique in the collective experience of the team, it shaped their reactions and emotions. The second theme that emerged from the data was “The End” which explored the core IT teams' perceptions of how the team viewed the attack as being over. While some team members attributed the end to

specific events, others indicated that the attack left a lasting impact on the way the team perceives the current cybersecurity landscape and their current practices.

Nobody's Seen Something Like This Before

Only three days into the school year, students and staff left the Fern Valley School District for the Labor Day weekend. The first indication that something technology-based was wrong came through a help desk ticket on Saturday morning. George received a report that a staff member was unable to access files on their shared network drive. About the same time, another help desk ticket came in from a high school teacher who was concerned that he was locked out of server files hosted in FVSD for a program he had developed. George recalled as he first looked into the reports, "the server was being taken down actively, though I didn't realize it was being taken down actively because nobody's seen something like this before." As George recalled in the interviews, the cyber attack was unlike anything else the core IT team had experienced previously. Interviews captured how throughout the attack, the uniqueness of the event affected the decisions, reactions, and perceptions of the core IT team, and without prior experience, participant responses showed that core IT team members struggled to make sense of the situation. Due to the unparalleled experience, two subthemes emerged. The first subtheme, "Not Knowing Completely What's Going On" examined how the team's perceptions and reactions were impacted by a lack of information to help shape their decisions. The second subtheme, "Complex Emotions" explored how the unprecedented attack led to the core IT team members experiencing a range of emotions as they navigated the cyber event.

Not Knowing Completely What's Going On. For the first theme, the initial subtheme to emerge was "Not Knowing Completely What's Going On," which explored how the newness of the cyber attack experience impacted the core IT team's ability to gain a comprehensive

understanding of what was going on at any given moment. At 7:55 Sunday evening, Fern Valley School District sent their first communication to district staff that referenced a “network vulnerability” and in bold letters, “At this time, we ask that you please refrain from using any district account (e-mail, network) and device” (Fern Valley School District, personal communication, September 1, 2019). At the time staff received the email, Haley, along with three core IT team members, Martin, George, and Tom, had been in the district’s technology center for close to four hours trying to assess what exactly had occurred. Haley remembered siting in the technology center, still unsure of what exactly was happening, but thinking that something should be communicated:

> And while we're sitting in silence in the NOC (technology center), one of the things I do is I get communication out to the families and to the teachers to say do not use your device anymore. Again, not knowing completely what's going on, but knowing I didn't want whatever was going on to get worse. (Director of Technology Haley, interview, January 10, 2024)

From the moment the core IT team realized that something unusual was happening in the network, and throughout the remediation process, the team struggled with “not knowing completely what’s going on.” Since no one had experienced a large scale cyber attack, the team had to address challenges and make decisions with incomplete information. Sitting in the technology center, Haley didn’t have a full understanding of the situation, and recalled that at this point the team still hadn’t confirmed it was a “cyber attack,” but she knew she had to do something so things didn’t “get worse.” Haley also expressed that people outside of the department, including the superintendent and assistant superintendent, wouldn’t understand what was going on and it would require trust as decisions were made. Regarding the initial

communication, Haley said “the people I were talking to weren't understanding what was happening… and maybe thought I was overreacting… but in some way they didn't because they allowed the message to go out.” Even though FVSD hadn’t even confirmed they had experienced a cyber attack at this time, the core IT team had to move forward, figuring out as much information as they could at the time, and make decisions based on the limited knowledge that was available.

When Andrew was first contacted on Sunday that something was wrong, he remembered he was skeptical that the issue was even a cyber attack since the core IT team still didn’t know what was happening and he had never experienced an attack. While sitting by the pool with his family, he had to Google cyber attacks to gain a better understanding of what might be occurring. He recalled as he read more about cyber attacks, he reflected, “wow, this is actually more of a possibility than I care to admit, and then I thought, we’ll wait for more information because we’ll better be able to know what direction once Martin arrives at the NOC (district).” Since this was a new situation that none of the core IT administrators had experienced, Andrew felt that he had to do more research to try and understand what was happening. A lack of knowledge about the event also delayed Andrew’s reaction since he was “waiting for more information.” While Andrew indicated that having to research what a cyber attack was delayed his response, other members of the team felt the lack of knowledge impacted the team’s communication.

Upon hearing about the attack, Hillary said that she could tell something was wrong, but didn’t quite understand the scope of the issue:

> Martin called me and I can tell by the tone of his voice, we were in an unusual situation. And because it was so new to everybody, I think we all spoke differently because we weren't sure- was uncharted territory. So, we weren't sure. At least I didn't know. You felt

> like you didn't know what to say, and how to say it. (Web/Communication Specialist Hillary, interview, January 4, 2024)

Hillary described the attack as an “unusual situation” and that it was “uncharted territory,” showing how she, and the rest of the team, did not have experience with this kind of situation which impacted her ability to know what was happening. Since the team did not know everything that was going on, Hilary stated that it affected how the team communicated internally regarding the attack, indicating “we all spoke differently” and she didn’t know “what to say, or how to say it.” So, a lack of knowledge of what was going on shaped the team’s internal communications as they determined what had really occurred during the cyber attack.

Even after Martin confirmed the district had indeed suffered a cyber attack at 1 AM on Monday morning after finding a digital ransom note on one of the servers, he still was unsure of the breadth of what had happened. Not knowing the true extent of the damage, Martin recalled having to assume that everything was impacted. Martin recalled in the interviews that “we can't trust anything… we have to assume everything has been corrupted… anything digital has to be addressed and assumed corrupted.” With a lack of knowledge, visibility into the network, and prior experiences to fall back on, Martin speculated that everything digital in the district was “corrupted.” In addition to not knowing the damage locally within the district, Martin also worried about the unknown if the threat actors took anything out of FVSD:

> My concern is did they get data? Do they have any information from us? Things are being destroyed, files are being destroyed or being corrupted, but do they have backups? Do they have copies of these files? Do they have data that they shouldn't have? It’s just a dreadful thought. No matter what the overall condition is afterwards, when it's all done- if

> they still have our data, that's a terrible situation. (Technology Supervisor Martin, interview, January 30, 2024)

While Martin struggled with not knowing whether he could trust any piece of technology in the FVSD, he also didn't know if the threat actors had stolen the district's data. Not knowing whether data was stolen concerned Martin because regardless of whether the team was able to remediate the cyber attack locally, if the threat actors still have the data it's "a terrible situation" since the district did not know what would happen with that data. Due to the fact that Martin and the rest of the team did not know all of the details of what technology was impacted and what data was impacted, and that the team could not compare this to prior experiences, it made it difficult to share information with others about what was going on.

Hilary, who was responsible for sending all official FVSD communications, shared in the interviews that communication outside the core IT team was a challenge since it involved balancing what was known and what was unknown. She highlighted that a challenge for the core IT team was answering "do we know what's actually happening and what's still there?" Since the team did not have the answers to this question, Hilary said it led to ambiguous communication, even though FVSD administrators wanted to keep the district informed:

> We wanted to be informative, but I felt like we were limited in our ability to be transparent, because of the sensitivity of the situation. And we were in it. You know, we were figuring it out while we were trying to sort of communicate about it. (Web/Communication Specialist Hilary, interview, January 4, 2024)

Since the core IT team was "figuring it out" and still trying to understand what was going on in the district, it impacted how "transparent" the team's external communication could be with people outside of the core IT team. Not having the answer to "what's actually happening" also

impacted the timing of communication. Hilary said, in regard to communication, the team "belabored that (timing) a little bit because you're trying to understand what you're even dealing with." Hilary's responses demonstrated that due to the team's insufficient information related to the attack, it was difficult to provide timely communication to anyone outside of the team. Interviews showed a lack of knowledge about what was happening during the cyber attack impacted communication between team members. In addition, the lack of knowledge also influenced the detail and timing when the team was communicating with the rest of the district.

Participant responses indicated that from the moment that core IT team members were informed of unusual events on the network, to the first district communication referencing a "network vulnerability, through confirming it was a cyber attack and the attack's remediation, the core IT team was impacted by "not knowing completely what's going on." Participant responses further showed a lack of prior experience with cyber attacks limited the knowledge of team members and caused the team to research what was happening, make assumptions about the impact, and make decisions without all the details. Furthermore, a lack of knowledge and experience led to difficulties with team members communicating within the group and also communicating externally what was happening to the rest of the district. Overall, since the cyber attack was unlike anything the core IT team had seen before, it led to situations where no one knew exactly what was going on.

Complex Emotions. The second subtheme to emerge from "Nobody's Seen Something Like This Before" was "Complex Emotions" and explored how the new experience of a cyber attack elicited a range of feelings in the core IT team. Throughout the cyber attack, core IT team members struggled with knowing the details of what was happening during the event. With this uncertainty, the core IT members experienced a range of emotions that included fear, paranoia,

and anger which were described in the interviews. George specifically described the unique situation of the cyber attack and commented that with a lack of information about who was responsible "paranoia… sets in, I think for everybody." He went on to reference the questions that were going through his mind of: "What happened? How did it happen? Is my name involved? Can they trace back to something I did? Was it a website that I went on? Were they going to replace me?" George described paranoia related to all the unknowns, but specifically traced it back to whether he would be blamed for the cyber attack, questioning whether "Is my name is involved?" or "Can they trace it back to something I did?" In addition to the paranoia associated with being blamed, George also was fearful that if he was blamed he would lose his job when he considered "Were they going to replace me?" Since the cyber attack was a new and unique experience for George, he considered a lot of questions regarding his potential involvement in the attack and his future in the organization. These unknowns ultimately impacted his emotional reaction. Furthermore, since all of the core IT team members were going through the new experience, it also impacted their communication with each other.

In his interviews, George recalled members of the core IT team were not openly talking to each other "for fear of self-preservation" and would withhold information in an effort to protect their own culpability:

> There was a lot of, there was a lot of secrets being held back, and a lot of times you could feel… you couldn't tell if somebody was talking about you, or if you came up in conversation… because at this point in time, again, the idea you know, everybody's looking for somebody to point at. (Technical Support Specialist George, interview, January 4, 2024)

George felt that after the attack that people were holding a lot of "secrets" and were not being truthful with one another, adding to the feeling of paranoia. Again, George expressed a strong fear of being blamed since "everybody's looking for somebody to point at." While this atmosphere heightened feelings of paranoia, George recognized that team members were just trying to protect themselves through self-preservation in order to navigate an unparalleled experience.

Like George, Hilary questioned whether she would be held responsible for the attack, and referenced the need for self-preservation:

> Because when something like this happens, you feel like, back to the blame thing, is somebody gonna get… how did this happen?... did somebody open an email?... who was that person?... You know, and nobody, really…we all sort of… you sort of want an answer, but you don't want an answer. (Web/Communication Specialist Hilary, interview, January 4, 2024)

Hilary's questions of "how did this happen?...did someone open an email?...who was that person?" captured the same paranoia that George experienced related to whether they would be blamed for what happened. Hilary also expressed a contradiction between wanting to know who was responsible and not wanting to know since "you sort of want an answer, but you don't want an answer." Hillary was hesitant to know who was responsible because she was worried it would be her:

> You know, part of you worries about yourself, even though I think for the most part we're selfless. You go through a blip of worrying about yourself, and I don't want to say selfish, because it's not… not a standard selfishness. It's the, it's the present self-

> preservation selfishness of like, did I do this… like… how did this happen? (Web/Communication Specialist Hilary, interview, January 4, 2024)

Hilary considered "did I do this?," showing, like George, that she was concerned someone would blame her for the attack. Also, similar to George, with the fear of potential blame, Hilary felt the need to worry about herself. At the same time, she struggled between "self-preservation" and feeling "selfish," stating that what she was feeling was "not a standard selfishness" because everyone had to look out for themselves.

While some members of the team had an emotional response of fear and paranoia due to the potential of being blamed, other members of the team felt anger towards the situation based on how they experienced the situation. When Martin was asked how he felt during the attack he mentioned he had never considered how he felt. After pausing for a brief time, he expressed that he felt violated and angry:

> It's dreadful- violated, we've just been violated by some out outside entity, some exterior external source… an external entity successfully penetrated in some form our defenses and did everything they could to manipulate and create as much damage as possible, deliberately. So, the feeling of violation… I was angry for the district. (Technology Supervisor Martin, interview, January 30, 2024)

Martin explained his initial reaction after the attack was he felt "violated" by the people who orchestrated the attack. The feeling of violation stemmed from the fact that a threat actor outside of FVSD intentionally manipulated and created "as much damage as possible" and left the school district without a working technology infrastructure. Martin's feelings of violation also led to feelings of anger directed at the outside threat actors because he cared about the school district and didn't want anything to happen to FVSD. In this situation, Martin's anger was directed

outside of FVSD at the threat actors; however, the attack also led to team members directing anger at members within FVSD.

As the cyber attack progressed, Haley also referenced she had feelings of anger, but her feelings were directed internally to anyone in FVSD who was not going through the same unique situation the core IT team was experiencing. She felt her perspectives regarding cyber threats changed dramatically during the first 12 hours of the attack and it made her angry that others in the organization weren't seeing or feeling the same experience she was having. She said in the interviews "my entire worldview shifted in 12 hours of silence, and anybody else who didn't experience that same change at the rate that I was, angered me, and it frustrated me, that they could be so ignorant to it." In another interview, Haley expanded on her feelings of anger towards staff members in FVSD regarding how much people use technology, but at the same time do not care how it works:

> I was angry that people underestimate how much they rely on technology. They take it for granted. They underestimate how complicated it is. And that it is everywhere. And I know I was angry. I was angry at most people for their lack of care, their abundance of ignorance versus lack of abundance of ignorance of how they live their lives. And that they could not see that potential danger or evil is sitting right next to them or in their hand. (Director of Technology Haley, interview, January 10, 2024)

Haley was angry because people took technology for "granted" and "underestimated" how much work it required to make technology function in the schools. She felt it was everyone's responsibility to be informed about technology and she was angry because people were unaware of the "danger" and "evil" that existed all around them in the technology they were using. Haley felt members of FVSD did not take responsibility for their technology use. Haley's interview

responses, like other members of the core IT team, demonstrated that the new experience of the cyber attack caused a complex range of emotions for the team members.

The End

The second theme that emerged related to how core IT team members experience a cyber attack was "The End," and explored when team members considered the attack over. As the cyber event progressed, core IT team members navigated an event unlike anything they experienced before, not always knowing what was going on, and experiencing a range of emotions. For some, the feelings of not knowing what was going on subsided as the team achieved different milestones during the remediation. For others, the attack left a lasting impression. In the interviews, Andrew distinguished two different components of the end of the cyber attack. While Andrew referenced the end of the attack by FVSD "physically" returning to normal after the attack through different tangible events, he added "that it's never over mentally." In the interviews, participant responses showed that other team members had differing perspectives of when they experienced that the cyber attack was over. Some viewed the attack as being "physically" over through various milestones, but many also referenced that the attack is never really over. From the data, two subthemes related to "The End" emerged capturing the participants' differing opinions of when the cyber attack was over. The first subtheme was "Milestones" and explored the tangible moments during the cyber attack when team members considered the attack over. The second subtheme was "Never Really Over" and examined the team's perceptions that the cyber attack will always be with them mentally.

Milestones. The first subtheme that emerged in relation to when the core IT team considered the cyber attack over was "Milestones" which examined tangible events during the cyber attack that team members identified as the end of the cyber attack. From the school district

lens, FVSD released their final official district update twenty-five days after the attack (see Figure 4) with the first bulleted item focusing on Internet services being restored to four of the nine buildings as well as the district office. At this point, the update referenced that the district had restored devices for staff members, but students still did not have devices, and lunch systems were still not online. By the beginning of November, all updates and FAQs related to the cyber attack were removed from the district website. While FVSD had removed information regarding the attack from the website in November, members of the team each experienced different milestones for when they considered cyber attack over.

Figure 4

Final District Update on Cyber Attack: September 25, 2019

Sent: Wed 9/25/2019 5:33 PM
Subject: Network Disruption Update #6

Dear FVSD Parent/Guardian,
Over the last few weeks we have made tremendous strides in remediating the damage to our network. Progress has been steady, and I am pleased to report that we are now hitting key milestones that will enable us to resume normal operations soon. As you will see in the details listed below, our situation is improving rapidly.

- As of today, we have restored Internet service to the High School, Fern Creek and Fern Field Middle Schools, Fern Pond Elementary School, and the District Office.
    - We anticipate Internet service being restored to all remaining schools by the middle of next week.
- While we continue to clean and re-image all computers, the process of distributing restored machines is ongoing.
    - As of today, computers are being distributed to staff members, and the distribution of devices to students should begin soon.
- Home Access Center (HAC) - HAC is now available for parents using their existing username and password. Click here to access HAC. Parents may use the "Forgot My User Name or Password" link for login assistance.
- Lunch Accounts – Cafeteria staff have been recording all student lunch purchases. Student lunch accounts in MySchoolBucks are secure but are currently not being updated when lunches are purchased. Once cafeteria computers are back online, student lunch accounts with MySchoolBucks will be updated and a grace period will be available for parents to fund student accounts.

Looking ahead, we will continue to restore other systems and instructional applications for students' use. I am grateful for your patience and assistance as we emerge from this difficult period in our District's proud history.

Sincerely,
Superintendent of Schools

Note: Superintendent of FVSD Schools, personal communication, September 25, 2019

Hilary recalled that she felt relief when FVSD "resolved our negotiations with the attackers and had the ability to restore some things as a result of that." While she recalled that this was roughly two weeks after the attack, she said it felt like an eternity. Hilary went on to explain, that while the threat actors leaving was "an invisible thing and not tangible," and as long as they were in the picture "you didn't know like when was another shoe going to drop" or if things in FVSD were going to get worse as a result of the attack. Even though the threat actors were physical, Hilary described them as "invisible" and "not tangible" because the core IT team never saw the threat actors or directly interacted with them. While Hilary experienced the attack as over based on a definitive milestone for FVSD, others experienced the attack as over based on their personal experiences.

Martin also experienced that the event was over after confirming the attackers were gone, but because of his network-based position in the department, he did not consider the attackers gone until weeks after negotiations were completed. During the interviews, Martin remembered being in the district's technology center by himself on a Saturday bringing up file servers. Martin described the situation as "all of the embers are just kind of settling down and now we're working our way up," indicating that things were no longer getting worse in the district and the core IT team was starting to bring back pieces of technology that were destroyed. He recalled he had already located every device that was on the network, and they were being re-imaged, and he was getting ready to reconnect the district to the outside world via the Internet. While he was working, he recalled looking down at his computer, and he saw a little folder on the screen, and recalled "I'm looking at this little folder that's not…I'm not used to seeing this little folder, on the C: drive, and I said to myself, oh my god… it's not done yet… there's something out there now." Martin mentioned at this point in the interview that their outside

consultants had warned that one of the biggest potential issues during recovery was reinfection if any part of the malware still remained on any of the thousands of machines in the district. Martin had felt to this point that FVSD was moving in a positive direction, and as he looked at this unknown folder, he believed he was now "looking at a machine that's already infected."

Martin's positive outlook quickly changed to one of fear because he thought the threat actors still had access to the district:

> I thought I was gonna have a heart attack… that panic. Like, we're already weeks into this process, and I'm thinking we're going to be going back to a meltdown in no time at all… it was so daunting, and I felt… I was done. I felt like I was really done.
>
> (Technology Supervisor Martin, interview, January 30, 2024)

After weeks of trying to restore technology access to FVSD, and feeling like things were moving in a good direction, Martin was now afraid he had just reinfected the entire school district. The fear of starting over made Martin feel like he was going to "have a heart attack" and that he reached his breaking point since he felt "I was really done." However, after a quick search on his phone, Martin confirmed that the folder was not malicious. Martin recalled "he had to get through that scare" to feel the attack was actually over. After this scare, Martin felt milestones started to fall in place, such as restoring the Internet and returning devices to teachers and students. At this point, he perceived FVSD was able to "get back to some assemblance of normalcy." While Hilary and Martin cited specific moments they considered the attack over, Tom experienced the end of the attack when duties related to his specific position were completed.

For Tom, while work to rebuild the district continued, he felt the attack was over once every staff member and student in the district had a device with the new endpoint protection.

Since Tom was in charge of managing all devices, he felt the district was in a good place "once the customers all had what they needed to do their jobs, or do their studies, or teach all the portions that make this machinery go." Tom also mentioned that when he started to get requests for specific software installs for computer labs, he felt that "if you can complain about the minutia, the big problem is mostly gone." Tom's experience of the attack ending focused on feeling he had completed his part of the recovery efforts and everyone in the district had the tools to return to normal teaching and learning.

While Hilary, Martin, and Tom referenced specific milestones as the end of the attack, Andrew experienced the end of the event as a progressive series of milestones. Andrew initially indicated the attack was over in the first few days for the core IT team since "there was so much that was locked or destroyed that you pretty much knew and nothing more was happening." Andrew then added in the interviews that reconnecting to the Internet was a major milestone and said, "I think that was a big step to feeling like a lot of a lot of it was over." Andrew also indicated that distributing devices to staff and students was yet another milestone. For Andrew, the experience of the cyber attack ending was not a single event, but rather a progression of milestones that showed the district was returning to normal.

Never Really Over. The second subtheme related to when members of the core IT team considered the attack over was "Never Really Over" and examined how members of the team felt the cyber attack was ongoing and never ended. While milestones were important to Andrew, he also cited in his interviews that while physically FVSD was recovering, mentally the attack was "never over." After recalling multiple tangible landmark events during recovery, Andrew concluded that while there were milestones and the district started to return to normal after the cyber attack, "the impact is forever." He believed that while "there is endpoint protection and

there are things that are ongoing that keep people safe," the cyber attack was an education that you need to remain vigilant:

> I don't know if I would ever say it's really over because attacks have increased. I would say we heard more about schools being attacked after we were… so it's about vigilance. (Digital Media Specialist Andrew, interview, January 8, 2024)

Since there are ongoing threats of cyber attacks and attacks on schools are increasing, Andrew experienced that you can never consider the attack completely over because you are always improving efforts to "keep people safe." Given the potential for future attacks, Andrew felt that organizations need to remain "vigilant" in their security practices to minimize threats in the future.

The experience that the attack was never really over was also referenced by George. In his interviews, he mentioned that as long as there are threat actors attacking organizations, then the cyber event will never be over for the district:

> I don't think it is quite over, because as long as there's actors out there still doing what they're doing, and there's still money to be made in all this, you're always going to still be a target to some degree. So, nothing is actually ever over, and we're always being looked at, and I believe that we're always being tested. (Technical Support Specialist George, interview, January 4, 2024)

Like Andrew, the potential for a future attack led George to feel the attack was never "quite over." George felt that as long as there are threat actors and "money to be made," attacks will never go away. As a result of experiencing the cyber attack, George also feels that FVSD is "always being tested" showing that there are constant ongoing cybersecurity threats.

Since there is the need for ongoing cybersecurity, Haley also believed that the attack is never over, and it is now ingrained in every member of the core IT team. During the interviews, regarding the end of the cyber attack, Haley recalled, “it's not over…it is with us… it is the ‘About us,’ it’s in our fabric.” Haley went on to say that there are attacks every day and FVSD will experience other attacks. While Haley felt that the district would experience another attack, she recalled she had recently told the school, “but the next time it will be different, and our recovery will be better and quicker.” Haley believed that as a result of experiencing the attack, and the ongoing impact on the team, the team would be better prepared in the future to address potential threats. Haley added on a personal side, that when another attack occurs “that the posture of the sky is falling, and the wanting to throw up driving back and forth to work would be very different.” With the experience of the cyber attack and its lasting impression of never being over, Haley felt that not only was there a change in the way the team prepared for future attacks and the way they would handle future attacks, but she would also personally handle future attacks differently as well.

Even with the potential for future attacks and ongoing vigilance, James referenced that while a future attack is a possibility, he is positive that the team is in the best position they can be in:

> Is it, when not if? For folks it hasn't happened to yet that haven't taken some of the steps that we've taken because it happened, you know that we've tried to share the knowledge on in so many different forms and ways. If they haven't taken that on… it's certainly when, not if… you can't say it's not ever going to happen again. Can we say that? I'm not sure how we could be in any better of a position than we are right now, to hopefully prevent it. (Network Administrator James, interview, January 17, 2024)

From going through the attack, James feels the vigilance and outlook on cybersecurity of the core IT team has set up FVSD in the best possible position if an attack were to occur again. James also expressed the need for other organizations to listen to the experiences and impact of groups that have experienced an attack stating, “we’ve tried to share the knowledge in so many different forms and ways.” So, in addition to feeling that while the cyber attack was physically over, James believed another attack was a probability, and it was important to share FVSD’s experiences to help other organizations.

As a result of experiencing the cyber attack, some core IT team members felt the attack was over based on physical milestones as the district recovered, while others had personal experiences that signified the attack was over. Even though core IT team members referenced milestones as part of their experience, most members of the team also referenced that the attack is “never really over” and the experience is now part of the “fabric” of the group. Since there are ongoing threats, and there is the potential for future attacks, team members feel there is a need for ongoing vigilance to protect FVSD. The cyber attack experience has left the team feeling there will be future attacks, but as part of the attack never being over mentally, the team also expressed that they hope their current security posture is set up to make sure another attack does not have the same profound impact as the original event.

Question 2

The second research question examined how experiencing a cyber attack influenced FVSD’s core IT team’s current practices and policies. From the data, two themes emerged. The first theme from the data was “Finding a Voice” which explored how the core IT team feels that experiencing the cyber attack improved their communication between team members and between other district departments. The second theme that emerged was “Trust Nothing” and

showed how after going through the cyber attack, the core IT team felt they could not fully trust the tools they have in place to prevent future attacks. Overall, experiencing a cyber attack led to perceived changes in the security practices and policies of the core IT team.

Finding A Voice

Interviews indicated that after the attack, there were many changes within the district that impacted the daily functions of the core IT administrative team and one of the biggest was a change in the culture around communication about technology. Members of the core team referenced in the interviews that before the attack they felt siloed within the department and pressured to "make things work" by administrators outside of the department. After experiencing the attack, during the interviews, the core IT administrative team expressed a positive shift in communication between team members and between other administrators in FVSD.

Andrew expressed during the interviews "I think going through the shared experience and everybody supporting the process of the cyber attack helped us understand that there is a better way for us to work together as a team beyond whatever our title may be." Before the attack, team members expressed that other members didn't talk openly with each other about projects related to their specific position, and after the attack, team members felt they were in constant communication with each other to make sure they were developing comprehensive solutions for problems. In addition to internal communication, core IT members also described a change in communication with other administrators as a result of the attack. Andrew felt experiencing the attack "definitely changed the way people communicate with each other in a positive way because people were able to have a voice who had ideas and directions that could be heard and then evaluated by cabinet." Andrew described that after the attack, district leaders listened to the recommendations of the core IT team members before making decisions that impacted

technology. Participant responses showed that core IT team members believed improved technology related communication, or finding a voice, had a positive impact on the progression of the department after the cyber event. As a result of the attack, the core IT team described a culture where internally they were able to find a voice because they were no longer siloed by their title, and organizationally they were able to find a voice because other administrators in the district considered their recommendations before making decisions.

When describing their experiences before the attack, core IT team members described their work environment as siloed and there was a lack of communication between different positions on the team, which limited their voice within the department. Andrew recalled prior to the cyber attack that the culture of the FVSD core IT team was different, and it led to a lack of communication:

> I think it was the culture and structure of what existed that just landed the tech team in a silo. Some was the learned behavior of members of the department and lack of access to sharing thoughts and ideas. (Digital Media Specialist Andrew, interview, January 8, 2024)

Andrew believed that the culture of being siloed in a position impacted pre-attack communication since team members were not "sharing thoughts and ideas." Tom also recounted in his interviews that there was an internal culture regarding communication that limited how the team interacted since "we didn't have meetings- we didn't go over anything- nobody knew who knew what." Tom felt that a lack of meetings and communication limited team members' voices before the attack, and he was unaware of what information other team members had that might influence a decision. Since team members lacked a voice within the core IT team, there was an impact on FVSD's cybersecurity practices. Hilary remembered the pre-attack environment as

“there wasn't as much discussion within the department freely to talk about network security.” Prior to the attack, team members recalled not communicating with each other, and this lack of voice internally led to team members not knowing what each other was doing and negatively affected their security practices.

During the interviews, Tom explained that going through the attack pushed core IT team members out of their “comfort zones” and there was a shift from pre-event communication of staying in your silo to team members making sure their voice is heard in all department projects:

> Everybody used to just stay quiet and do their own thing- if they were asked they would speak up. Now it's not that way, in any way shape or form. If I talk about something that pertains to device deployment, and James hears it and has a question, or doesn't like something about it, we're talking right then. There's, there’s no filter. There's no “Oh, I wish I knew.” As a result of the attack, it's talk it out, then and if it's not something that's we're both in alignment with, schedule a meeting, loop in other people to get some insight into it. (Device Manager Tom, interview, January 18, 2024)

Tom viewed that communication had changed after the attack within the team and now “there’s no filter,” so team members are listening to each other and making suggestions on how to improve projects. Also, if the team members are not in agreement, then they make sure they “loop in other people” so that everyone has a voice in how a project proceeds. Tom added in the interviews that the shift to everyone having a voice within the team was hard for him because it required a lot of “pride swallowing” since his ideas were not always the direction a project would proceed.

Haley expanded on how the team now considers others’ opinions, stating in the interviews that she will not move forward until someone else is going up the “ladder” with her

when the team is initiating a new project or assessing new security threats. She also noted in the interviews that this is a change from prior to the cyber attack since before the attack "we were together, but we were individuals." She also acknowledged the benefits of moving forward as a team since "we figure out what we need to do, and how we're going to support each other, and that makes it feel way more manageable." While some team members expressed that it can be hard listening to others' opinions and voices in decisions, Haley believed it is important to support other team members and that having everyone as part of a resolution makes everything feel more "manageable." So, after the attack, the core IT team felt that communication between team members improved and positively impacted the team's actions.

While the FVSD core IT team observed a shift in their internal communication practices, the cyber attack also led to a shift in communication outside of the department. Prior to the attack, Martin recalled that the mentality of the district was that "IT was never at the table for discussions about things… we were just told what we're going to be doing, what's coming next, and what resources are going to be provided for that." Without a voice "at the table," Martin felt that the core IT team didn't have an opportunity to help inform how projects would happen and establish proper timelines and resources. After experiencing the cyber attack, responses also showed that core IT team members felt they found a voice with other administrators.

During the interviews, Haley referenced that the change in communication or voice, both internally and externally, was attributed to the core team feeling more comfortable with who they are and what they have to offer. She believed that the core IT administrative team had regressed in communication prior to the attack due to cultural shifts, but regained what they had lost after the attack:

> I would say they have changed only because their comfort has increased. And there is self-efficacy, whatever you want to call it, has increased. And I believe, and I wasn't here when they all started, but I believe that was all there. But I believe over the years, you know, there was a protective layer put over it, or there was a layer removed from each time that they didn't have the voice… they didn't have the support. (Director of Technology Haley, January 25, 2024)

Haley felt that before the attack, FVSD had developed a culture where the core IT team did not have a voice in what was happening regarding technology and that they gradually put up a "protective layer" to shield themselves against a lack of support from the rest of the district. This ultimately led to a lack of external communication. After the event, Haley believed that core IT team members regained a level of comfort and self-efficacy, which led them to start voicing their opinions again.

Haley also went on to share a story about Martin who had recently told the superintendent that he could not access his digital files saved in the district from home since it was a security violation. Haley highlighted this as a huge step because prior to the attack everyone on the core IT administrative team knew accessing the drive from home was a risk, but no one on the team would say "no," especially to the superintendent. Interview responses showed the core IT team now believes they need to stand up for what they know will keep the district safe and they need to voice their opinion regardless of the person making the request.

During the interviews, Andrew also acknowledged there was a shift in communication after the attack and expressed that it is important for core IT team members to feel confident in expressing their opinions because so many of the daily operations of FVSD rely on technology:

> Every…all components of the school district move together, technology and curriculum, and student safety, all those things. So, I think that it (the cyber attack) really opened up dialogue. It opened up communication between people who do not have communication. opportunities with each other- IT department directly the superintendent. There was a lot of conversations that happened in conference rooms that usually went through someone, went through an individual versus, you know, other members of the team having direct access. (Digital Media Specialist Andrew, interview, January 11, 2024)

Andrew perceived that it is crucial for technology to work together with other departments in FVSD because technology is a part of most projects that are happening. Andrew also emphasized how the cyber attack "opened up dialogue" and gave team members a voice in those projects, and he expressed the importance of the shift to "direct access" to other departments. Andrew's experience before the attack was technology conversations with other district departments went through one person, and the rest of the team was not present for meetings. Andrew did not feel that this method of communication was conducive to everyone having a voice.

Haley, also articulated the importance of having technology voices at the table since "as you know, anything that's going to be any idea that anybody has, you know, invite somebody from the technology department because it's bound to have some type of technical component." Haley explained how technology is pervasive in so many aspects of the day-to-day operations in the school district and the importance of technology working together regardless of the department. Haley went on to say, "so from facilities, to tech, to food service, to safety, to our transportation services… so since everybody was impacted…the culture was improved." Haley indicated that because so many departments outside of technology were impacted by the cyber attack, it helped improve the communication culture where technology voices were valued. With

the realization of the importance of technology within the district, Haley perceived departments outside of technology had more respect for the core IT team, which facilitated open dialogue with the core IT team.

Martin reflected on the current communication culture during the interviews and expressed that after the attack, there has been an increase in communication outside the department, and that discussions now happen much slower so everyone can have a voice. He also attributed that this shift in communication is because more people respect the need for technology to be part of the conversation. Martin felt that before the attack "there was no discussion" but after the attack "now there's lots of talk…discussions…conversations are slowing down… there's a whole lot more respect for the communication needed." Martin now believes there is more respect for what the core IT team does, and other departments are more willing to engage in communication with the department since members of FVSD saw the prevalence of technology when the cyber attack occurred.

Participant responses demonstrated that after experiencing the cyber attack, communication between the core IT team and members outside the team increased. Members of the core IT team expressed prior to the attack, the team received directives and didn't have a voice in how technology initiatives proceeded. Then during the cyber attack, all departments in FVSD were impacted by the lack of technology and realized the importance of the technology department's feedback for decisions. In addition, the technology department felt that members outside the core IT team developed a greater respect for technology because of its prevalence in the district. So, as a result of experiencing the cyber attack, core IT team members shared that increased internal and external communication had a positive impact on cybersecurity practices and policies.

Trust Nothing

The second theme related to how a cyber attack influenced the core IT team's cybersecurity practices and policies is "Trust Nothing" which examines how the team now has a heightened sense of what they consider a cyber threat. Participant responses showed the cyber attack left a lasting impression on the core IT administrative team. Despite finding a voice in both internal and external communications, which some members of the team attributed to greater trust, the team also adopted new robust tools to help minimize cyber threats that included endpoint protection. However, as a result of experiencing a cyber attack, the team expressed they have adopted a posture that you can't trust that anything is ever secure. Haley explained in the interviews that the team now approaches cybersecurity with the view that "you don't trust anything…we don't think we are ever safe…we don't think we ever will be…we react to the smallest thing in the effort to change people's behavior." Haley believed that regardless of how small a threat might seem, the core IT team cannot trust a threat is benign and the team needs to treat it as if it is capable of causing the destruction of the original cyber attack. Haley went on to say that she treats every threat as if it's the day of the cyber attack "all over again" and that even if it's the middle of the night, she is making phone calls, sending emails, and treating it like it's "day zero." Regardless of the layers of security protection and the perceived quality of their tools, with a fear of experiencing another cyber attack, Haley felt that the team can never do too much to be safe and there is no such thing as a minimal cyber threat.

George expanded on the lack of trust and linked it to the fear of experiencing another cyber attack. In the interviews, George explained that even if someone in the district does something that doesn't seem serious on a computer, they will still erase the entire device:

> If they (member of the district) installed a browser extension that looks a little crazy, we go ahead and we reimage, we don't take any chances on anything having a little bot (malicious software), like the one that blew the damn daylights out of this place when it first took off. (Technical Support Specialist George, interview, January 10, 2024)

George went on to say that these actions are from paranoia that an attack will happen again. In order to ensure that a cyber attack never happens again, George feels that the team needs to treat every potential security vulnerability with the most extreme remediation because there could be a "bot," or virus, hidden somewhere on the device.

Martin explained further that the team doesn't even trust when their endpoint protection determines that a potential security threat is remediated. While he believed that these extreme actions might not be necessary, he will err on the side of caution:

> Do we have to (erase the device), some would say no, you don't have to because it was mitigated, it was something defined by the endpoint protection software; however, we shouldn't, nobody, no IT entity should ever trust, entirely any product. At minimum, our product was able to give us a report telling us they found something and did something. Well, there's a percent chance that there's other things that happened to that machine at that same time that they didn't detect. (Technology Supervisor Martin, interview, January 31, 2024)

Martin questioned whether the team's actions were necessary since the endpoint protection says it has eliminated a threat; however, he felt that you can never "entirely trust any product," so the core IT team's actions are justified. Like George, Martin expressed fear that there was something potentially hidden on the device that could cause another attack that the endpoint protection did not detect.

Tom echoed George and Martin's perceptions that you can't trust that something malicious is not hiding on a device. Tom also felt that even though he perceived the current endpoint protection as a good tool for addressing cyber threats, he still doesn't believe the tool's assessment that something was resolved:

> We can't do enough to make sure that we don't miss any possible threat, we have an outstanding security product now, and they'll tell us that they detected something- low- medium- high priority…they'll even tell us that they remediated it, but we're not taking their word. (Device Manager, Tom, interview, January 18, 2024)

As with the rest of the team, Tom expressed a fear that the endpoint protection or the core IT team would miss a possible threat. Tom also expresses that even though he considers the tool "outstanding," he doesn't trust the endpoint protection's security assessment and he is "not taking their word" that something has been remediated.

James continued the core IT team's sentiments that there is always the possibility that a malicious threat is undetected and hiding on a device regardless of what any tool determines:

> And even if it says remediation actions… none, we still fall on the side of, let's reimage the device, because that's going to be the safest, even if they believe they got all the artifacts. We know we're gonna get all the artifacts if we reimage the device or wiping it. So again, we fall on the side of more secure. (Network Administrator James, interview, January 17, 2024)

James indicated that the only way to be completely secure is to erase the device to ensure that there is no longer something hidden. James also referenced that the team's actions are to increase the feelings of security. While James expressed a lack of trust in the endpoint protection, he also feels that it is the best product that FVSD could have implemented. In regard to the endpoint

protection, James said, “there might be, maybe… might be one other player that we potentially could choose from, but everybody else is like left in the dust.” So, even though James believes FVSD’s current security tools are the best tools available, there is still a lack of trust that they can keep the district secure from another cyber attack.

As a result of experiencing the cyber attack, the interviews showed the core IT team at FVSD adopted the mentality that they cannot fully trust any of the tools they have implemented to keep the district safe from future attacks. The team expressed a fear of having to live through another cyber attack, and that their actions can never be secure enough. Interviews show there is also a fear, that regardless of actions, there is still something malicious that can be hiding on a device. Andrew expressed in the interviews that a reason for the fear of something hiding is “cyber attacks evolve all the time…it will always be a race between how much more cunning and complex the attacks can be versus the cybersecurity that is meant to protect us keeping up with preventing those new attacks.” Since cyber threats are always evolving, Andrew described security as a race between threat actors and the tools that are intended to protect organizations. The core IT communicated during the interviews that given their experience, they do not trust that cybersecurity tools, regardless of how good they perceive them to be, are winning the race. As such, team members expressed that they never trust that something malicious isn’t hiding on a device and that anyone, or thing, will be able to find it.

Summary

This qualitative case study explored how core IT administrators in the FVSD experienced a cyber attack through two research questions that examined how the team members experienced the time during the attack, and how the cyber attack influenced current practices. Through inductive coding, I identified two themes related to each research question. From participant

responses, core IT administrators experienced that the cyber attack was unlike anything else they had been through. Since this was a new experience for everyone on the core IT team, team members recalled not having a comprehensive understanding of what was happening during the attack. In addition, team members recalled experiencing a wide range of emotions as they navigated the new experience. In addition to experiencing different emotions, team members expressed different perceptions of when they considered the cyber attack over, but most felt that the attack never ended mentally and it continues to influence their actions today.

After the attack, core IT team members referenced changes in their views related to cybersecurity practices in FVSD. Participant responses showed that team members felt they had "found a voice" and their expertise was valued and heard by not only other members of the core IT team but also other administrators and departments in the district. Furthermore, even though FVSD had implemented new security tools, interview responses indicated that the core IT team had developed a position of "trust nothing" regarding any tool that identified potential threats. With the fear of experiencing another attack, the team expressed they always erred on the side of implementing the most secure actions.

Chapter 5

Summary of the Study

This research explored the experiences of IT administrators after living through a large scale cyber attack on a K-12 public school. The study was conducted in one southeastern Pennsylvania school district and all of the participants were IT administrators who had worked in the district during a cyber attack. Using a case study research methodology, participants' experiences were examined through the use of two semi-structured interviews and the collection of artifacts related to the event. Researchers utilize a case study methodology when they want to study "a contemporary phenomenon (the 'case') in depth and within real world context, especially when the boundaries between the phenomenon and the context may not be clearly evident" (Yin, 2018, p. 15).

Cyber attacks on K-12 schools are increasing, and after the COVID-19 pandemic, public schools have implemented more digital technology which creates additional vulnerabilities for threat actors to exploit and initiate cyber attacks (Castelo, 2020). While there is an increase in attacks on K-12 schools, research on how IT administrators in any field, let alone K-12 schools, experience a cyber attack is limited. This study explored how K-12 administrators in one K-12 public school experienced a cyber attack and how it influenced their ongoing cybersecurity practices. K-12 administrators, teachers, and stakeholders can use this study to help understand how K-12 IT administrators experience an attack, which can help inform cybersecurity decisions to protect school districts and their stakeholders.

This study was guided by two research questions:

- How do K-12 IT administrators describe their experiences during a cyber-attack within their district?

- How do K-12 IT administrators see a cyber-attack as influencing current practices and policies?

Through inductive coding of participant responses from the semi-structured interviews, four themes emerged from the data. In addition, artifacts from the cyber attack provided a deeper understanding of participants' experiences and allowed for triangulation of the themes. Furthermore, the Technology Threat Avoidance Theory (TTAT) (Liang & Xue, 2009) was used to help guide and inform the research. TTAT outlines a decision-making process of how individuals assess cyber threats and implement a coping strategy. Overall, this research delves into themes reflecting the firsthand experiences of K-12 IT administrators, offering insights into how they encountered a cyber attack.

This chapter presents what insights other K-12 IT administrators and stakeholders can learn from this research. The first section is a discussion of the findings, followed by implications for practice. This is followed by a section that examines how the research relates to the Technology Threat Avoidance Theory. The final sections of the chapter include limitations, recommendations for future research, and a conclusion that summarizes the key findings of the research.

Discussion of Findings

Participant interviews in this study explored two research questions that examined how IT administrators experience a cyber attack, and how experiencing a cyber attack impacts IT administrators' cybersecurity related processes and policies. Through inductive coding, four themes emerged that address the research questions. The first theme that related to how IT administrators experience a cyber attack was "Nobody's Seen Something Like This Before" which examined how the cyber attack was an unparalleled experience for the FVSD core IT

team. Interviews demonstrated how the core IT team struggled to fully understand what was going on during this new experience, and also had a range of complex emotions as a result of going through the attack. The second theme to emerge from the data regarding the first research question was “The End” which explored how some core IT team members considered the attack over through tangible milestones during the recovery process, while others felt the attack never ended since there are still ongoing threats. Two themes emerged from the participant responses related to the second research question of how experiencing the attack impacted practices and policies, which were “Finding a Voice” and “Trust Nothing”. “Finding a Voice” examined how the core IT team felt the cyber attack positively changed their internal and external communication which has shaped their cybersecurity practices, while “Trust Nothing” explored the concept that the team does not feel they will ever be safe from potential cyber threats. Overall, participant responses and themes align with existing data related to cyber attacks.

As a result of the cyber attack, FVSD core IT administrators expressed that they struggled to fully know what was going on during the event. Research shows that cyber attacks are often underreported (Cashell et al., 2002; Furnell et al., 2015) and organizations lack models to truly conceptualize the damage caused by an attack (Agrafiotis et al., 2018). For organizations that have not experienced an attack, underreporting and a lack of comprehensive reports can lead to a lack of knowledge regarding cyber attacks. This can limit an organization’s ability to understand what is happening once they experience an attack. From the moment FVSD core IT team members found out about the attack, they expressed the need to research cyber attacks to gain a better understanding of what might be happening. In addition, a lack of prior knowledge and knowing what was occurring impacted the team’s ability to assess the damage related to the

attack. Throughout the attack, the core IT team struggled with knowing information related to the attack, and this impacted their ongoing remediation efforts.

Even though the core IT team members were closest to the attack in FVSD, a lack of understanding about what was occurring during the attack impacted their ability to communicate with each other and other stakeholders. Research shows that stakeholders should prepare for ambiguous communication during a cyber attack due to a threat of escalation from the threat actors and other complexities related to the attack (Richardson et al., 2020; van Zedlhoff, 2016; Watkins, 2014; Zhang et al. 2018). Participants shared that from the moment they found out about the attack, they didn't know how to talk about it with other team members, which impacted their internal communication. Furthermore, from the initial email to staff, to subsequent follow-up communications, team members shared that they were still trying to figure out what was going on and didn't have a full understanding of the situation while sending communications to other members of the district. In addition, participants shared that a lack of knowledge about whether the threat actors still had access to the FVSD network made it difficult to communicate. This aligns with Edwards et al. (2017) since the research indicated that organizations need to be aware of how communication can continue further escalation of the event if the threat actors are still involved. While current literature demonstrates that stakeholders outside of the IT department struggle with ambiguous communication during a cyber attack, this study demonstrates that those individuals closest to the attack also struggle with a comprehensive understanding of what is happening during a cyber event. A lack of understanding can impact the ability of those closest to the attack to communicate within their own team, as well as outside the team to other stakeholders.

Since it was difficult to communicate comprehensive information during the cyber attack, participants shared that they experienced a complex range of emotions. Literature shows that ambiguous communication related to cyber attacks can lead to individuals feeling "stressed, frustrated, anxious, scared and panicked" (Zhang et al., 2018, p.1066). In addition to ambiguous communication, research also indicates that a lack of information about the person or group committing the cyber attack can lead to individuals experiencing personal culpability for the attack (Bada & Nurse, 2019). Core IT team members shared that during the attack they felt paranoid, which was partially related to their potential culpability and their fear of being blamed for the attack. While research regarding the emotional reaction to cyber attacks focuses mainly on organizational stakeholders outside of core IT teams, this study showed how those closest to the attack can experience similar emotions. Core IT team members had also referenced in the interviews a fear of being blamed for the attack, which further aligned to research on the emotional reaction to cyber attacks.

In addition to the fear of being blamed for the attack, core IT team members also expressed a fear of having another attack. Minei and Matusitz (2011) identified in their research that when individuals experience a cyber attack, "in most cases the fear, the reaction, and the uncertainty is more damaging than the actual damage wrought by the cyber attack" (2011, p. 1007). Furthermore, research highlighted that the possibility of an attack can influence an individual's fear and anxiety as significantly as actually experiencing an attack (Gross et al., 2017). Core IT team members shared in their interviews there were elements of uncertainty surrounding the cyber attack since there was a lack of knowledge, and they also expressed a fear of personal culpability. This uncertainty and fear left a lasting impression on the team when they stated during the interviews that the cyber attack was "never really over." After going through

the attack, team members indicated that because of ongoing cyber threats, they now felt that the team needed to be constantly vigilant to protect the school district. So, due to an ongoing fear of another attack, the team felt that the cyber attack never ended, and this ultimately impacted their security practices.

After going through the cyber attack, the core IT team also reported that they do not trust that anything is safe. Research shows that while cybersecurity experts are confident in their ability to identify a malicious threat, they lack confidence in labeling a situation as harmless (Ben-Asher & Gonzalez, 2015). Throughout the interviews, core IT team members shared that while they believe they have the best tools available, they do not trust in their cybersecurity tools to fully identify every potential cyber threat to the school district. As such, team members remediate every potential threat at the most extreme level by erasing the device regardless of perceived severity. Team members indicated in the study that erasing the device is the only way to ensure anything malicious is destroyed. These actions relate to the research on response efficacy or a user's belief that their actions and tools are able to fully extricate a threat from a device (Jansen & van Schaik, 2017; Johnston & Warkentin, 2010). An individual's perception of response efficacy can positively impact whether the user will take steps to remediate the security threat. While core IT team members shared that they lack confidence in their ability to make sure that they have identified every possible threat, in order to address the fear of missing something malicious, they treat every potential threat with the only response they feel will fully rectify the situation.

Relation to Technology Threat Avoidance Theory

This study was informed by the Technology Threat Avoidance Theory (TTAT) (Liang & Xue, 2009) which outlines a process on how individuals make cybersecurity related decisions.

During the cybersecurity decision process, individuals initiate a threat appraisal, which includes the perceived susceptibility and the perceived severity of a potential cyber threat. At the same time, an individual will also consider the perceived avoidability of a threat through an analysis of the perceived effectiveness of the tools available to prevent a threat, the cost of implementing those tools, and a user's self-efficacy to prevent a threat. Concurrently influencing the decision-making process are the individual's risk tolerance and social influences. Based on the tenets of TTAT, a technology user will either implement a problem-focused solution where an individual initiates measures to minimize the threat or implements an emotion-focused solution where they fail to implement any measure to minimize the threat.

FVSD participant responses showed that after experiencing a cyber attack, core IT administrators perceived potential threats differently, which impacted their security decisions. Regarding susceptibility and severity, the two elements that informed perceived threat, the team indicated that they viewed that susceptibility was a certainty since they indicated a future attack was inevitable, and they perceived severity was at the highest level since they took the most extreme actions on every security threat. Independent of experiencing an attack, Young et al. (2016) found that the correlation between perceived susceptibility and perceived threat had already decreased since the original Liang and Xue studies. They attributed this decline in correlation to the fact that cyber attacks have become more common and that individuals now assume they will experience an attack. Team members stated in the interviews that it is "when, not if" in relation to whether another cyber attack will occur. This indicated that the core IT team felt that their susceptibility to another attack was assured, and this aligned with research that showed experiencing an attack increases perceived susceptibility (Mwagwabi, 2015). Mwagwabi found that even though perceived susceptibility does not have a strong impact directly on

security intentions and behaviors, there is a potential link between perceived threat and security behaviors after an attack. Participant reactions in this study, when compared to current research, call into question whether perceived susceptibility is a critical indicator of security decisions for IT administrators who have experienced a cyber attack and whether perceived threat is independent of perceived susceptibility.

Furthermore, Carpenter et al. (2019) found a negative interaction between perceived threat and safeguard effectiveness. The researchers speculated that if an individual perceived a threat as too severe or too likely, the individual would initiate an emotional coping mechanism over a problem-focused decision. Given that core IT team members expressed in the interviews that susceptibility was a certainty, and they perceived each threat was capable of recreating the original cyber attack, the core IT team's responses demonstrated that their perceived threat was at the highest level. Based on Carpenter's findings, the heightened sense of perceived threat should indicate that the team would initiate an emotional coping strategy rather than a problem-focused strategy; however, this was not the case since core IT team members reported they continue to actively remediate potential threats. While the team perceives there is the maximum threat of a cyber attack, and they do not completely trust any of their tools for safeguard effectiveness, they still continue to remain vigilant and implement problem-focused actions to address cyber threats.

Implications for Practice

The findings of this study bear significance to K-12 IT administrators, public school leaders, public school stakeholders, and the larger cybersecurity community. The implications of this study connect to the organizational structure of cybersecurity practices in K-12 institutions and include communication, remaining vigilant, and the mental health of K-12 IT administrators.

Furthermore, the findings in this study have implications for the application of the Technology Threat Avoidance Theory to K-12 IT administrators who have experienced a cyber attack.

Communication

Communication is a key element of preventing and navigating a cyber attack and participant responses referenced how communication impacted their experience of a cyber attack in the themes of "Nobody's See Something Like This Before" and "Finding a Voice." Based on the findings of this study, there are implications related to how organizations communicate during a cyber attack. In addition, there are implications for how strengthening organizational communication can foster a stronger cybersecurity environment after an attack, and finally, there are implications focusing on how sharing cyber attack experiences can promote better security practices for all K-12 institutions. All three types of communication can have an impact on the experiences and emotional responses of the individuals involved.

Providing Information During an Attack. During a cyber attack, it is important for IT administrators to communicate what is occurring in a transparent manner. Participant responses related to the theme of "Not Knowing Completely What's Going On" indicated that during an attack, they struggled to understand what was happening and this impacted their decision-making processes. A lack of knowledge led to the need for the core IT team to conduct more research, delay actions, alter team communication, and make decisions that were based on partial information. While participants shared that it was hard to accurately communicate in the midst of an attack, it is critical that core IT administrators relay as much information to each other during a cyber attack to promote effective remediation plans and minimize the negative impact on core IT team members. Findings showed that beyond a negative impact on remediation processes, a failure to effectively communicate can lead to complex emotions of paranoia and fear within the

department. To minimize delays related to a lack of information and minimize emotional reactions, in the event of a cyber attack, K-12 institutions should implement a plan to establish clear lines of communication between core IT team members. This should initially include daily updates for all team members as well as opportunities for team members to pose questions and concerns related to the attack. While there is a possibility that core IT team members will struggle to completely know what's going on and experience complex emotions during any cyber event, findings from this study demonstrated the importance of maintaining transparent communication to ensure effective decision making and minimize the emotional impact to technology staff in leadership positions.

Fostering Internal and External Departmental Communication. In addition to communication during an attack, public school districts need to foster technology related communication before and after an attack. Participant responses related to the theme of "Finding a Voice" demonstrated that improved communication within the team, and with other departments in the school district has helped to increase the cybersecurity posture of the district. Participants recalled that prior to the cyber attack, they were siloed and did not openly discuss cybersecurity within the team, or even seek out each other's expertise to inform internal projects. After the cyber attack, team members expressed the importance of working together and collectively solving problems and addressing security threats. While increased internal communication was a product of experiencing an attack, school leaders and IT teams can proactively create IT cultures where team members routinely collaborate to come up with comprehensive solutions to department projects. Promoting a culture of collaboration within the technology department prior to experiencing an attack can help school districts better prepare and address cyber threats.

While participant responses highlighted the benefits of internal communication, core IT members also expressed the importance of including the IT department in all department meetings within school districts. Given the prevalence of technology in all things education, including digital learning programs, student information, HVAC and lighting controls, security systems, and payroll, it is crucial to make sure that IT administrators are helping to inform technology implications related to any district initiative. K-12 administrators should consider the prevalence of technology in the different aspects of K-12 organizations and ensure that core IT members are present for district decisions that have technology components. Proactively including core IT team members, and giving them a voice at the table, can minimize the potential of creating cybersecurity vulnerabilities in the district and decrease the possibility of a cyber attack.

Sharing and Listening Outside the Organization. This study demonstrated how a lack of knowledge regarding cyber attacks impacted the core IT team's reactions to the attack. Through the theme of "Nobody's Seen Anything Like This Before," participants shared that not knowing what was going on shaped their reactions, communications, and decisions. Furthermore, research showed that cyber attacks are often underreported and there are a lack of models to effectively communicate the impact of attacks. This study showed the FVSD core IT team did not have the proper knowledge to effectively address a cyber threat since there was a lack of awareness regarding the impact of cyber attacks on K-12 institutions. To address the lack of knowledge that the core IT team reported in this study, K-12 institutions that have experienced a cyber attack need to share their experiences to increase the knowledge base for other K-12 organizations. Whether through conference presentations, technology related organizations, or other means, K-12 institutions that have experienced a cyber attack should have outlets to record

and share their cyber event so the experiences are available to other organizations. K-12 organizations that have experienced an attack can also work together to create a model that provides a more comprehensive understanding of how cyber attacks impact public school districts.

Furthermore, K-12 organizations that have not experienced an attack need to proactively seek out information regarding cyber attacks so they have a better understanding of the potential impacts on their institution. While it is probable that no two organizations will experience a cyber attack in the same way, increasing knowledge prior to an attack can potentially help to minimize feelings of not knowing what's going on and decrease the complex emotions that FVSD core IT administrators reported they experienced. In addition, sharing information between K-12 organizations could positively impact the threat and coping appraisals of core IT teams related to the TTAT increasing the likelihood that core IT teams will implement effective problem-focused strategies. Overall, there is the increasing reality that K-12 organizations have experienced, or will experience a cyber attack, and fostering open communication about the lived experiences of IT administrators will decrease the likelihood that IT teams will struggle with not completely knowing what's going on during a cyber event.

Mental Health of K-12 IT Administrators

Participant responses in this study showed that core IT team members experienced a theme of "Complex Emotions" as a result of the attack that ranged from paranoia to anger. FVSD core IT team members also expressed the fear they had of future attacks and that they trust that nothing is safe anymore. Existing research showed that experiencing a cyber attack can lead to individuals feeling "stressed, frustrated, anxious, scared and panicked" (Zhang et al., 2018, p.1066), and "in most cases the fear, the reaction, and the uncertainty is more damaging

than the actual damage wrought by the cyber attack" (Minei & Matusitz, 2011, p. 1007). Furthermore, studies on crime in general show that victims of crime can experience posttraumatic stress disorder (PTSD), increased levels of vulnerability and fear, and lower levels of self-efficacy (Kilpatrick et al., 1987; Lurigio, 1987). Given the experiences of the participants in this study and the implications that self-efficacy can have on cybersecurity decisions in the TTAT, it is important that K-12 school districts consider the mental health of K-12 IT administrators after an attack.

After crises such as school shootings, schools provide counselors to help staff and students navigate the emotional impact of the event (Brown, 2020); however, participants in this study did not indicate that any mental health services were provided to help them cope with the complex emotions and ongoing impact the event had on them. This study highlighted the complex emotions that experiencing a cyber attack can have on the long-term mental health of an IT administrator, and K-12 institutions should acknowledge that cyber attacks can profoundly impact the emotional reactions of their IT administrative staff. As a result of the emotional impact, K-12 institutions should provide supports to ensure that the negative emotions are minimized. While the main focus of providing mental health supports is the emotional well-being of the IT administrators, improving the team's self-efficacy can also positively impact future cybersecurity decisions and decrease the possibility of a future attack.

Remaining Vigilant

Related to the theme of "Trust Nothing," participants in this study shared that they do not trust that any tool will keep the school district completely safe, and they need to remain vigilant against potential cybersecurity threats. After the cyber attack, the findings showed that the team is constantly addressing potential threats, regardless of the perceived severity, to ensure that

nothing is able to attack the district again. Also, while the core IT team shared they had security practices in place prior to the event, experiencing a cyber attack led to an increase in the security tools they use, and currently they feel they have the best tools on the market.

Experiencing an attack was the catalyst for the FVSD core IT team to implement robust tools and processes to keep the district safe; however, school districts that have not experienced an attack should analyze their current practices and tools to assess whether they are suitable for the current cybersecurity landscape. Participant responses demonstrated that the core IT team does not take chances regarding cyber threats and has adopted practices that will minimize the likelihood of experiencing another attack. If districts that have not experienced an attack analyze and update their tools and processes, it can decrease the chances they will experience a cyber attack in the future.

Technology Threat Avoidance Theory

This study poses implications regarding the application of the TTAT to K-12 IT administrators who have experienced a cyber attack. Participant responses in this study directly addressed the components of the threat appraisal of TTAT, as well as the perceived effectiveness of their tools and processes related to the coping appraisal. However, responses did not relay the perceived cost of their tools, or an individual's self-efficacy that they would be able to prevent an attack. While self-efficacy was not openly mentioned in the interviews, members universally mentioned the concept of relying on the team for input related to cybersecurity related decisions. Since core IT team members found that finding a voice, and increasing communication within the team had a positive impact on the group's security decisions, it could indicate that in addition to self-efficacy, including an individual's perception of the group's collective efficacy in TTAT could offer a better understanding of how K-12 core IT team members make security related

decisions. Collective efficacy, or a group's belief they are able to achieve a particular action (Bandura, 1986; Gibson et al., Gibson et al., 2000; Shamir, 1990), is evident in participants' responses since they emphasize the importance of working as a collective unit. Including collective efficacy in the coping appraisal for K-12 IT administrators who experienced a cyber attack could offer greater insight into why team members make their security decisions.

Limitations

When assessing research studies, it is necessary to address the potential limitations of the findings. It is first important to consider that I am currently an administrator in FVSD. While all of the participants in the study are also administrators in FVSD, and none of the administrators directly report to me, the collegial relationship between myself and the participants may have influenced what was shared during the interviews. Furthermore, since the cyber attack occurred four years prior to the study, the lapse of time may have impacted the participants' ability to recall specific facts regarding the event. Since the purpose of this study was to examine how IT administrators personally experience a cyber attack, and not the specific details of the attack, the interviews captured the authentic reactions of the administrators as situated at the time of the research. Regardless, given the time between the actual attack and the interview, specific details about the attack referenced in the participants' responses may have been impacted by the gap of time between experiencing the attack and the interviews.

In addition to the working relationships and lapse of time, I also had firsthand experience with the cyber attack. This experience could potentially influence the findings of the study. Additionally, given the qualitative case study methodology of this study, the findings lack generalization to other contexts; however, the findings can still offer insights for other K-12 organizations on how IT administrators experience cyber attacks. While there are limitations to

the study, I made every effort to minimize the impact of the potential limitations to accurately examine the experiences of IT administrators after a cyber attack.

Recommendations for Further Research

This qualitative case study explored how K-12 IT administrators experience a cyber attack and how it impacts their cybersecurity practices. This study adds to the limited amount of research that currently exists regarding cyber attacks in K-12 institutions. With the increase in potential cyber vulnerabilities related to the expanded adoption of technology after the COVID-19 pandemic and the escalation of cyber attacks on K-12 organizations that existed before the pandemic, additional research is needed regarding cyber attacks on public education.

While this study captured the experiences of one core IT team of administrators, cyber attacks are constantly evolving and can potentially impact K-12 school districts in different ways. Expanding this study to include IT administrators from other school districts who have experienced a cyber attack could help provide a more comprehensive understanding of how IT administrators experience attacks and how the evolution of attacks and remediation practices impacts administrators' experiences. With a more comprehensive understanding of how IT administrators experience an attack, K-12 organizations can better prepare themselves to prevent and address cyber threats and also support IT administrators during an attack.

Since this study occurred after a cyber attack, it is important for research to look at cybersecurity from a proactive position as compared to a reactive position. In the findings, the core IT administrative team referenced that there was a change in the culture surrounding technology culture as a result of the attack. Future research could examine the current cybersecurity cultures in K-12 institutions that have not experienced a cyber attack and the culture's impact on the practices in the districts. By gaining a better understanding of what works

to prevent attacks and how organizations approach cybersecurity, future research can help minimize future attack susceptibility for K-12 districts.

Furthermore, while this study focuses on the lived experiences of IT administrators, there are a number of stakeholders in K-12 institutions that are potentially impacted by a cyber attack. Further qualitative studies could examine how non-IT administrators, teachers, students, and parents experience a cyber attack. Each stakeholder group potentially has a different level of knowledge on how a cyber attack is progressing and could have different reactions and impacts. Understanding how different groups with a K-12 district experience an attack could allow schools to implement proactive, and reactive, plans to address cybersecurity, and also maintain that all stakeholders are supported during a cyber event.

In addition to the lived experiences of IT administrators and other K-12 stakeholders during an attack, this study indicates that further research on how the Technology Threat Avoidance Theory applies to K-12 IT administrators who have experienced a cyber attack. Findings indicate that for K-12 IT administrators who experienced an attack, there is a potential decrease in the relationship between perceived susceptibility, perceived severity, and perceived threat. Additional research to test the interactions between the components of perceived threat could indicate the need for revisions to TTAT related to K-12 IT administrative teams. In addition, since this study highlighted the importance of working as a team to address cyber threats, additional research could test the impact of collective efficacy (Bandura, 1986; Gibson et al., Gibson et al., 2000; Shamir, 1990) in addition to an individual's self-efficacy. This research could inform important elements of how core IT teams in K-12 organizations could function to better meet the cybersecurity needs of a school district.

Conclusion

This qualitative case study examined how IT administrators in one PA school district experienced a cyber attack and how it influenced their cybersecurity practices. Given the limited research on the impact of cyber attacks on individuals within an organization, a qualitative case study methodology provided an opportunity to explore a single event through the lived experience of organizational members closest to the event. Through an analysis of participant interviews and artifact collection, several themes emerged. Participants described the difficulties of navigating a cyber attack, as well as the lasting impact the event had on their cybersecurity practices and processes. While this case study may not be generalizable to other systems and settings, there are still important implications from this study for K-12 school district leaders who have experienced a cyber attack, and those who have not experienced an attack. From the findings of this research, it is important that K-12 institutions promote more effective communication between core IT administrators within the school district, and between the core IT administrators and other departments within the organization to help improve cybersecurity processes. In addition, to increase the knowledge of core IT teams, K-12 organizations that have experienced a cyber attack need to share their experiences so IT administrators are better prepared to face the challenges of addressing a cyber threat. Finally, this study has implications in the application of the Technology Threat avoidance Theory to K-12 IT administrators who have experienced an attack, specifically in the areas of the threat appraisal, and the interaction of self/group efficacy.

As the dependence on technology grows in K-12 institutions, from student devices to digital systems that manage the infrastructure of districts, maintaining effective cybersecurity practices is an essential component. The likelihood that a school district will experience a cyber

attack is increasing, and school leaders need to be intentional in their preparation and planning to minimize the impact on their stakeholders. Knowledge and communication surrounding cyber attacks and their impact on IT administrators, those closest to the prevention and remediation of attacks, is paramount to ensure K-12 school districts remain safe. This study provides strategies for K-12 leaders to enhance robust cybersecurity practices by providing support to IT administrators. By doing so, they can effectively safeguard districts and protect stakeholders from potential cyber threats.

References

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber harms: Defining the impacts of cyber attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy006

Ahern, K. J. (1999). Ten tips for reflexive bracketing. *Qualitative health research*, *9*(3), 407-411.

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. Computers & Security, 68, 160-196.

Alqahtani, H., & Kavakli-Thorne, M. (2020). Does decision-making style predict individuals' cybersecurity avoidance behaviour?. In HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22 (pp. 32-50). Springer International Publishing.

Andrews, E. (2018, December 18). *Who Invented the Internet?* https://www.history.com/. Retrieved January 19, 2023, from https://www.history.com/news/who-invented-the-internet

Bada, M., & Nurse, J. R. C. (2019). The social and psychological impact of cyber attacks. In V. Benson & J. Mcalaney (Eds.), *Emerging cyber threats and cognitive vulnerabilities* (1st ed., pp. 73–92). Academic Press.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cybersecurity awareness campaigns: Why do they fail to change behaviour?. arXiv preprint arXiv:1901.02672.

Ballard, B. (2021, February 15). *Cybercrime apparently cost the world over $1 trillion in 2020*. TechRadar. Retrieved January 22, 2023, from https://www.techradar.com/news/cybercrime-cost-the-world-over-dollar1-trillion-in-2020

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review*, *84*(2), 191.

Bandura, A. (1986). *The social foundations of thought and action.* Englewood Cliffs, NJ: Prentice Hall.

Bandura, A. (1994). Self-efficacy. In V. S. Ramachaudran (Ed.), *Encyclopedia of human behavior* (Vol. 4, pp. 71-81). New York: Academic Press. (Reprinted in H. Friedman [Ed.], *Encyclopedia of mental health*. San Diego: Academic Press, 1998).

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cybersecurity knowledge on attack detection. *Computers in Human Behavior*, 48, 51-61.

Bentley, J. M., Oostman, K. R., & Shah, S. F. A. (2017). We're sorry but it's not our fault: Organizational apologies in ambiguous crisis situations. *Journal of Contingencies and Crisis Management*, *26*(1), 138–149. https://doi.org/10.1111/1468-5973.12169

Brown, C. H. (2020). School counselors' response to school shootings: Framework of recommendations. *Journal of Educational Research and Practice*, *10*(1), 18.

Bryant, M. (2016, March 3). *20 years ago today, the World Wide Web opened to the public*. TNW | Insider. Retrieved February 8, 2023, from https://thenextweb.com/news/20-years-ago-today-the-world-wide-web-opened-to-the-public

Bushweller, K. (2022). What the massive shift to 1-to-1 computing means for schools, in charts. *Education Week*. https://www.edweek.org/technology/what-the-massive-shift-to-1-to-1-computing-means-for-schools-in-charts/2022/05

Butin, D. W. (2010). *The education dissertation: A guide for practitioner scholars*. Corwin.

Carver, C. S. (2006). Approach, avoidance, and the self-regulation of affect and action. *Motivation and emotion*, *30*, 105-110.

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, 44.

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber attacks. Congressional research service documents, CRS RL32331 (Washington DC), 2.

Castelo, M. (2020, October 2). *Cyber attacks Increasingly Threaten Schools — Here's What to Know*. Technology Solutions That Drive Education. Retrieved February 8, 2023, from https://edtechmagazine.com/k12/article/2020/06/cyber attacks-increasingly-threaten-schools-heres-what-know-perfcon

Chan, Z. C., Fung, Y. L., & Chien, W. T. (2013). Bracketing in phenomenology: Only undertaken in the data collection and analysis process. *The qualitative report*, *18*(30), 1-9.

Chen, H. S., & Jai, T. M. C. (2019). Cyber alarm: Determining the impacts of hotel's data breach messages. *International Journal of Hospitality Management*, *82*, 326–334. https://doi.org/10.1016/j.ijhm.2018.10.002

Chen, Y., & Zahedi, F. M. (2016). Individuals' Internet Security Perceptions and Behaviors. *Mis Quarterly*, 40(1), 205-222.

Cheng, C., Chan, L., & Chau, C. L. (2020). Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. Computers in Human Behavior, 108, 106311.

Chenoweth, T., Minch, R., & Gattiker, T. (2009, January). Application of protection motivation theory to adoption of protective technologies. In *2009 42nd Hawaii International Conference on System Sciences* (pp. 1-10). IEEE.

Climer, S. (2019, March 21). *History of cyber attacks from the morris worm to exactis*. Retrieved February 8, 2023, from https://gomindsight.com/insights/blog/history-of-cyber attacks-2018/

Colbaugh, R., & Glass, K. (2011, July). Proactive defense for evolving cyber threats. In *Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics* (pp. 125-130). IEEE.

Commonwealth of Pennsylvania. (2022). Future Ready PA Index. Retrieved September 1, 2023, from https://futurereadypa.org/

Confente, I., Siciliano, G. G., Gaudenzi, B., & Eickhoff, M. (2019). Effects of data breaches from user-generated content: A corporate reputation analysis. *European Management Journal*, *37*(4), 492–504. https://doi.org/10.1016/j.emj.2019.01.007

Coombs, W. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review,* 10, 163-176.

Creswell, J. W., & Creswell, D. J. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). SAGE Publications, Inc.

Creswell, J. W. (2016). *30 essential skills for the qualitative researcher*. Sage Publications.

Crowdstrike. (2023). 2023 Global Threat Report. Retrieved September 26, 2023, from https://go.crowdstrike.com/2023-global-threat-report.html

Cuban, L. (1993). Computers meet classroom: Classroom wins. *Teachers college record*, *95*(2), 185-210.

Cybersecurity and Infrastructure Security Agency. (2021a, February 1). *What is Cybersecurity?* Cybersecurity and Infrastructure Security Agency CISA. Retrieved July 5, 2023, from https://www.cisa.gov/news-events/news/what-cybersecurity

Cybersecurity and Infrastructure Security Agency. (2021b, October 25). *UK and US Security Agencies Issue COVID-19 Cyber Threat Update | CISA*. Cybersecurity and Infrastructure Security Agency CISA. Retrieved June 30, 2023, from https://www.cisa.gov/news-events/news/uk-and-us-security-agencies-issue-covid-19-cyber threat-update

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. International journal of engineering sciences & Emerging technologies, 6(2), 142-153.

Edwards, B., Furnas, A., Forrest, S., & Axelrod, R. (2017). Strategic aspects of cyber attack, attribution, and blame. *Proceedings of the National Academy of Sciences*, *114*(11), 2825–2830. https://doi.org/10.1073/pnas.1700442114

Egelman, S., & Peer, E. (2015, April). Scaling the security wall: Developing a security behavior intentions scale (sebis). In Proceedings of the 33rd annual ACM conference on human factors in computing systems (pp. 2873-2882).

Federal Bureau of Investigation. (2022a). Internet Crime Report. In *https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf*.

Federal Bureau of Investigation. (2022b, April 29). *Ransomware*. Retrieved July 5, 2023, from https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware

Federal Trade Commission. (2022, February 9). How To Recognize, Remove, and Avoid Malware. Retrieved September 26, 2023, from https://consumer.ftc.gov/articles/how-recognize-remove-avoid-malware

Fossey, E., Harvey, C., McDermott, F., & Davidson, L. (2002). Understanding and evaluating qualitative research. *Australian & New Zealand journal of psychiatry*, *36*(6), 717-732.

Furnell, S., Emm, D., & Papadaki, M. (2015). The challenge of measuring cyber-dependent crimes. Computer Fraud & Security, 2015(10), 5-12.

Gibson, C. B., Randel, A. E., & Earley, P. C. (2000). Understanding group efficacy: An empirical test of multiple assessment methods. *Group & organization management*, *25*(1), 67-97.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cybersecurity behavior intentions. *Computers & Security*, 73, 345-358.

Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity*. Published. https://doi.org/10.1093/cybsec/tyw018

Gudmundsdottir, G. B., & Hathaway, D. M. (2020). 'We always make it work': Teachers' agency in the time of crisis. *Journal of Technology and Teacher Education, 28*(2), 239–250.

Halevi, T., Memon, N.D., Levis, J.A., Kumaraguru, P., Arora, S., Dagar, N., Aloul, F.A., & Chen, J. (2017). Cultural and psychological factors in cybersecurity. *Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services*.

Hanson, R. F., Sawyer, G. K., Begle, A. M., & Hubel, G. S. (2010). The impact of crime victimization on quality of life. *Journal of Traumatic Stress: Official Publication of The International Society for Traumatic Stress Studies*, *23*(2), 189-197.

Hiscox. (2022). *Cyber Readiness Report 2022*. Hiscox. https://www.hiscox.co.uk/sites/default/files/documents/2022-08/Hiscox-UK-Cyber-Readiness-Report-2022.pdf

Hoblit, G. (Director). (1998). *Fallen* [Film]. Turner Pictures, and Atlas Entertainment.

Home Office of the United Kingdom (2015). *The serious and organised crime strategy: annual report for 2014*. London: HMSO.

IBM. (n.d.-a). *The Fundamentals of Networking | IBM*. https://www.ibm.com/topics/networking. Retrieved June 25, 2023, from https://www.ibm.com/topics/networking

IBM. (n.d.-b). *What is a threat actor?* Retrieved July 5, 2023, from https://www.ibm.com/topics/threat actor

Jansen, J., & Van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information & Computer Security*, *25*(2), 165-180.

JavaTpoint. (2021). *Types of Computer Network*. www.javatpoint.com. Retrieved July 5, 2023, from https://www.javatpoint.com/types-of-computer-network

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS quarterly*, 549-566.

Kilpatrick, D. G., Saunders, B. E., Veronen, L. J., Best, C. L., & Von, J. M. (1987). Criminal victimization: Lifetime prevalence, reporting to police, and psychological impact. *Crime & delinquency*, *33*(4), 479-489.

Kizza, J. M., Kizza, W., & Wheeler. (2013). Guide to computer network security (Vol. 8). Berlin: Springer.

Kostyuk, N., & Wayne, C. (2019). *Communicating cybersecurity: Citizen risk perception of cyber threats*. Retrieved March 12, 2023, from http://www-personal.umich.edu/~nadiya/communicatingcybersecurity.pdf

Kovačević, A., Putnik, N., & Tošković, O. (2020). Factors related to cybersecurity behavior. IEEE Access, 8, 125140-125148.

Kuipers, S. L. & Schonheit, M. (2021). Data breach and effective crisis communication: a comparative analysis of corporate reputational crises, Corporate Reputation Review, 1-22. doi: 10.1057/s41299-021-00121-9

Lewis, J. A. (2002). Assessing the risks of cyber terrorism, cyber war and other cyber threats (p. 12). Washington, DC: Center for Strategic & International Studies.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS quarterly*, *33*(1) 71-90.

Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 1.

Lurigio, A. J. (1987). Are all victims alike? The adverse, generalized, and differential impact of crime. *Crime & Delinquency*, *33*(4), 452-467.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, *19*(5), 469-479.

Malby, S., Mace Robyn M., Anika, H., Cameron, B., Stefan, K., & Eva, I. (2013). Comprehensive Study on Cybercrime. *United Nations Office on Drugs and Crime,* 1–320. https://doi.org/10.1103/Phys RevLett.105.018904

Manalu, E. P., Muditomo, A., Adriana, D., & Trisnowati, Y. (2020, August). Role of information technology for successful responses to covid-19 pandemic. In 2020 International Conference on Information Management and Technology (ICIMTech) (pp. 415-420). IEEE.

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cybersecurity. *Journal of Internet Commerce*, 9(1), 23-41.

McMahon, C. (2020). In defence of the human factor. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.01390

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation* (4th ed.). Jossey-Bass.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia - Social and Behavioral Sciences*, *147*, 424–428. https://doi.org/10.1016/j.sbspro.2014.07.133

Microsoft. (2023). *What Is an Endpoint?.* Retrieved July 5, 2023, from https://www.microsoft.com/en-us/security/business/security-101/what-is-an-endpoint#:~:text=Endpoints%20are%20physical%20devices%20that%20connect%20to%20and%20exchange%20information,%2C%20embedded%20devices%2C%20and%20servers.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of applied social psychology*, *30*(1), 106-143.

Minei, E., & Matusitz, J. (2011). Cyberterrorist messages and their effects on targets: A qualitative analysis. *Journal of Human Behavior in the Social Environment*, 21(8), 995-1019.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International journal of advanced research in computer science*, *8*(5), 1938-1940.

Mueller, R. S. (2012, March 1). *Combating threats in the Cyber World: Outsmarting terrorists, hackers, and Spies*. FBI. Retrieved January 19, 2023, from https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

Mwagwabi, F. M. (2015). A Protection Motivation Theory approach to improving compliance with password guidelines (Doctoral dissertation, Murdoch University).

National Institute of Standards and Technology. (n.d.-a). *Cyber attack - Glossary | CSRC*.. Retrieved January 21, 2023, from https://csrc.nist.gov/glossary/term/cyber_attack

National Institute of Standards and Technology. (n.d.-b). *Malware- Glossary*. COMPUTER SECURITY RESOURCE CENTER. Retrieved July 5, 2023, from https://csrc.nist.gov/glossary/term/malware

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. *Proceedings - 2011 1st Workshop on Socio-Technical Aspects in Security and Trust, STAST 2011*, 60–68. doi:10.1109/STAST.2011.6059257

Pennsylvania Department of Education. (2022). *Glossary of child accounting terms*. Retrieved July 5, 2023 from https://www.education.pa.gov/Teachers%20-%20Administrators/Child%20Accounting/Pages/Glossary-of-Terms.aspx

Pratt, M. K. (2021, January 13). *Cyber attack.* SearchSecurity. Retrieved November 9, 2021, from https://www.techtarget.com/searchsecurity/definition/cyber attack

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/10.1177/0018720815585906

Purplesec. (2020). *2020 cybersecurity statistics: The ultimate list of stats, data & trends.* Purplesec. https://purplesec.us/resources/cybersecurity-statistics/#:~:text=The%20total%20number%20of%20breaches,per%20lost%20record%

Whitney, L. (2020, September 15). *Cyber attacks against schools are on the rise.* TechRepublic. https://www.techrepublic.com/article/cyber attacks-against-schools-are-on-the-rise/

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for cybersecurity in schools: The human factor. *Educational Planning., 27*(2), 23–39.

Ring, J. (2023, April 30). *30 years ago, one decision altered the course of our connected world*. NPR. Retrieved June 24, 2023, from https://www.npr.org/2023/04/30/1172276538/world-wide-web-internet-anniversary#:~:text=Fresh%20Air-,The%20World%20Wide%20Web%20became%20available%20to%20the%20broader%20public,with%20graphics%2C%20audio%20and%20hyperlinks.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, 91(1), 93-114.

Roscini, M. (2014). *Cyber operations and the use of force in international law*. Oxford University Press, USA.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future internet, 11(4), 89.

Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabaee, S., Choo, K. K. R., & Al-Qirim, N. (2022). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digital Communications and Networks*.

Scheier (2012). *On Cyberwarfare.* DCAF Horizon Working Paper 7. https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf

Shamir, B. (1990). Calculations, values, and identities: The sources of collectivistic work motivation. *Human Relations, 43*, 313-332.

Stacey, P., Taylor, R., Olowosule, O., & Spanaki, K. (2021). Emotional reactions and coping responses of employees to a cyber attack: A case study. *International Journal of Information Management*, 58, 102298.

Topper, A., & Lancaster, S. (2013). Common challenges and experiences of school districts that are implementing one-to-one computing initiatives. *Computers in the Schools*, *30*(4), 346-358.

Triplett, W. J. (2022). *Addressing Cybersecurity Leadership Challenges in Organizations* (Doctoral dissertation, Capitol Technology University).

Tufford, L., & Newman, P. (2012). Bracketing in qualitative research. *Qualitative social work*, *11*(1), 80-96.

United Nations. (2020). Policy brief: Education during COVID-19 and beyond. United Nations. https://www.un.org/development/desa/dspd/wp-

content/uploads/sites/22/2020/08/sg_policy_brief_covid-19_and_education_august_2020.pdf

U.S. Department of Education. (2017). Building Technology Infrastructure for Learning. In *https://tech.ed.gov*. Office of Educational Technology. Retrieved June 24, 2023, from https://tech.ed.gov/files/2017/07/2017-Infrastructure-Guide.pdf

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems*, 15(10), 2. 679-722.

van Zadelhoff, M. (2018, February 6). *The Biggest Cybersecurity Threats Are Inside Your Company*. Harvard Business Review. Retrieved March 15, 2023, from https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company

Wang, L., & Alexander, C. A. (2021). Cybersecurity during the COVID-19 pandemic. AIMS Electronics and Electrical Engineering, 5(2), 146-157.

Wang, P., & Park, S. (2017). Communication in cybersecurity: A public communication model for business data breach incident handling. *Issues In Information Systems*, *18*(2), 136–147. https://doi.org/10.48009/2_iis_2017_136-147

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. IEEE transactions on professional communication, 55(4), 345-362.

Watkins, B. (2014). The impact of cyber attacks on the private sector. Briefing Paper, Association for International Affair, 12, 1-11.

Wiener, N. (2019). *Cybernetics or Control and Communication in the Animal and the Machine*. MIT press.

Woon, I., Tan, G.-W., and Low, R. 2005. "A Protection Motivation Theory Approach to Home Wireless Security," AIS, International Conference on Information Systems (ICIS 2005), Las Vegas, NV, December 11-14.

Yin, R. K. (2018). Case Study Research and Applications: Design and Methods (6th ed.). Thousand Oaks, CA: Sage.

Young, D. K., Carpenter, D., & McLeod, A. (2016). Malware avoidance motivations and behaviors: A technology threat avoidance replication. *AIS Transactions on Replication Research*, 2(1), 8.

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems*, 16(6), 2.

Zhang-Kennedy, L., Assal, H., Rocheleau, J., Mohamed, R., Baig, K., and Chiasson, S. (2018). *The aftermath of a crypto-ransomware attack at a large academic institution.* Proceedings of the 27th USENIX Conference on Security Symposium, SEC'18, pages 1061–1078, Berkeley, CA, USA. USENIX Association.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cybersecurity awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1), 82-97.

Appendix A

IT Administrative Staff Protocol Interview #1

Researcher statement: I want to thank you for volunteering your time to participate in this research today. This is the first of two interviews, and the purpose of this study is to gain a better understanding of how K-12 IT administrators experience a cyber attack and how it impacts their views on cybersecurity. During this interview, I am assuming the role of a researcher and not an employee of the XXXXXX school district who experienced a cyber attack myself.

This study is not intended to be critical or evaluative; nor is it intended to share specific infrastructure cybersecurity measures that are currently in place. I am looking to better understand your experiences and feelings within the context of a cyber attack. Please share as much as you are comfortable while protecting your role as a leader and the cybersecurity practices of the district. I know the cyber attack happened several years ago, but providing any specific details you remember will provide context to the experience. If you experience any negative feelings as a result of this interview, there is free counseling available through the XXXX employee assistance program, and contact information will be shared at the conclusion of the interview.

All interviews will be coded with pseudonyms to protect identities. Both interviews will follow a semi-structured format, which means I have a set of pre-determined questions; however, there is flexibility to explore new topics or conversations as they come up. I will be recording this interview for review and will also be taking notes to document our conversation. Do you have any questions or concerns before we begin?

1. Please tell me about your career history including education, previous positions, and how you came to work in K-12 technology?

2. At the time of the cyber attack, what was your role in the district?
3. Please tell me about how you learned of the cyber attack in 2019? Where were you?
4. Please think back to that day. Describe your initial reaction. How did you feel?
5. What were your initial concerns when you learned of the cyber attack? What was your first action? If needed: Who did you contact?
6. How did you (and/or your team) address the immediate challenges and disruptions you faced in the aftermath of the cyber attack?
7. Describe what your role was during the initial days of the cyber attack. Did it change over time?
8. How did communication within the technology department and outside your department regarding the cyber attack impact the time after the attack?
9. How did you manage the work-life balance during the cyber attack?
10. What was the hardest part of experiencing the cyber attack?
11. When did you consider the cyber attack over? Please describe what happened once your team determined the cyber attack was over.
12. How has the cyber attack influenced your relationships with others on the IT admin team?
    a. Other administrators?
    b. Other stakeholders in the district?

Appendix B

IT Administrative Staff Protocol Interview #2

Researcher statement: I want to thank you again for volunteering your time to participate in this research today. This is the second of two interviews, and as with the first interview, the purpose of this study is to gain a better understanding of how K-12 IT administrators experience a cyber attack and how it impacts their views on cybersecurity. During this interview, I am assuming the role of a researcher and not an employee of the XXXXXX school district who experienced a cyber attack myself.

I would like to remind you that this study is not intended to be critical or evaluative; nor is it intended to share specific infrastructure cybersecurity measures that are currently in place. I am looking to better understand your experiences and feelings within the context of a cyber attack. Please share as much as you are comfortable while protecting your role as a leader and the cybersecurity practices of the district. I know the cyber attack happened several years ago, but providing any specific details you remember will provide context to the experience. If you experience any negative feelings as a result of this interview, there is free counseling available through the XXXX employee assistance program, and contact information will be shared at the conclusion of the interview.

All interviews will be coded with pseudonyms to protect identities. As with the first interview, this interview will follow a semi-structured format, which means I have a set of pre-determined questions; however, there is flexibility to explore new topics or conversations as they come up. I will be recording this interview for review and will also be taking notes to document our conversation. Do you have any questions or concerns before we begin?

1. What were your feelings about the network security of the school district prior to the cyber attack? In what ways did those feelings change (or not change) after the cyber attack?
2. What was the biggest impact to the school district as a result of the cyber attack?
3. How did the cyber attack impact the IT team's security practices? How has the cyber attack impacted your role in cybersecurity?
4. What lessons have you learned from this experience? What lessons do you think the district learned from the cyber attack?
5. What advice or recommendations would you offer to other K-12 IT administrators based on your experiences with this cyber attack?
    a. What is the most important action you do now to prevent another attack?
    b. What is the most important action that others can do to prevent another attack?
6. How do you assess potential cyber threats after the attack?
7. What was something positive that came out of the cyber attack?
8. Is there anything else that you think is important to share regarding the cyber attack?