9-24-2025

Cyberloafing and the Effects on Information Technology Infrastructure

Robert Ceneskie
Walden University

<u>Walden University</u>

College of Management and Human Potential

This is to certify that the doctoral study by

Robert J. Ceneskie

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Constance Blanson, Committee Chairperson, Information Technology Faculty
Dr. Jon McKeeby, Committee Member, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2025

Abstract

Cyberloafing and the Effects on Information Technology Infrastructure

by

Robert J. Ceneskie

MS, Walden University, 2020

BS, Walden University, 2017

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

September 2025

Abstract

Cyberloafing, or the use of business resources for nonwork-related internet activity, can negatively affect technology infrastructure and organizational productivity. In K–12 public school districts, IT administrators and school leaders are directly affected, as network degradation and ransomware attacks can disrupt instruction, compromise sensitive data, and reduce access to critical resources. This quantitative correlational, ex post facto study, grounded in activity theory and the theory of human-technology interaction, was to determine whether there was a statistically significant relationship between employee cyberloafing, network degradation, and ransomware security attacks in the education sector. Data were collected through public records requests for bandwidth usage, web traffic, and firewall alerts from next generation firewalls. The sample consisted of K-12 public school districts in one southeastern U.S. state, representing 67 districts and more than 4,2000 schools. Pearson correlation analysis indicated strong positive relationships between cyberloafing and network degradation ($r = .69$, $p < .001$) and ransomware activity ($r = .72$, $p < .001$), both representing large effect sizes under Cohen's guidelines. Findings suggest that monitoring and managing cyberloafing can mitigate cybersecurity risks and performance issues in educational IT environments. A key recommendation is for district IT leaders to implement proactive policy enforcement and employee awareness training. The implications for positive social change include the potential for school IT leaders to implement policies that enhance network security, benefiting students and staff by ensuring safer and more reliable educational technology environments.

Cyberloafing and the Effects on Information Technology Infrastructure

by

Robert J. Ceneskie

MS, Walden University, 2020

BS, Walden University, 2017

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

September 2025

Dedication

This dissertation is dedicated to my father, Wayne Ceneskie. From an early age, my father has been my greatest teacher, role model, and supporter. Growing up, faced many challenges together—mentally and physically—but through it all, he remained a steady source of strength, wisdom, and love. Some of my earliest memories are of watching him work in the garage or around the house, always letting me observe and learn. vividly remember the excitement of setting up my first IBM PS/2 Model 50 in the dining room—an incredible technological leap forward. Curious, moved the system files into a folder to make things “organized,” unknowingly causing the system to fail on reboot. That moment, while humbling, was my first real lesson in computers—and my father never scolded me. Instead, explored, learned, and repaired together. From then on, weekends were spent at yard sales and swap meets, finding old computer parts to build or upgrade machines. It was during those moments that my passion for technology was born. My father encouraged me to pursue what loved as grew older. His belief in me led to a degree in computer information systems, a career in technology, and this dissertation. Through every setback and success, he has offered a listening ear, honest advice, and encouragement precisely when needed it. Without his unwavering support, may have lost sight of my goals. Instead, pressed forward, determined to become the first in my family to earn a doctorate and show of what am truly capable. Thank you, Dad. could not have done this without you.

Acknowledgments

This dissertation represents the culmination of years of academic study and the support, encouragement, and sacrifices of many people along the way. I am deeply grateful to everyone who played a role in helping me reach this milestone. First, I would like to express my sincere appreciation to my committee chair and members. Your guidance, constructive feedback, and unwavering support have been instrumental in shaping this work's direction and quality. Thank you for your time, expertise, and encouragement throughout this process. To my professors and mentors throughout my academic journey, thank you for challenging me to think critically and cultivating a more profound passion for learning and discovery in information technology. To my colleagues and peers, thank you for the professional camaraderie, shared knowledge, and moral support during the most demanding phases of this journey. Your collaboration made the road easier and the process more fulfilling. To my family and friends, your patience and understanding were never unnoticed. Whether through a listening ear, words of encouragement, or simply being there, your presence meant more than I can say. A special and heartfelt thank you to my father, Wayne Ceneskie. Your unwavering belief in me, quiet strength, and constant encouragement made this accomplishment possible. This journey began with your guidance and inspiration and ends with my deepest gratitude. Finally, thank you to all who have supported me in ways big or small. This achievement belongs to all of us.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Background of the Problem

With businesses moving many resources online, daily tasks can be completed without going somewhere physically. While this has made increasing productivity and managing lives easier, it has also impacted on companies and organizations. In the past, individuals would have to use their breaks or lunchtime to complete errands physically.

However, individuals now use their computers during scheduled work hours to complete these errands. When people use the company or organization's computers and internet for personal use (e.g., Facebook, Amazon, YouTube, online banking), it is called cyberloafing (Sener, 2020). Over the last decade, cyberloafing has become an increasing problem, but the growing security threats and network degradation have caused it to be more of a concern.

Research has been conducted into the effects of cyberloafing on information technology (IT) infrastructure and found that 73% of security breaches were caused by employee internet misuse (Mamat & Baqutayan, 2021). Cyberloafing costs businesses around $85 million annually in lost productivity (Ohana et al., 2024). An organization will experience severe strain on network performance and introduce security threats to the network (e.g., viruses and malware; Mamat & Baqutayan, 2021).

Information Technology Problem Focus and Project Purpose

Problem Statement

Employees using business resources for cyberloafing can negatively affect network performance and other employees at various levels of severity (Hadlington & Parsons, 2017). In a recent study, on average, employees spent between three hours per week and 2.5 hours a day using business resources for cyberloafing instead of performing assigned work-related tasks (U.S. Bureau of Labor Statistics, 2023). The general IT problem is that some school districts in K-12 public school systems cannot protect their IT infrastructure from network degradation and ransomware security threats. The specific IT problem is that some school districts in K-12 public school systems cannot protect their IT infrastructure from network degradation and ransomware security attacks due to employee cyberloafing.

Purpose Statement

In this quantitative correlational study, I aimed to examine the relationship between network degradation, ransomware security attacks, and employee cyberloafing. For this study, the research was conducted through a written request under public records request, containing criteria that needed to be gathered from enterprise-level Next Generation Firewall (NGFW) appliances. Students cannot complete standardized testing, and productive employees cannot perform necessary work-related tasks while network resources are being compromised by individuals using them for cyberloafing (Chen & Gopalan, 2021). Improving awareness regarding the importance of network degradation and ransomware security attacks may enable employees to perform better school-related tasks, such as presenting education-related materials, conducting school research, and completing online standardized testing, which may lead to positive social change.

Theoretical Framework

Activity theory (AT) provides a unique perspective for understanding human-technology interaction and guiding research. AT helps understand how people interact with their environment, including the role of technology in shaping human activity (Kaptelinin & Nardi, 2018). It allows for examining the complex interplay between individual actions and the broader social, cultural, and historical context in which they occur. Engeström's (2015) modified version of AT emphasizes the importance of understanding how human activity shapes and is shaped by the broader system in which it occurs (Kaptelinin & Nardi, 2018).

Applying AT to the study focused on network degradation, ransomware security attacks, and employee cyberloafing. For example, Li, He, et al. (2019) and Karlsson et al. (2022) suggested that examining how the organization's culture influenced information security behaviors could help identify potential interventions that addressed underlying factors, including network degradation. Similarly, Siponen et al. (2014) and Yazdanmehr and Wang (2023) emphasized the importance of organizational policies in shaping employee behavior and adherence to information security policies. When effectively implemented, these policies significantly impacted network degradation by minimizing risks and optimizing resource usage.

Analyzing these policies helped identify areas for improvement and strategies to promote compliance with information security protocols. Moreover, Yuryna Connolly et al. (2020) studied ransomware vulnerability and found that factors such as inadequate security awareness training, outdated software, and insufficient backup systems increased the risk of ransomware security threats. Organizations developed strategies to mitigate the risk of ransomware security threats and network degradation by analyzing the technology infrastructure and identifying potential vulnerabilities.

Operational Definitions

Cyberloafing: Using the work Internet during working hours for personal activities unrelated to work or class (Sener, 2020).

Malware: Unwanted software deployed to systems that attackers use to launch cyberattacks (Aslan & Yilmaz, 2021).

Network Degradation: Measurements based on bandwidth and latency between network segments to determine the quality of service (Shukla et al., 2023).

Ransomware: Encrypts files on systems, making them inaccessible and users powerless without a decryption key (Alqahtani & Sheldon, 2022).

Security Threats: Targeted attacks (e.g., sabotage), email attacks (e.g., phishing, malware, spam), web attacks, and ransomware (Yurekten & Demirci, 2021).

System Performance: Condition of a framework that plays out its expected capacities without being corrupted or debilitated by changes or interruptions in its internal or external environments (Gegan et al., 2020).

Research Question and Hypothesis

RQ: What is the relationship between network degradation, ransomware security attacks, and employee cyberloafing?

$H_0$1: There is no statistically significant relationship between network degradation, ransomware security attacks, and employee cyberloafing.

H_a1: There is a statistically significant relationship between network degradation, ransomware security attacks, and employee cyberloafing.

Assumptions, Limitations, and Delimitations

Assumptions

An assumption is not classified as a lie or falsehood but is accepted as accurate without proof (Lau et al., 2021). Within quantitative research, I evaluated a hypothesis that examined an assumption and relationships between dependent and independent variables (see Bloomfield & Fisher, 2019). Any hypothesis was considered an assumption until the study was completed, data collected, and a statistical analysis was conducted.

Regarding the effects of cyberloafing, I identified several underlying assumptions. First, there was a perception that an increase in cyberloafing resulted in an increase in ransomware security attacks and network degradation. Furthermore, cyberloafing was believed to increase the danger of ransomware security attacks. In addition to these security issues, the report also argued that cyberloafing reduced bandwidth availability. The network performance of the entire system was thus assumed to be negatively impacted by this constrained bandwidth.

Limitations

Weaknesses within a study were known as limitations that could have influenced the outcomes or conclusions (Ross & Zaidi, 2019). Limitations may have existed in the data collection, analysis, and study results phases. During data collection, a limitation could have occurred if the school district did not have an NGFW capable of collecting the data needed for the research or if the school district responded to what they believed the researcher was looking for (Ross & Zaidi, 2019).

There were two opportunities for limitations during data analysis. One included using non-probability sampling over probability sampling within a target population (Ross & Zaidi, 2019). Another occurrs when unplanned posthoc analyses were employed and not declared before the initial analysis (Ross & Zaidi, 2019).

The study results' limitations focused on validity. There were two types of validity: internal (reliability or accuracy) and external (generalizability; see Ross & Zaidi, 2019). Threats included time instead of maturation, instrument modification, repeated measurement, and participant selection extremes (Ross & Zaidi, 2019).

Delimitations

Researchers defined delimitations as neither positive nor negative but as limitations (e.g., boundaries or limits) set forth by the researcher to make the objectives possible to achieve (Theofanidis & Fountouki, 2019). For example, when looking at an SQL query statement for retrieving data from a database, delimitation would have been considered a where clause that filtered the data, so only the necessary data would have been retrieved. In this study, several delimitations were developed to ensure focus and prevent the study from becoming oversaturated with data.

Several delimitations were established for this study to ensure clarity and specificity in the research process. First, I used information received from K-12 public school districts. Requests for replies were sent to K-12 public school districts with access to NGFW appliances and consoles. The scope of data collection was limited to devices and programs intended to collect data on bandwidth use, website usage, and potential security risks. Importantly, strict precautions were put in place to ensure that no information was acquired that could identify students, employees, or faculty members. Any data that did not fit the study's predetermined criteria was immediately eliminated and did not impact the outcome.

Significance of the Study

Several aspects of the research have been conducted on the topic of cyberloafing and the effects it has on the workplace. As other research demonstrated, cyberloafing increases productivity by limiting aggression and stress in the workplace. However, individuals took advantage of this ability, impacting system performance.

There were a couple of different implications that could have resulted from this study. It may have been determined that cyberloafing significantly affected the organization's information technology infrastructure and ransomware security attacks, or it had no significant impact. If a correlation were discovered, researchers and practitioners could begin developing methods to decrease the effects of cyberloafing. However, it required an internal social change in how cyberloafing and browsing etiquette were perceived.

No matter what the outcome, sound arguments could have been produced on either side. Finding no impact meant that cyberloafing could continue to decrease aggression and stress while increasing productivity (Liang et al., 2022). On the other hand, if cyberloafing had an effect, ways to limit time spent doing so or circumvent the dangers (e.g., downloading files, preventing specific sites) could be developed while still allowing some cyberloafing to continue.

Managing cyberloafing may impact K–12 public school systems and promote social change. Reducing cyberloafing leads to increased network performance, allowing students and staff to access external (e.g., assessment testing sites) and internal resources (e.g., file shares) uninterrupted (Lim & Teo, 2024). Along with reduced security threats that prevented workstations from being usable, it also limited the number of students and staff accessing resources.

Social change may have occurred over time as more students gained access to uninterrupted resources, allowing them to expand their knowledge and prepare for their future. Uninterrupted resources enabled them to access information, accelerate learning, practice what they had learned, and deepen their understanding of concepts (Foutsitzi & Caridakis, 2019). These varying perspectives tended to lead to advancements and improved the world around us, allowing more students to expand their knowledge through innovative technologies.

Transition

In this study, I investigated the relationship between network degradation, ransomware security attacks, and employee cyberloafing. This section provided an in-depth background into the study's problem, purpose, and nature. Midway through the section, the activity theoretical theory framework used in the study was discussed.

As the study progressed, many more details are covered in the following sections. The next section is the literature review, which provides a critical analysis and synthesis of literature from the last 5 years. Some topics discussed in section three include the researcher's role, population and sampling, ethics in the study, data collection techniques, and validity. Finally, in section four, the findings are presented along with the application of the study to professional practice, how the study affects social change, and recommendations for further action.

Section 2: Literature Review

Review of the Professional and Academic Literature

In several articles, it was credited that Kamins first published the term *cyber-loafing* (Simsek & Elciyar, 2021). However, it was not until the early 2000s that research into cyberloafing began to gain attention, and research outlined eight items related to browsing activities and three for emailing activities (Lim, 2002). However, with technological advancements and widespread adoption over the decades, cyberloafing has had adverse effects (Tandon et al., 2022).

The problem with cyberloafing is that it distracts users from their work and introduces network degradation and ransomware security threats (Tandon et al., 2022). Employee cyberloafing broadened to include online shopping, blogging, gaming, instant messaging, online gambling, pornography, and tracking of personal investments (Lim & Teo, 2024). The reasons behind cyberloafing were more intriguing, such as boredom, lack of control, lack of justice, computer skills, and job satisfaction (Simsek & Elciyar, 2021).

However, regarding cyber risks, users were the weakest link and introduced viruses and malware into the technology infrastructure (Sulaiman et al., 2022). Malware and viruses reduced user productivity by limiting network bandwidth and posting information security breaches (Wu et al., 2020). Within a school district, security breaches could have had detrimental long-term effects, especially if attackers gained access to young students' personal information (e.g., social security numbers). The attackers could have used this information to open accounts that would not have been discovered for years, until it was too late.

Search Analysis and Synthesis

I used references from 105 peer-reviewed publications in this study. Of the total, 89 publications (or 85%) were released in the previous 5 years, highlighting the most recent advancements and innovative studies in ransomware security attacks, cyberloafing, and network deterioration. These recent studies provided the most current theoretical developments, methodologies, and up-to-date data, which were extremely helpful to my research on the quantitative correlational relationships among these variables.

The remaining 16 articles (or 15%) were released more than 5 years ago. Although published more than 5 years ago, these papers were crucial to my study since they established fundamental theories and well-established empirical results in network security, cyberloafing, and network deterioration. These older studies provided a historical viewpoint and a standard against which more contemporary changes and trends were evaluated.

The amalgamation of perspectives from both contemporary and past papers facilitated a thorough comprehension of the dynamic character of network security predicaments and their influence on staff conduct. The methods and analysis of my study were supported by this well-balanced collection of foundational and contemporary literature, which offered a robust framework for examining the intricate interactions between technology vulnerabilities, security breaches, and employee behavior within enterprises.

Review Organization

The organization of the literature review was designed to be simple and to flow logically, allowing readers to gain a better understanding of the topic. Gaining a better understanding of the meaning of cyberloafing was an essential first step. Next, outlining information technology infrastructure provided context on components that were important in technology and could be affected by cyberloafing. This led to the final part, which discussed the relationship between cyberloafing and ransomware security threats.

Purpose

The purpose of this quantitative correlational study was to examine the relationship between network degradation, ransomware security attacks, and employee cyberloafing, with a specific focus on the difficulties encountered in K–12 public school districts (see Wlosinski, 2020). These educational institutions were precarious because they relied on technology for instruction and faced resource constraints. Degradation of the network impaired regular administrative operations and interfered with crucial academic procedures, immediately impacting student learning outcomes. These problems were worsened by ransomware attacks, which jeopardized the security and integrity of private student information and seriously harmed districts’ finances and reputations (Koomson, 2021).

Furthermore, in this intricate situation, the problem of employee cyberloafing, which was frequently disregarded, was crucial (Tandon et al., 2022). In addition to adding to the network's bandwidth demands, employees who used the internet for non-work-related purposes during working hours created more security holes that increased the network's vulnerability to ransomware attacks (Giordano & Mercado, 2023). Such actions had far-reaching consequences that affected the school district's cybersecurity posture and network performance (Tandon et al., 2022).

In this regard, I sought to increase knowledge of the interdependence of online habits, network health, and cybersecurity concerns among all stakeholders in the education sector (see Bhaskar, 2022). I aimed to promote more responsible internet usage and proactive cybersecurity policies by deepening my awareness of these links (see Cremer et al., 2022). This is especially important in the K–12 public school setting, where it was imperative to prioritize protecting the network and the educational experience of the pupils (Levin, 2021). The ultimate objective was to provide a more robust, safe, and effective digital environment where staff members could work confidently knowing that their network technologies were reliable and secure, and where students could flourish without hindrance.

Theoretical Framework

Researching different theoretical frameworks was a tedious process, as each one had to be analyzed to determine its viability for the study. While AT may not have initially seemed like a good fit, it provided the correlation needed to deduce the relationship between network degradation, ransomware security attacks, and employee cyberloafing. Human-technology interaction was crucial since humans engaged in cyberloafing, influenced network performance, and introduced ransomware security threats.

AT emphasizes the importance of context in understanding human activity, considering the social, cultural, and historical factors that shaped it (Engeström, 2015). It outlines a framework for evaluating and comprehending the complex and dynamic nature of human activity, recognizing that activity was not just a phenomenon that affected one person but also many people and objects (Leont'ev, 1978). It emphasizes the importance of contradictions and conflicts in human activity, which drove change and innovation (Nardi, 1995). However, it was often overly complex and challenging to apply in practice. The framework's focus on the multiple levels of activity systems and their dialectical relationships made it difficult to identify and analyze specific elements of human activity (Batiibwe, 2019). It may not have adequately accounted for individuals' subjective experiences and motivations within an activity system. The framework's emphasis on the collective and contextual nature of activity could have overlooked the role of individual agency and personal meaning-making (Bloch et al., 1994). It has been criticized for being too abstract and lacking concrete guidelines for practical application. While the framework provided a valuable lens for understanding activity, it does not always offer clear strategies or solutions for addressing problems within activity systems (see Vygotsky, 1978).

AT also demonstrates how technology affected the work environment and human behavior (Beer & Mulder, 2020). For instance, I examined how changes in technology impacted employees' work habits and the potential risks associated with these changes. By identifying these risks, organizations could develop strategies to minimize potential harm to employees and the organization (Veazie et al., 2022). AT provided a valuable framework for analyzing the complex interplay between human behavior, technology, and organizational factors, critical to understanding the relationship between network degradation, ransomware security attacks, and employee cyberloafing (Dutta et al., 2021).

Several recent studies supported the use of AT in understanding this relationship. Syed (2020) found that employees engaged in cyberloafing were more likely to experience adverse job outcomes, such as decreased job satisfaction and increased turnover intention. Lim and Teo (2024) examined the relationship between cyberloafing and information security threats and found that cyberloafing was positively related to security threats, including the risk of ransomware security attacks. Several researchers found that cyberloafing was negatively related to creativity, suggesting that employees who engaged in cyberloafing were less productive and innovative (Tsai, 2023). Deterding et al. (2011) examined the impact of gamification on cyberloafing and found that gamification increased employee engagement with work-related tasks, thereby reducing the likelihood of cyberloafing.

Recent studies also examined the impact of the COVID-19 pandemic on remote work and cyberloafing. Galanti et al. (2021) analyzed the pandemic's impact on remote work and found that it led to significant changes in work activities, including an increase in cyberloafing. They suggested that organizations develop new strategies for managing remote workers to minimize the potential risks associated with cyberloafing and other work-related behaviors. Alkhalil et al. (2021) and Williams et al. (2020) examined the impact of COVID-19 on organizations' information security and found that the pandemic increased the risk of cyberattacks, including ransomware security threats. They emphasized the need for organizations to invest in cybersecurity measures and to train employees to recognize and respond to security threats.

AT offered a valuable framework for understanding the complex relationship between human behavior, technology, and organizational factors in network degradation, ransomware security attacks, and employee cyberloafing. It helped identify potential interventions to address underlying factors, vulnerabilities in technology infrastructure, and strategies to minimize potential harm to employees and the organization. Several studies supported the use of AT in exploring these relationships. Recent research also examined the impact of the COVID-19 pandemic on remote work and employee cyberloafing, suggesting new strategies for managing remote workers to minimize the potential risks associated with network degradation, cyberloafing, and other work-related behaviors (Reizer et al., 2022).

Apart from its theoretical foundations, AT provided valuable perspectives on the reasons underlying cyberloafing (Giordano & Mercado, 2023). According to AT, every human action has a purpose, and addressing the underlying reasons for cyberloafing requires understanding those purposes (Giordano & Mercado, 2023). For example, workers may have resorted to cyberloafing as a stress-reduction strategy or due to low engagement or job satisfaction (Giordano & Mercado, 2023). To create more effective regulations and interventions that went beyond simple limitation and monitoring—and instead, focused on building a more rewarding and engaging work environment—it was imperative to identify these root causes (Jack, 2021).

Additionally, AT helped investigate how corporate culture influenced workers' behavior regarding network security (Karlsson et al., 2022). The theory suggests that all activity systems, including organizations, were shaped by preexisting norms, values, and practices (Yip et al., 2020). Employees may have been more likely to engage in risky cyber behaviors where security protocols were not prioritized or where network usage was viewed casually (Cremer et al., 2022). As a result, applying AT assisted in designing organizational changes that promoted a culture of cybersecurity awareness and responsibility (Bhaskar, 2022).

AT's emphasis on collaborative and mediated action provided a framework for understanding how cooperation and communication within an organization could be used to counter cyberloafing and improve network security (Morrison-Smith & Ruiz, 2020). According to Tandon et al. (2022), companies could enhance their ability to manage and reduce the risks connected with cyberloafing by increasing collaborative processes and communication channels. This included holding regular team meetings to discuss cybersecurity concerns, working together to create security standards, or utilizing peer-to-peer support and learning platforms (Tandon et al., 2022).

The development of safer and more user-friendly technological systems benefited from applying AT to analyze the relationship between technology and human behavior. Designers and IT specialists could build systems that are more aligned with users' needs and habits while being more resilient to threats like ransomware by better understanding how employees use technology (Moustafa et al., 2021). By making work-related tasks more engaging and fulfilling, this alignment could have helped decrease cyberloafing by naturally encouraging employees to avoid unproductive activities (Mazzetti & Schaufeli, 2022).

AT offered a fresh perspective for understanding and addressing the complex phenomena of ransomware attacks, employee cyberloafing, and network deterioration (see Yuryna Connolly et al., 2020). AT provided insightful analysis and practical solutions for enhancing network security and worker productivity by considering the complexity of human behavior and the interactions between individuals, technology, and organizational context (Dutta et al., 2021).

When working with theoretical frameworks, many different options were available, especially those relevant to technology. However, the number that could facilitate the relationship between network degradation, ransomware security attacks, and employee cyberloafing was limited. To better understand why a framework may not have worked, several examples are examined, and the justifications are discussed.

Technology Determinism Theory

Analyzing the relationship between ransomware security assaults, employee cyberloafing, and network degradation may not have been appropriate if the notion that technology was the primary driver of societal change was advanced (Cheng, 2022). At the heart of the technology determinism theory, this theory ignores the complex socio-technical factors that led to these occurrences. Organizational policies, technological flaws, sociocultural factors, and human behavior influenced cyberloafing, which in turn affected ransomware security risks and network degradation (Hallström, 2022). The technology determinism theory emphasizes technology as the sole factor influencing social shifts and ignored these complex factors (Hallström, 2022).

The reciprocal nature of the interaction between technology and society was not considered by the deterministic approach that regarded technology as the primary agent of change (Hallström, 2022). Human actions, choices, and cultural circumstances both influenced and were influenced by technology. For example, an organization's rules, culture, and employee conduct all affected how network security measures were designed and implemented (Grobler et al., 2021). Technology determinism theory is limited in its usefulness when studying the intricacies of cyberloafing and its effects, as it failed to account for this bidirectional influence (Hallström, 2022).

According to recent research, human agency and decision making were crucial for comprehending the connection between ransomware security threats, network degradation, and employee cyberloafing (Argaw et al., 2020). Individual intentions and behaviors primarily drove these occurrences (Li & Liu, 2021). Employee motivations, attitudes, and awareness were crucial factors influencing whether they participated in cyberloafing activities and unintentionally contributed to ransomware security risks (Snider et al., 2021). This emphasis on individual agency contradicted the deterministic perspective of the technology determinism theory, which minimized the role of human intentions and decisions in technological events (Hallström, 2022).

Hallström (2022) argued that the technology determinism theory fails to adequately consider how organizational variables influenced technology use and its outcomes. The way technology was employed in a business was affected by policies, management techniques, and workplace culture (Easa & Orra, 2021). Strict guidelines and constant observation, for instance, could have lessened cyberloafing but may also have hurt staff morale and innovation. Understanding such organizational dynamics required awareness of network security and employee behavior (Quader & Janeja, 2021).

The technology determinism theory was not appropriate for examining the complex relationship between ransomware security attacks, employee cyberloafing, and network degradation because it could not adequately capture the intricate interplay of human behaviors, intentions, and sociotechnical factors involved in these phenomena (see Hallström, 2022). A more comprehensive approach was required for a thorough understanding that considered the complex interconnections between people, technology, and their social surroundings (Parker et al., 2022).

The theory's deterministic approach overlooked the possibility of proactive and adaptable solutions to technology problems (Hallström, 2022). Workers, for example, could have been educated to identify and address cybersecurity risks, converting potential weaknesses into advantages (Soon Chew, 2023). The lack of consideration for flexibility and the ability to learn and evolve in technology determinism theory limited its applicability when considering the current cybersecurity landscape (Hallström, 2022).

Technology determinism theory provided valuable perspectives on the impact of technology on societal transformation. However, its deterministic framework was inadequate for examining the intricate and diverse relationships between technology, organizational culture, and human behavior regarding ransomware attacks, network degradation, and cyberloafing (Aboramadan et al., 2019). For a more accurate and successful examination of these problems, a more integrated approach that recognized the interaction of technical and human variables was necessary.

Unified Theory of Acceptance and Use of Technology (UTAUT)

According to Momani (2020), the UTAUT concerns how people accept and use technology in different contexts, particularly in the workplace. By considering elements including performance expectations, effort expectations, social influence, and enabling conditions, it sought to explain users' behavioral intentions and technology usage. Although UTAUT offered insightful information about how people accepted and used technology, it did not explicitly address the connection between network degradation, ransomware security threats (malicious software that prevented access to a computer system until a ransom was paid), and employee cyberloafing (using technology for nonwork-related activities; Tamilmani et al., 2021).

Furthermore, according to Dwivedi et al. (2019), the UTAUT does not explicitly consider security-related aspects of technology use, such as the dangers and repercussions of engaging in cyberloafing or the avoidance and mitigation of ransomware security attacks. Given that I examined the connection between network degradation, ransomware security attacks, and employee cyberloafing, it was critical to consider the broader cybersecurity environment, and the unique motives and behaviors connected to these phenomena. To examine the connection between network degradation, ransomware security attacks, and employee cyberloafing, other frameworks or theories that focused on information security, cybersecurity behavior, or individual motives in the context of harmful behaviors were more pertinent.

Although UTAUT was a valuable framework for analyzing technology acceptance and use, it might not have been the best for examining the connection between network degradation, ransomware security attacks, and employee cyberloafing (see Momani, 2020). Alternative theories or frameworks that addressed cybersecurity, why people engaged in nonwork-related activities, and their effects on ransomware security threats were considered.

Although the UTAUT framework offered a solid foundation for comprehending broad trends in technology adoption and use, more modifications were necessary for its use in cybersecurity risks and network integrity challenges (Cremer et al., 2022). This theory emphasized elements that motivated people to accept and employ modern technologies, primarily focusing on the positive aspects of technology adoption. However, when it came to network security and cyberloafing, the key factors went beyond adoption and utilization; they also involved user actions that might have unintentionally jeopardized network security (Herath et al., 2022). For instance, UTAUT failed to explain why workers could have circumvented security procedures or participated in cyberloafing even when they knew the possible hazards. This suggested that, to address the intricacies of user behavior more comprehensively in cybersecurity, psychological and behavioral insights needed to be integrated into the UTAUT model (Moustafa et al., 2021).

There was a notable vacuum in the UTAUT model's attention to the drawbacks of technology use, particularly considering the ramifications of ransomware and cyberloafing (Maalem Lahcen et al., 2020). Individual user behaviors could have influenced the security and health of an organization's network in increasingly connected work settings (Giordano & Mercado, 2023). A more complex understanding of how and why users participated in actions that jeopardized network security may have been possible by including risk perception, user accountability, and the possibility of unfavorable consequences in the UTAUT framework (Cremer et al., 2022). This enlarged viewpoint helped in understanding the causal links between employee behavior and network problems and in creating focused measures to reduce these risks (Moustafa et al., 2021).

Diffusion of Innovations Theory

The diffusion of innovations theory focuses on adopting and diffusing recent technologies or innovations within a social system (Dearing & Cox, 2018). According to Xiong et al. (2016), they strongly emphasized relative advantages, compatibility, complexity, trialability, and observability. While ransomware assaults involved malicious software that encrypted files and demanded ransom payments, cyberloafing referred to the behavior of employees indulging in non-job-related internet activities while at work. These phenomena pertained to employee behavior and cybersecurity issues rather than the adoption or spread of recent technologies. The diffusion of innovations theory's fundamental ideas and frameworks did not directly correspond with the study subject.

To explain how innovations spread and are adopted, the diffusion of innovations theory focuses on the traits of innovations and those of adopters, such as innovativeness and opinion leadership (Dearing & Cox, 2018). However, network degradation, ransomware security attacks, and employee cyberloafing are separate phenomena with distinct causes and effects; this study focused on how they relate. Ransomware attacks typically result from malicious intent or coordinated criminal operations directed at specific individuals, businesses, or institutions, whereas employee cyberloafing is motivated by personal issues such as boredom, lack of enthusiasm, or a poor work environment. The multidimensional nature of these phenomena is not sufficiently captured by the elements driving the transmission of innovations, which limits the applicability of the diffusion of innovations theory to this study.

Although the diffusion of innovations theory has been widely applied in various contexts, it may not be directly applicable to research examining the relationships among network degradation, ransomware security attacks, and employee cyberloafing. These issues focus more on employee behavior and cybersecurity than on the acceptance and spread of new technologies. Moreover, the elements emphasized by the theory do not adequately reflect the complexities and motivations underlying these issues. Alternative frameworks that concentrate on organizational issues, cybersecurity, or employee behavior may be better suited to examine these connections.

Granić (2022) observed that although the diffusion of innovations theory provides insight into how modern technologies spread throughout a community or an organization, its primary emphasis is on the benefits of technology adoption and the conditions that encourage it. This perspective is limited when considering ransomware attacks and network disruption, which are often the result of harmful conduct or external malicious acts (Yuryna Connolly et al., 2020). The theory does not account for the dynamics of harmful technology use, such as ransomware deployment or cyberloafing, and how these practices propagate within an organization or affect its technical infrastructure (Beer & Mulder, 2020). A theoretical framework that incorporates both technology adoption and misuse, as well as the broader effects of such misuse on organizational security and efficiency, is necessary to understand these negative dynamics (Wolff, 2021).

Bozkus (2024) further argued that the diffusion model largely overlooks corporate culture and the internal environment, which can either reduce or increase the risks of technology misuse. The way technology is used or abused within an organization depends heavily on factors such as organizational policies, employee supervision, training initiatives, and overall work culture (Mazzetti & Schaufeli, 2022). These elements are essential for understanding and addressing network security and cyberloafing challenges (Giordano & Mercado, 2023). A theory that incorporates organizational components provides a more comprehensive understanding of how internal practices and culture influence employee behavior and, in turn, network performance and security.

Finally, the diffusion of innovations theory does not adequately address the psychological factors and human motivations underlying employee cyberloafing and susceptibility to ransomware attacks (Yuryna Connolly et al., 2020). Although the theory explores the traits of technology adopters, it does not account for the psychological and personal factors that lead individuals to become victims of ransomware or engage in cyberloafing (Bansal, 2021). Fully understanding these issues requires examining factors such as individual attitudes toward cybersecurity, awareness of risks associated with online behaviors, and the psychological appeal of cyberloafing (Kennison & Chan-Tin, 2020). Frameworks such as the theory of planned behavior or the health belief model, which focus on individual decision-making in the context of cybersecurity, may provide more appropriate approaches for this area of research (Maalem Lahcen et al., 2020).

Technology Acceptance Model

The technology acceptance model (TAM) focuses more on how people adapt to and accept technology than on their behavior or activities (Vorm & Combs, 2022). Cyberloafing, or the unauthorized use of the internet and other digital resources for nonwork-related activities at work, is a behavioral issue rather than a problem of technology adoption (Tandon et al., 2022). Ransomware security threats, by contrast, involve malicious software that encrypts files or systems and demands a fee to decrypt them (Hull et al., 2019). Instead of exploiting people's acceptance of technology, these attacks target vulnerabilities in computer systems. Therefore, examining the connection between network degradation, ransomware security attacks, and employee cyberloafing falls outside the scope of TAM.

The security component of technology, which is central to ransomware threats, is not explicitly considered by TAM. Cybercriminals deploy ransomware to gain unauthorized access to systems, steal data, and cause harm. Understanding the relationships among network degradation, ransomware security attacks, and employee cyberloafing requires examining security awareness, adherence to security policies, and the influence of individual behaviors on system vulnerabilities (Reshmi, 2021). TAM does not provide a comprehensive framework for capturing these dynamics and their role in the occurrence of ransomware threats.

Although TAM is frequently used to investigate technology adoption and acceptance, it may not be the most appropriate framework for examining the relationship between network degradation, ransomware security attacks, and employee cyberloafing. Theories that specifically address behavior, security knowledge, and the impact of user actions on the occurrence of ransomware security attacks provide a more suitable foundation (Alkhalil et al., 2021).

TAM is also less appropriate for examining behavioral nuances related to ransomware and cyberloafing because its primary focus is on adoption and use from a user's perspective (Bello et al., 2021). The model explains how individuals adopt and integrate technology into their daily lives, but it does not address misuse or behavioral patterns that result in security breaches (Ishaq et al., 2021). Cyberloafing represents a form of technological misuse influenced by organizational culture, personal work ethics, and perceptions of managerial oversight (Giordano & Mercado, 2023). These elements extend beyond the scope of TAM, which primarily emphasizes factors affecting constructive technology adoption (Nguyen et al., 2020).

Furthermore, TAM does not adequately address the cybersecurity challenges posed by ransomware. Such attacks exploit human error, carelessness, and technological vulnerabilities (Yuryna Connolly et al., 2020). Ransomware frequently takes advantage of behaviors such as falling for phishing attempts or failing to follow security protocols (Bansal, 2021). Addressing these challenges requires a framework that incorporates cybersecurity awareness, attitudes, and behaviors in addition to technology adoption

(Bansal, 2021). This holistic perspective is absent from TAM, which focuses primarily on usability and functionality rather than risk and security management (Shrestha et al., 2021).

Finally, Jan et al. (2022) argued that TAM does not sufficiently account for the organizational context in which technology is used or misused. Technology use is shaped by factors such as leadership style, administrative policies, and technical infrastructure (Dhamija et al., 2023). The organizational environment can either mitigate or exacerbate risks related to ransomware and cyberloafing (Yuryna Connolly et al., 2020). Reducing these risks requires organizations to prioritize cybersecurity and provide ongoing training and communication about online threats (Savaş & Karataş, 2022). These organizational dynamics are critical for understanding ransomware, network degradation, and cyberloafing, but TAM, with its focus on individual acceptance and usage, does not capture them (Hull et al., 2019).

Independent Variables Analysis and Synthesis

Ransomware is a form of malware that encrypts a victim's data and demands payment in exchange for the decryption key. Its emergence as a major security threat has generated widespread concern among individuals, businesses, and governments. Although a strong backup and recovery plan can help mitigate the severity of ransomware incidents, such attacks continue to have a substantial impact on organizations.

From a critical analysis perspective, ransomware poses serious consequences for victims, including financial losses, reputational damage, and potential legal liability (Humayun et al., 2021). At the societal level, ransomware disrupts critical infrastructure, compromises sensitive data, and fuels the growth of the cybercrime industry (MacColl et al., 2022). Some researchers have noted that its proliferation is partly due to increasingly sophisticated attackers who exploit software and system vulnerabilities (Sharton, 2021). In addition, the rise of cryptocurrency has made it easier for attackers to remain anonymous and collect ransom payments.

Network performance is a vital component of an organization’s digital infrastructure (Nadkarni & Prügl, 2020). Reliable performance is necessary for efficient daily operations and effective cybersecurity. Poor performance can delay the detection and response to cyber threats, including ransomware (Cremer et al., 2022). From a critical analysis perspective, network degradation exacerbates the negative effects of ransomware. For example, latency or downtime can delay the deployment of security patches or the execution of disaster recovery plans, thereby increasing both the severity and the duration of an attack.

From a synthesis perspective, ransomware and network degradation are intertwined factors that require a multifaceted approach for effective mitigation (Yuryna Connolly et al., 2020). This approach should include both technical and organizational measures, such as implementing strong access controls, performing regular backups, optimizing network performance, and educating employees on safe computing practices

(Argaw et al., 2020). These strategies reinforce one another; for instance, a high-performing network supports real-time monitoring systems that can rapidly detect ransomware activity. Because ransomware is a global threat, international cooperation is also critical for prevention and response (White House, 2021). Cybersecurity frameworks and information-sharing platforms that integrate ransomware risks and network performance metrics facilitate collaboration among governments, law enforcement agencies, and the private sector (Taherdoost, 2022).

In addition to technical and organizational measures, it is imperative to address the psychological and behavioral components of ransomware threats. Because outbreaks often succeed due to human error or negligence, employee behavior plays a pivotal role in cybersecurity. Establishing a culture of accountability and awareness within organizations is just as important as implementing technical safeguards (Bhaskar, 2022). Frequent training sessions, phishing simulations, and awareness campaigns help staff understand ransomware risks and the best practices for prevention (Jampen et al., 2020). Organizations strengthen their defenses against this evolving threat by cultivating a security-conscious workforce while deploying robust technological solutions (Goel, 2021). Integrating behavioral science insights also allows the design of user interfaces and security procedures that account for human tendencies and errors, thereby lowering the likelihood of ransomware breaches (Moustafa et al., 2021). This holistic approach—combining a deep understanding of human behavior with technical expertise—is essential for addressing the dynamic risks posed by ransomware in an increasingly connected digital world.

Dependent Variable Analysis and Synthesis

Cyberloafing refers to the use of the internet and digital devices for personal activities during work hours, which can reduce productivity, impair job performance, and increase security risks for organizations. From a critical analysis perspective, cyberloafing has been widely studied, and a growing body of research highlights both its negative and positive aspects. On one hand, cyberloafing decreases work performance and productivity, as employees spend time on nonwork-related activities such as social media, online shopping, and browsing the internet (Liang et al., 2022). This behavior is detrimental to organizational goals and can result in financial losses.

On the other hand, some research suggests that allowing employees to engage in limited nonwork-related online activities may increase job satisfaction, reduce stress, and foster creativity and innovation (Zhong et al., 2022). Conversely, restricting internet access during work hours can have negative consequences, such as elevated stress and lower morale. From a synthesis perspective, cyberloafing is best understood as a complex phenomenon influenced by multiple individual, organizational, and situational factors.

These factors include job demands, task autonomy, organizational culture, and individual differences such as personality and motivation (Bennett & Robinson, 2000). To mitigate the adverse effects of cyberloafing, organizations have implemented policies such as internet usage guidelines, monitoring software, and time management tools

(Giordano & Mercado, 2023). However, it is important to balance internet regulation with promoting employee well-being and job satisfaction (Schemer et al., 2021).

The technical environment in which cyberloafing occurs continues to evolve due to the rise of new digital platforms and the widespread use of mobile devices (Wolff, 2021). These developments make cyberloafing more covert and accessible, posing challenges to traditional monitoring and control methods (Tandon et al., 2022). As a result, companies must continually adapt their policies and strategies (Giordano & Mercado, 2023). This includes updating internet usage guidelines to reflect modern digital behaviors and implementing new monitoring technologies (Tandon et al., 2022). Organizational culture and technological advancements together shape the dynamic nature of cyberloafing practices (Giordano & Mercado, 2023).

Research on the psychology of cyberloafing indicates that it often reflects deeper workplace issues, including poor work-life balance, low engagement, or job dissatisfaction (Liang et al., 2022). Strict internet restrictions are not always effective in reducing cyberloafing; instead, addressing these underlying factors can be more successful (Liang et al., 2022). This approach includes fostering a healthy organizational culture, supporting employee well-being, and creating a more engaging workplace (Van der Voordt & Jensen, 2023). Such strategies provide benefits to both employees and employers by reducing cyberloafing while enhancing job satisfaction and productivity (Sao et al., 2020).

It is also important to consider cyberloafing in the broader context of cybersecurity (Cremer et al., 2022). While some forms of cyberloafing may appear harmless, they can unintentionally expose organizations to threats such as malware or phishing (Cremer et al., 2022). Consequently, effective strategies to address cyberloafing should include cybersecurity education and awareness initiatives (Bhaskar, 2022). By teaching employees about the risks of specific online activities and fostering shared responsibility for cybersecurity, organizations can reduce the likelihood of security breaches. Aligning cybersecurity objectives with efforts to manage cyberloafing ensures that interventions both minimize unproductive behavior and strengthen overall security posture (Cremer et al., 2022).

Measurement of Variables

Measurement is a fundamental aspect of quantitative research that involves assigning numerical values to variables to facilitate data analysis. Variables are generally classified into two types: independent and dependent. Independent variables are manipulated or controlled by the researcher, whereas dependent variables are observed and measured to determine the effects of the independent variables (Barroga & Matanguihan, 2022).

Selecting appropriate measures is essential to ensure the validity and reliability of quantitative study. Measurement scales include nominal, ordinal, interval, and ratio (Sekaran & Bougie, 2016). Nominal scales are used for categorical variables, while ordinal scales rank variables in a specific order. Interval scales provide equal intervals between values, and ratio scales include an absolute zero point (Sekaran & Bougie, 2016).

Measurement tools such as questionnaires, surveys, and interviews are often used to collect data (Tiersma et al., 2022). These tools should be carefully designed with consideration of research objectives and target population characteristics. Data analysis methods such as descriptive statistics, inferential statistics, and regression analysis are then applied (Hair et al., 2019). Descriptive statistics summarize the data, while inferential statistics test hypotheses and generalize findings to the population (Field, 2019). Regression analysis examines relationships between independent and dependent variables (Field, 2019).

Operationalization is central to measurement, as it translates abstract concepts into quantifiable variables (Eisend & Kuss, 2019). Each variable must be precisely defined in terms of how it will be assessed to ensure alignment with the concepts under study (Abulela & Harwell, 2020). For instance, operationalizing employee satisfaction may involve defining "satisfaction" and selecting a quantitative measure such as a Likert-scale survey (Abulela & Harwell, 2020). Proper operationalization ensures that the data collected is relevant and addresses the research questions, whereas poorly defined variables can result in data that is difficult to interpret (Eisend & Kuss, 2019).

The validity and reliability of measurement tools are also critical in quantitative research (Saltos-Rivas et al., 2021). Reliability refers to a tool's ability to yield consistent results under stable conditions (Ramezani et al., 2022). Validity concerns the extent to which a tool measures what it is intended to measure (Bakker et al., 2020). For example, a survey designed to measure job satisfaction should consistently produce similar results over time (reliability) while also accurately capturing employees' true sentiments (validity; Langner et al., 2023). To achieve this, researchers frequently conduct pilot studies or formal reliability and validity testing before using instruments in a full study (Phillips et al., 2021a). Such tests help identify and address weaknesses, improving the quality of research findings (Phillips et al., 2021b).

Ethical considerations are equally important in the measurement process (Favaretto et al., 2020). Researchers must obtain participants' informed consent, safeguard privacy and confidentiality, and avoid methods that could cause harm or discomfort (Grant, 2021). For example, survey or interview questions should not intrude on personal privacy or cause distress (O'Sullivan et al., 2021). Researchers must also ensure secure data management and transparency about how collected data will be used (Favaretto et al., 2020). Ethical measurement practices not only protect participants but also enhance the legitimacy and integrity of research, thereby strengthening confidence in the study's findings (Yadav, 2022).

Points of View and Relationship

Over the years, researchers have examined cyberloafing primarily in relation to its behavioral and psychological effects. Studies have explored whether cyberloafing is associated with productivity, stress, performance, and job satisfaction, with extended debates over its positive and negative aspects.

More recently, research has expanded to include organizational ramifications in addition to immediate behavioral and psychological outcomes (Giordano & Mercado, 2023). For example, scholars have investigated the impact of cyberloafing on company culture and team dynamics (J. Li et al., 2021). In organizations where cyberloafing is common and implicitly accepted, work ethics often decline, and organizational culture shifts toward lower productivity (Zhang et al., 2022). Conversely, in companies where cyberloafing is prohibited and tightly controlled, employee morale and trust may decline (Lunde et al., 2022). These organizational consequences affect not only individual productivity and satisfaction but also the overall well-being and effectiveness of the company (Roczniewska et al., 2022). Researchers have also examined financial implications by attempting to measure the cost of missed work hours and security risks related to cyberloafing (Giordano & Mercado, 2023).

As technology and workplace practices continue to evolve, researchers have studied how trends such as remote work, flexible scheduling, and the use of personal devices (BYOD) influence cyberloafing behaviors (Aczel et al., 2021). The blurring of boundaries between work and personal life in remote or hybrid contexts has challenged traditional definitions of cyberloafing and created the need for more nuanced inquiry. Studies have examined how remote work arrangements, worker autonomy, and the integration of social media into professional settings shape cyberloafing and its consequences (Giordano & Mercado, 2023). This emerging body of work is essential for organizations seeking to adapt management policies to the modern digital workplace.

These perspectives can be grouped into five views:

- Negative view - Many employers regard cyberloafing as misconduct that reduces productivity and poses security risks (Song et al., 2021). Employers adopting this view often deploy monitoring and access controls to prevent cyberloafing, protect sensitive data, and promote productivity (Giordano & Mercado, 2023). This strategy reflects concern with maintaining data integrity and organizational effectiveness.
- Positive view - Some researchers argue that brief nonwork-related online activity can improve morale and satisfaction (Liang et al., 2022). Occasional cyberloafing may reduce stress and foster creativity. Proponents of this perspective suggest that permitting moderate cyberloafing can support a more relaxed workplace climate, encourage teamwork, and enhance well-being (Ohana et al., 2024).
- Neutral view - Other scholars adopt a balanced stance, noting that cyberloafing can have both positive and negative effects depending on the type and frequency of activity and the organizational culture (Giordano & Mercado, 2023). From this perspective, context is key; organizations are encouraged to tailor guidelines that align with their goals and workforce dynamics (Tandon et al., 2022).
- Individualistic view - Some argue that cyberloafing is a personal choice and that employees should manage their own time, provided performance is unaffected (Razali, 2020). This perspective prioritizes outcomes over monitoring, emphasizing autonomy and accountability (Reisinger & Fetterer, 2021). By

focusing on results, organizations can build mutual trust while encouraging employee creativity and initiative.

- Technological view - Another perspective emphasizes that cyberloafing is a byproduct of increased technology use in the workplace. This view highlights the need for policies and training that balance technological benefits with productivity demands (Mason, 2022). Employers adopting this perspective stress adaptation and continuous education to mitigate risks associated with technology-enabled cyberloafing (Liang et al., 2022; Wolff, 2021).

In relation to this study, prior research primarily examined employees in business environments, whereas the current investigation focused on K–12 public schools, specifically targeting system administrators. Unlike earlier studies that sought to understand the motivations for cyberloafing, this study aimed to determine the correlation among network degradation, ransomware security attacks, and employee cyberloafing.

Transition

In the literature review, prior research on cyberloafing was analyzed to better understand its underlying causes. Several perspectives were presented, including positive, negative, neutral, individualistic, and technological viewpoints. The review also compared findings from previous studies with the focus of the current study. Despite these insights, there remains much to be learned about cyberloafing, particularly its effects on technology infrastructure.

Section 3 addresses the researcher's role, population and sampling, ethical considerations, data collection techniques, and validity. Section 4 will present the findings and discuss their application to professional practice, implications for social change, and recommendations for future research and action.

Section 3: The Project

Project Ethics

Role of the Researcher

Depending on the type of research conducted, the researcher can take on an engaging role. As a quantitative researcher, my role was divided into several facets, including developing the topic, research questions, and hypotheses, conducting and composing the literature review, analyzing data, and presenting the findings. This is aligned with Allen (2017), who stated that the role of a quantitative researcher was to determine a relationship between variables by obtaining and measuring data in a quantifiable way, such as through surveys, experiments, field research, and public data. Furthermore, experiments allowed the researcher to manipulate conditions to observe and analyze the effect on variable(s) (Allen, 2017).

Researchers played an essential role, but this could have introduced bias if they were related to the topic, participants, or area. I focused on cyberloafing and its effects on information technology infrastructure in K–12 public school districts in the United States. As a researcher, my relationship to the topic was through direct observation. I was a systems administrator and had witnessed the effects of cyberloafing on my information technology infrastructure. Having over 15 years of experience in information technology provided the knowledge needed to understand and analyze the data obtained through research.

The Belmont Report outlined the "ethical principles and guidelines for protecting human subjects of research" through the three principles of respect for persons, beneficence, and justice (United States Department of Health and Human Services, 1979, para. 12). Reviewing the Belmont Report provided an understanding of individual autonomy, protection from harm, securing well-being, and ensuring equality (see United States Department of Health and Human Services, 1979). These were achieved by obtaining informed consent, assessing risks and benefits, and selecting subjects appropriately. It was crucial for individuals to be allowed to determine what would and would not happen to them (United States Department of Health and Human Services, 1979).

Data for the study came from K-12 public school districts with Next Generation Firewall appliances. The data did not include personally identifiable information (e.g., name, address, social security number). The school districts were required to redact personally identifiable information. This may have resulted in out-of-scope data, but it helped provide control data for comparison.

Ethical Research

When conducting research, the researcher had to assess ethics and how they applied to the study. As a researcher, it was important to contribute to society, do no harm, be trustworthy and honest, act fairly, respect privacy, and maintain confidentiality (see Brinkman et al., 2017). The primary way to address and disclose ethical concerns was through informed consent.

Informed consent was provided to human participants with a form that explained the study's purpose, procedures, nature, risks and benefits, compensation, privacy agreement, and contact information. The informed consent process included three elements: it was an ongoing process updated after the study's success, participants had access to data, and they could request withdrawal of consent at any time (see Jacquier et al., 2021). However, there were no human participants in this study, and data was collected under the public records request, so informed consent was not applicable (Edwards, 2020). Since information was assembled in accordance with the public records request and no individuals participated, there was no method for withdrawal from the study.

To protect participants, no personally identifiable data was collected. Data collection focused on key areas: network degradation (capturing bandwidth usage and latency metrics), ransomware security attacks (including attack logs, intrusion attempts, and threat intelligence alerts), and employee cyberloafing (evidenced by URL access logs, application usage data, and time spent on non-work-related activities). Additionally, all data was time-stamped to ensure accurate tracking and correlation. Users' names, login information, or computer names that could identify a user were not collected. Each school district was assigned a random alphanumeric code to identify the collected data.

All data collected throughout the study was stored on a USB drive and will be housed in a safe deposit box for at least 5 years. This ensures that the data is not readily accessible or easy to read, thereby upholding participants' confidentiality and privacy.

Once the 5-year period was reached, the USB drive was destroyed using an industrial shredder regularly employed to destroy hard drives. The Walden University Institutional Review Board approved the study (IRB Approval Number 04-05-24-0670797).

Nature of the Project

A quantitative correlational study was conducted to determine the relationship between network degradation, ransomware security attacks, and employee cyberloafing—or individuals using network resources (i.e., computers, internet) for personal use. A quantitative method allowed statistical data to be collected through written requests and submitted electronically (Clifton-Sprigg et al., 2020). Data were then analyzed to find the interconnection between network degradation and ransomware security attacks while individuals used the network resources for personal use. A qualitative method did not fit this study, as the data did not need to be collected on-site, and only statistical data were collected (Lenger, 2019). Also, mixed methods implied that quantitative and qualitative designs would be used. A qualitative method was not used, meaning mixed methods were not a good fit for this study (Busetto et al., 2020).

A correlational design acknowledged the direct relationship between the independent and dependent variables (Seeram, 2019). An experimental design allowed a test environment to be set up and used to collect data (Sandjakoska & Stojanovska, 2020). However, this study used data related to network degradation, ransomware security attacks, and employee cyberloafing from NGFWs. While meta-analysis analyzed statistical data, it used multiple scientific studies (Eisend et al., 2020).

In the study exploring the relationship between network degradation, ransomware security attacks, and employee cyberloafing, the chosen data collection technique further affirmed the decision to employ an ex post facto research design. This method was particularly appropriate for this research, as an ex-post facto approach improved the effectiveness of research in several key respects.

Public records laws require that state and local government records be open for inspection and copying by any person. For this study, school districts were treated as public education agencies subject to such laws. A written request for information was submitted to each district to obtain the data for the research, preferably in an Excel spreadsheet format. A response within a reasonable timeframe, as outlined by the applicable statutes, was appreciated to facilitate timely progress in the research.

Document review as a data collection technique involved analyzing existing records or documents relevant to the research question (Dalglish et al., 2020). In this study's framework, these documents included IT logs, security incident reports, and personnel records related to employee behavior. Based on the analysis of previously available data to understand relationships and causation, the ex post facto model was perfectly compatible with document review. As the study did not involve manipulating variables, document review provided an excellent and discreet data source. It allowed researchers to observe and analyze them as they were typically followed.

For ethical reasons, this approach was constructive. An ex post facto design based on a document review ensured that research did not interfere with or manipulate natural real-world systems and events, which could have been risky or unethical (Busetto et al., 2020). In examining sensitive topics such as network degradation and ransomware attacks, an ex post facto design based on a document review ensured that research did not interfere with or manipulate the event. Instead, it facilitated an interdisciplinary examination of these phenomena that occurred naturally and provided insights into actual world events that did not involve ethical complications related to experimental manipulation.

In addition, a comprehensive understanding of the phenomena investigated was facilitated through document review. The documents often contained detailed, longitudinal data that provided a deeper understanding of the temporal dynamics of network degradation, security incidents, and employee behavior (Busetto et al., 2020). The application of AT, which stresses an understanding of broader context and historical development of interactions in an interconnected environment, was driven by the depth and richness of information.

However, other research designs could not fully exploit the existing data available through documents. For example, experimental designs focused more on current or future conditions created for the study, potentially overlooking the wealth of historical data at their disposal (Kulkarni et al., 2022). Similarly, while a longitudinal study could also have used document review, it would have required additional time and resources to monitor changes over time. In contrast, an ex post facto design efficiently used existing data for more immediate analysis (see Audulv et al., 2022).

In this study, selecting an ex post facto research design with a document review method was particularly effective. It offered an ethically sound, practical, and theoretically robust approach to examining the intricate relationships between network degradation, ransomware security attacks, and employee cyberloafing (Yuryna Connolly et al., 2020). This combination ensured a comprehensive and realistic analysis based on the reality of the phenomena under investigation.

Population, Sampling, and Participants

Population and Sampling

To complete a study, a researcher has to gather data from one or more sources and use the results to develop a conclusion. Conducting a survey is elaborate and time consuming, making it essential to refine the data collected to something more feasible and manageable (Qotba et al., 2021). Before techniques were applied to limit the focus of the study, this was referred to as the population, and once methods were implemented to filter the quantity studied, the sample remained (Jordan, 2018).

For this study, I sought to find the relationship between network degradation, ransomware security attacks, and employee cyberloafing. NGFWs were the main participants in this study. Data like bandwidth usage, latency metrics, attack logs, intrusion attempts, and threat intelligence alerts were essential for analyzing ransomware security assaults and network degradation on these NGFWs. To help fine-tune the amount of data collected, this was narrowed down to K-12 public school districts in the United States.

Within the quantitative method, there were two main sampling methods: probabilistic and non-probabilistic. Probabilistic sampling was used to select components so that each member of the population had the same chance of being chosen. When components could not be determined, non-probabilistic sampling was used (Amir et al., 2020). Considering the distinct attributes and technical information needed from the NGFWs, a non-probabilistic purposive sampling technique was used. This method enabled the selection of NGFWs according to factors including their kind, setup, and function within the network environment of K-12 public school districts, all related to the study's objectives.

Non-probabilistic sampling contained four subcategories that determined selected elements: availability, purposive, quota, and snowball. Availability sampling, also called convenience, was selected based on participants' immediate availability to the researcher and their willingness to participate (Vigneshwaran et al., 2017). Purposive sampling allowed individuals to be selected based on their experience with the research topic (Bailey et al., 2019).

Quota sampling involved breaking the elements into subcategories and required a specific number of participants to match each requirement (Talavera-Velasco et al., 2018). Finally, snowball sampling gained participants from the previous participants of another study that matched specific criteria (Patwardhan et al., 2017). Since I used data from NGFWs and needed to represent strict criteria, purposive sampling was used.

Participants

The NGFWs in the K-12 public school system were the main participants in this quantitative correlational research. These NGFWs were crucial to studying the link between network degradation (capturing bandwidth usage and latency metrics), ransomware security attacks (including attack logs, intrusion attempts, and threat intelligence alerts), and employee cyberloafing (evidenced by URL access logs, application usage data, and time spent on nonwork-related activities), along with timestamps. I examined information taken from these firewalls, including settings, security warnings, and traffic logs, to comprehend the subtleties of network performance and security in an educational setting.

In this study, systems administrators were essential facilitators. They operated as gatekeepers, allowing vital access to the NGFWs' data. Their knowledge and experience in administering and setting up these firewalls were crucial for appropriately interpreting the data. Spacey et al. (2021) stated that passing through a gatekeeper was frequently necessary to access an organization's data infrastructure. To start the gathering process, research was conducted in K-12 public school on the submittal process of the public records request, either through their website or by contacting the school district directly. Depending on the method provided for submitting a public records request, communication took place by email or in writing by mail.

In addition to advancing research, the information gathered from the NGFWs also benefited educational institutions. Fernandez et al. (2021) recommended that systems administrators consider deploying quality of service (QoS) protocols to maximize network performance, mainly if an investigation indicated excessive bandwidth utilization for non-educational purposes.

This research's participants were school districts with NGFWs deployed within K-12 public school system. To ensure a focused and uniform data collection process, the study excluded educational systems that were private, charter, religious, or located outside the United States. This delineation aimed to maintain a consistent study environment by concentrating on a specific educational sector facing similar cybersecurity challenges and regulatory constraints. Siegel and Navarro (2019) highlighted the importance of safeguarding data integrity and preventing eligibility fraud in academic research. Following their guidance, a request was directly submitted to the school districts under the public records request.

Instrumentation

Instrumentation refers to the tools, equipment, or materials used to collect data during a study (Babbie, 2016). Some of the most common research instruments were questionnaires, interviews, and observations (Zohrabi, 2013). Existing data gathered and reported from enterprise applications were used to obtain optimal statistical data for the study.

In the K-12 education sector, it was crucial to implement a firewall that monitored and recorded all the traffic across the network. This was needed to help protect students from accessing inappropriate materials, but it also prevented students and employees from accessing known malicious sites and monitored bandwidth usage.

The Electronic Communications Privacy Act of 1986 and several state statutes depict employee rights involving verbal and written communications (Freedman, 2023). Freedman (2023) explained that there was no expectation of privacy when using company devices, and it was assumed that user activity was visible to employers. To ensure that employees understood these expectations, a company had to devise an acceptable internet usage policy (Mohammad et al., 2019).

The organization was required to use an NGFW as it allowed more detailed data to be collected. Usually, a firewall contains source and destination IP addresses, protocol types, port numbers, packet sizes, and timestamps (Sanislav et al., 2018). An NGFW also collects application identification, user identification, content filtering, intrusion detection and prevention, and threat intelligence (Sridhar & Nandhini, 2021).

Taking a closer look at the data NGFW collected, I gained a clearer understanding of the concepts that were measured:

- Application identification – Applications used on the network, such as online browsing, email, social media, and file sharing, were recognized by NGFWs. By using this data, security regulations were upheld, and unwanted applications were avoided (Einy et al., 2021).

- User identification – Administrators were able to enforce security policies based on user identity and prevent unauthorized access to sensitive resources by using NGFWs, which identified specific users on the network (Jaggernauth & Rocke, 2021).
- Content filtering – NGFWs examined network traffic content, including emails, file transfers, and web pages. Administrators were able to prevent users from accessing harmful or unsuitable content (Duppa & Surantha, 2019).
- Intrusion detection and prevention – NGFWs recognized and stopped network-based threats like viruses, malware, and other harmful traffic (Alhasan & Surantha, 2021).
- Threat intelligence – Threat information feeds from other sources were included by NGFWs to find and stop known threats (Ibrahim et al., 2020).
- URL filtering – Next-generation firewalls examined the URLs accessed on the network and prevented access to harmful or unsuitable websites (Hussain et al., 2021).

Using a NGFW allows for the collection of all the data needed for the study. The data analyzed in the study included types of users (i.e., employees, students), types of websites visited, and content blocked/prevented from downloading or being accessed. To differentiate between student and employee data, user identification was helpful, allowing the focus to be placed on just employees. Next, it was necessary to determine sites that were visited outside the scope of an employee's regular work functions, so application identification was used to assess cyberloafing. Finally, the intrusion and prevention feature of the NGFW was used to flag sites determined as cyberloafing, high bandwidth use, or related to ransomware.

In a quantitative study, four measurement scales are commonly used: nominal, ordinal, interval, and ratio (Abulela & Harwell, 2020). Each scale supports different properties:

- Nominal – Classification
- Ordinal – Classification and rank order
- Interval – Classification, rank order, and equal interval
- Ratio – Classification, rank order, equal interval, and nonarbitrary zero (Bhandari, 2022a)

Different statistical tools are associated with each scale:

- Nominal – Frequency, percent, mode, bar charts, histograms, and pie charts
- Ordinal – Frequency, percent, median, mode (and in some cases mean and standard deviation), bar charts, histograms, and pie charts
- Interval – Mean, mode, median, standard deviation, range, and line graphs
- Ratio – Mean, mode, median, standard deviation, range, and line graphs (Bhandari, 2022a)

Three variables were examined in this study: network degradation, ransomware security threats, and employee cyberloafing. Because the analysis involved classification, rank order, and equal interval properties, variables were operationalized accordingly. For example, in the case of cyberloafing, websites were classified into genres such as social media, email, and streaming services. Bandwidth usage was measured for each category. For ransomware, the number of alerts triggered in association with the cyberloafing classifications was recorded.

It was expected that school districts would employ some form of firewall. However, it was not always clear whether they implemented an NGFW or another type of firewall lacking equivalent features. One limitation of the study was therefore related to the type of firewall deployed in a district. If a district did not have an NGFW, it could not provide all the requested data. In cases where NGFWs were implemented, the appliance was able to generate the necessary data, which was then supplied for analysis.

Scores were represented as whole numbers beginning with zero and increased by one each time an occurrence was logged. According to Cisco Systems (2021), NGFWs categorize websites into more than 200 possible categories, although the actual number implemented varies by organization. For each site logged under any category, the tally increased by one. Similarly, a secondary tally was recorded each time ransomware was detected after accessing a site, as well as the amount of bandwidth consumed by each category.

Here is an example of how the data appeared:

Table 1

Example Tally

Category	Visits	Ransomware	Bandwidth (GB)
Adult	7	5	12
Banking	15	0	2
Gambling	3	3	15
Shopping	32	12	25
Web-Based Email	107	59	120

When examining reliability and validity, this study measured the consistency and accuracy of the data. Unlike psychometric instruments, firewalls are not typically evaluated for these properties. Instead, common firewall performance metrics include detection rate, false positive rate, and response time. Effectiveness also varies depending on the type of firewall (software versus hardware). Several studies have found that hardware firewalls are more effective in detecting and blocking attacks (Konikiewicz & Markowski, 2017).

To address reliability and validity in this study, firewall data related to network degradation, ransomware security threats, and employee cyberloafing were evaluated using multiple strategies. Standard approaches include convergent validity, divergent validity, construct validity, internal consistency, and test–retest reliability (Fancourt et al., 2019). The strategies applied depend on the research question, sample size, measures, and study design.

For this study, the selected strategies included:

Validity

- Content validity - Content validity was addressed by ensuring that the criteria appropriately represented the measurement constructs (Liu et al., 2023). A literature review was conducted to identify existing scales or measures of network degradation, ransomware security threats, and employee cyberloafing. These items were then modified to fit the study's context to demonstrate content validity. Subject matter experts also reviewed and provided feedback on the criteria.
- Criterion-related validity - Criterion-related validity was assessed by comparing this study's results with established measures of risks associated with network degradation, ransomware security threats, and employee cyberloafing (Xie & DeVellis, 1992). Validated measures of these constructs were employed, and the findings from this study were compared to them to establish criterion-related validity.

Reliability

- Test–retest reliability - Test–retest reliability was assessed by administering the same criteria to the same participants at two different points in time (Kline, 2013). The results were then compared to evaluate consistency across administrations.

- Internal consistency - Internal consistency was measured by determining how closely the items represented the same construct. Inter-item correlations were calculated, and Cronbach's alpha was used to assess internal consistency (Nunnally & Bernstein, 1994).
- Split-half reliability - Split-half reliability was evaluated by randomly dividing the survey questions into two groups and comparing the outcomes. The Spearman–Brown prediction formula was then applied to calculate the correlation between the two halves (Streiner et al., 2015).

Adjustments are often required when standardized research instruments are adapted for a specific study. However, this investigation relied on data collected by next-generation firewalls (NGFWs) through a public records request and analyzed through document review. This did not eliminate the need for adjustments or revisions to the data-collection process. Under the public records request, the request included criteria such as bandwidth usage, latency metrics, attack logs, intrusion attempts, threat intelligence alerts, URL access logs, application usage data, and time spent on nonwork-related activities, all with associated timestamps. The public records request also required that personally identifiable information be redacted and removed before the data were provided.

Permissions to use instruments are included in the appendices section of the study, located after the references. Demonstrating that appropriate approvals were granted was particularly important. Any revoked approvals are also documented in the appendices.

Across the United States, there are numerous school districts and thousands of schools, creating significant potential for data collection. The raw data were not included in the dissertation to maintain clarity and avoid congestion. Instead, requests for raw data must be submitted to the researcher, who securely stored the data for the legally required retention period.

Data Collection Activities

Data collection is the process of gathering information that can be analyzed and interpreted to address research questions, hypotheses, and objectives (Barroga & Matanguihan, 2022). Each step in the research process is essential; while some may carry greater weight than others, data collection is central to the integrity of the study (Paradis et al., 2016). Errors during this stage can distort results and delay progress by months.

The technique used to collect data in this study is outlined below to ensure consistency and completeness:

1. Define the research question - The research topic was clarified before beginning the document review process (Xiao & Watson, 2019). This step guided the selection of documents most relevant to the study.

2. Request relevant data - Data pertinent to the research were requested from each K–12 public school district. These included both external documents (e.g., news articles, academic papers) and internal documents (e.g., reports, memos, policies) (Cooper et al., 2018). Next-generation firewalls (NGFWs) were internal

appliances; data were retrieved by filtering the requested information and exporting it into reports.

3. Create a review protocol - A document review protocol described how to evaluate and extract data from the identified documents (Petticrew & Roberts, 2006). This included specifying which documents to assess, how to review them, and how to extract relevant data (Petticrew & Roberts, 2006).

4. Review documents - After identifying relevant documents and establishing a protocol, each document was systematically reviewed to locate pertinent information that addressed the research questions. A consistent data extraction form was used to record findings (National Institute for Health and Care Excellence, 2022).

5. Analyze data - Once the review was complete, the collected data were classified, trends were identified, and judgments were made based on the results (Bloomfield & Fisher, 2019).

6. Interpret results - The findings were interpreted in relation to the research questions (Bauer & Scheim, 2019). This step involved drawing inferences from the data and assessing their implications for the study (Bauer & Scheim, 2019).

Using document review as a data collection technique offered both advantages and disadvantages, making it a suitable method for this study. Document review enabled the collection of large datasets efficiently and facilitated straightforward analysis in a quantitative framework.

According to the Centers for Disease Control and Prevention (2018), advantages and disadvantages of using document review as a data collection method include:

Advantages

- Cost efficiency - Document review generally does not require travel or specialized equipment, making it a cost-effective method.
- Historical data - Documents may provide historical information unavailable through other data collection approaches.
- Limited bias - Because the researcher does not interact directly with participants, document review is a nonreactive method that helps reduce potential biases.
- Large sample sizes - Documents often allow access to large datasets, which is particularly useful for studies requiring substantial sample sizes.

Disadvantages

- Existing data - Researchers may not have access to all of the information needed to fully address research questions, since document review is restricted to existing materials.
- Document creation bias - Documents may reflect the biases or limitations of the individual or group that produced them, potentially omitting important information.

- Difficulty obtaining documents - Accessing certain documents can be challenging, particularly when they are private or difficult to locate.
- Data quality control - Because the researcher does not generate the data directly, there is less control over its accuracy and quality.

After receiving Institutional Review Board (IRB) approval, conducting a pilot study is often considered an important step in ensuring research success. Because all studies involving human participants must be reviewed and approved by the IRB, this process safeguards participants' rights and welfare.

In this study, traditional pilot testing was substituted by rigorous compliance with IRB ethical standards and procedural protocols (Boise State University, n.d.). This approach integrated ethical and methodological rigor directly into the research design. By adhering to these standards, participant welfare was protected, risks were minimized, and research instruments and procedures were designed to be both ethically sound and methodologically robust.

This strategy also allowed potential ethical and methodological issues to be addressed preemptively, rather than uncovered through a pilot study. For example, comprehensive compliance reviews identified and corrected recruitment or data collection challenges to ensure alignment with ethical norms and research objectives. This commitment to standards enhanced the study's validity and reliability, as every component was executed with a clear emphasis on ethical responsibility and methodological precision.

Data Organization and Analysis Techniques

Collecting data is an integral part of research, but analysis is necessary to transform raw data into meaningful insights. Data analysis is the process of reviewing and interpreting collected information to draw conclusions, answer research questions, and address study objectives (Lester et al., 2020). Statistical and analytical approaches are used to organize, summarize, and analyze the data to identify patterns, correlations, trends, and associations (Mishra et al., 2019).

Data analysis in this study followed five general steps:

- Data preparation - To ensure accuracy and consistency, data were cleaned and organized (Kwak & Kim, 2017). This process included addressing errors, handling missing values, and removing outliers.
- Descriptive statistics - The basic properties of the data were summarized using descriptive statistics, which provided a fundamental understanding of the dataset (Kaliyadan & Kulkarni, 2019). Common measures included mean, median, mode, standard deviation, range, and percentages.
- Inferential statistics - Inferential techniques were applied to draw conclusions about the larger population from the sample data (Guetterman, 2019). Methods included regression analysis, confidence intervals, and hypothesis testing.
- Data visualization - Results were displayed using visual tools such as charts, graphs, and tables (Midway, 2020). Visual representations allowed patterns,

trends, and relationships within the data to be identified more effectively (Q. Li, 2020).

- Interpretation and findings - The results were interpreted in relation to the dissertation's goals and research questions (Johnson et al., 2020). Findings were discussed within the context of the existing literature and theoretical framework, enriching knowledge in the field (Grant & Osanloo, 2014).

When reviewing Section 1, the research question and hypotheses were recalled as follows:

Research Question

RQ: What is the relationship between network degradation, ransomware security attacks, and employee cyberloafing?

Hypotheses

$H_0 1$: There is no statistically significant relationship between network degradation, ransomware security attacks, and employee cyberloafing.

$H_a 1$: There is a statistically significant relationship between network degradation, ransomware security attacks, and employee cyberloafing.

A correlation analysis was conducted to assess the nature and direction of the relationships among network degradation, ransomware security attacks, and employee cyberloafing. This approach determined whether the variables exhibited linear relationships (Schober et al., 2018). Depending on the distribution of the data, either

Spearman's rank correlation coefficient or Pearson's correlation coefficient was applied (Schober et al., 2018).

Correlation analysis was selected because it quantifies both the intensity and direction of associations, making it particularly useful for analyzing how network degradation, ransomware activity, and cyberloafing relate to one another (Hung et al., 2017). The technique measured the degree of association, identified the direction and magnitude of the relationships, and served as a foundation for more advanced statistical analysis (Guetterman, 2019).

The correlation coefficient provided a measure of the strength and direction of association (Schober et al., 2018). For example, Fernando (2023) explained that the coefficient indicates whether variables move in the same direction (positive correlation), in opposite directions (negative correlation), or exhibit no discernible relationship. This measure offers insight into whether variables vary together in meaningful ways.

Correlation analysis also identified whether a linear relationship existed among network degradation, ransomware activity, and cyberloafing (Gravetter & Wallnau, 2017). This was important because it helped determine whether changes in ransomware activity or network performance were associated with shifts in cyberloafing behavior. The magnitude of the coefficient was used to gauge the closeness of the associations (Schober et al., 2018).

Finally, correlation analysis served as a starting point for further investigation. If statistically significant associations were identified, more advanced methods such as regression analysis could be used to explore predictive relationships while controlling for confounding variables (Bhandari, 2022b; Boston University, 2013). Correlation provided an essential first step for understanding the relationships among variables and guiding subsequent research (Rosseel, 2021).

Not all statistical techniques were appropriate for this study. Some methods are more suited to describing data than exploring relationships.

In particular:

- Descriptive statistics - While descriptive statistics such as means, frequencies, and percentages summarize data (Kaliyadan & Kulkarni, 2019), they cannot establish correlation or causation (Cooksey, 2020).
- Chi-square test - The chi-square test is often used to examine associations between categorical variables (Schober & Vetter, 2019). Although useful for categorical comparisons, it does not provide information about the strength or direction of relationships (H. Y. Kim, 2017).
- Analysis of variance (ANOVA) - ANOVA is used to compare means across groups (Kim, 2017). However, it is less suited for this study, which focused on continuous relationships rather than group differences (Sullivan, n.d.).
- Survival analysis - Survival analysis is designed for time-to-event data, such as time to failure or death (Le-Rademacher & Wang, 2021). Because the variables in this study were not inherently time-based, survival analysis was not appropriate.

Data cleaning and screening were essential steps to ensure accuracy, reliability, and suitability for analysis (Huebner et al., 2020). Data cleaning involved identifying and resolving errors, inconsistencies, and inaccuracies (van den Broeck et al., 2005). This process included handling missing values, addressing outliers, resolving formatting problems, and correcting entry errors. Data screening focused on verifying that the dataset met assumptions required for statistical analysis. This included checking distributional assumptions, assessing multicollinearity, identifying extreme outliers, and confirming patterns or anomalies (Flora et al., 2012). Conducting these procedures improved the trustworthiness of results and supported valid, reliable conclusions (Huebner et al., 2020).

The procedures for cleaning and screening data were as follows:

Data Cleaning

- Managing missing values - The dataset was examined for missing values, and appropriate handling methods were applied. Techniques included deletion (removing cases or variables with missing values) or imputation (replacing missing values with estimated values; Lin & Tsai, 2020).
- Dealing with outliers - Outliers—extreme values that could bias the analysis—were identified by reviewing the dataset. Depending on their impact and the data's characteristics, outliers were either retained, modified, or removed (Wada, 2020).

- Resolving formatting issues - Formatting errors such as incorrect date formats or inconsistent categorical variable representations were identified and corrected. Data was standardized to ensure uniformity across the dataset.
- Correcting data entry errors - Errors made during entry, such as transposed digits or typographical mistakes, were detected and corrected (Barchard et al., 2020).
- Handling data integrity issues - The dataset was checked for problems such as duplicate records or inconsistent information (Harris & Houser, 2018). Redundant entries were merged or deleted, and inconsistencies were resolved to preserve data integrity.

Data Screening

- Data distribution - The distribution of variables was examined to determine whether they met statistical assumptions (Thrun et al., 2020). Skewness, kurtosis, and normality were reviewed.
- Multicollinearity - Predictor variables were assessed for high intercorrelations, which could compromise regression models. Correlation coefficients and variance inflation factors (VIF) were calculated to detect and manage multicollinearity (Penn State University, n.d.).
- Influential outliers - Outliers with disproportionate influence on results or assumptions were identified using diagnostic tools such as Cook's distance and leverage statistics (Baba et al., 2021).

- Data patterns or anomalies - The dataset was reviewed for patterns, trends, or anomalies that could affect validity or interpretation. Plots and statistical tests were used to detect irregularities (Gianfrancesco & Goldstein, 2021).

In a quantitative study, addressing missing data is a crucial step in data analysis and interpretation. Missing data occurs when certain variables or observations in a dataset lack values or responses. If not properly handled, missing data can introduce bias and compromise the reliability of statistical analyses and research findings.

Several methods are commonly used to address missing data in quantitative research:

- Missing data pattern - Missing data were classified as missing completely at random (MCAR), missing at random (MAR), or missing not at random (MNAR) (Jakobsen et al., 2017; Perkins et al., 2017; Petrazzini et al., 2021).
- Extent of missing data - Each variable's percentage of missing data was examined to determine whether special handling was needed (Hayati Rezvan et al., 2015).
- Case analysis - Complete case analysis involved excluding incomplete cases, but this approach could bias results if missingness was related to study variables (Ross et al., 2020).
- Imputation - Missing values were replaced with estimated values using methods such as mean imputation, regression imputation, or multiple imputation (Hayati Rezvan et al., 2015).

- Sensitivity analysis - Findings were tested under different assumptions about missingness to evaluate robustness (Spineli et al., 2021; Tan et al., 2021).
- Missing data mechanism - Maximum likelihood estimation (MLE) and multiple imputation were applied depending on the missingness mechanism (Lee & Shi, 2021).
- Transparency and reporting - The percentage of missing data, methods used, and assumptions were documented to maintain transparency (Haneuse et al., 2021).

The following assumptions were assessed to ensure validity and reliability:

- Independence - Observations were assumed to be independent (Bakdash & Marusich, 2017). Violations could bias results (Schofield et al., 2021).
- Normality - Many methods assume data are normally distributed (Hayat et al., 2017). Deviations from normality can affect statistical accuracy (Knief & Forstmeier, 2021).
- Homogeneity of variance - Variability of the dependent variable was assumed constant across groups (Yang et al., 2019). Violations compromise ANOVA or t-test validity (Blanca et al., 2017).
- Linearity - Relationships between independent and dependent variables were assumed to be linear (Sarker, 2021). Nonlinear relationships require alternative approaches (Schuster et al., 2022).

- Absence of multicollinearity - Independent variables were assumed not to overlap excessively (Wallisch et al., 2022). Excessive multicollinearity leads to unstable coefficients (Giacalone et al., 2017).
- Random sampling - Statistical generalization assumes data are randomly sampled. Biased or non-random sampling undermines generalizability (Andringa & Godfroid, 2020; Wiśniowski et al., 2020).

To test and assess assumptions in a quantitative study, several techniques and procedures were applied:

- Visual examination - Histograms, scatter plots, and box plots were used to detect violations of linearity, variance homogeneity, and normality (Eberhard, 2021).
- Descriptive statistics - Means, standard deviations, skewness, and kurtosis were calculated (Bhandari, 2023a; Jammalamadaka et al., 2021).
- Normality tests - Shapiro–Wilk, Kolmogorov–Smirnov, and Anderson–Darling tests were applied, with caution regarding sample-size sensitivity (Rogers et al., 2020; Tomšik, 2019).
- Homogeneity of variance tests - Levene's and Bartlett's tests evaluated variance equality across groups (Cichoń, 2020; Odoi et al., 2019).
- Multicollinearity assessment - Correlation coefficients and VIF values were computed (Basu & Maji, 2022; Salmerón et al., 2020; Shrestha, 2020).
- Residual analysis - Residual plots were examined to identify issues with linearity and homoscedasticity (Feng et al., 2020; Schaffer et al., 2021).

- Robust methods - Nonparametric and robust alternatives were applied when assumptions were violated (Erceg-Hurn & Mirosevich, 2008).

Several strategies can be used to address violated assumptions in a quantitative study. The appropriate response depends on the specific assumption and the statistical analysis being conducted.

General approaches include:

- Transforming data - Logarithmic, square root, or Box–Cox transformations were used to address nonnormality (Raymaekers & Rousseeuw, 2021).
- Nonparametric tests - Tests such as Mann–Whitney U and Kruskal–Wallis were applied when assumptions were not met (Blanca et al., 2017; Mat Roni & Djajadikerta, 2021).
- Robust methods - Approaches such as weighted least squares regression provided reliable estimates despite violations (Ronchetti, 2021; van den Boogaart et al., 2020).
- Bootstrapping - Resampling with replacement generated confidence intervals and estimates without strict assumptions (Egbert & Plonsky, 2020).
- Sensitivity analysis - Results were reanalyzed under multiple scenarios to test robustness (Thabane et al., 2013).
- Reporting limitations - All assumption violations and remedies were reported to ensure transparency (Keserlioglu et al., 2019).

To interpret inferential results in quantitative study, researchers typically follow these steps:

- Understand research questions and hypotheses - Results were interpreted considering study hypotheses (Thelwall & Mas-Bleda, 2020).
- Identify statistical tests - Specific tests used (e.g., t-tests, ANOVA, regression, correlation) were reviewed.
- Examine p-values - P-values indicated the likelihood of results under the null hypothesis. Values below 0.05 were generally considered significant, though statistical significance does not always equal practical importance (Gao, 2020; Greenland et al., 2016; Mcleod, 2023).
- Consider effect size - Effect sizes such as Cohen's d, eta-squared, and Pearson's r quantified the strength of associations (Lakens, 2013; Schäfer & Schwarz, 2019).
- Assess confidence intervals - Confidence intervals (commonly 95%) indicated the range within which the true population parameter was expected to fall (Siegle, 2021). Results were considered statistically significant when the CI did not include zero (Greenland et al., 2016).
- Evaluate directionality and patterns - The direction of associations (positive, negative, or none) was compared against hypotheses.
- Account for confounding factors - Alternative explanations or influences were considered when interpreting results (Tennant & Ross-Hellauer, 2020; Varbanova & Beutels, 2020).

- Relate to existing literature - Findings were compared with prior research to assess consistency or divergence (Abu-Baker et al., 2021; Cooper et al., 2018; Zimmerman et al., 2021).
- Discuss limitations and implications - Study limitations, such as sample size and potential biases, were acknowledged, and implications for practice were addressed (Nadkarni & Prügl, 2020; Ross & Zaidi, 2019).

The statistical software program SPSS (Statistical Package for the Social Sciences) version 30 provided a wide range of data management and analysis capabilities. IBM's SPSS is well known for its user-friendly interface and broad functionality, making it widely used in the social sciences (Kulas et al., 2021). SPSS allows users to easily manage and import data from sources such as databases, text files, and spreadsheets. The software supported descriptive statistics, t-tests, ANOVA, regression, factor analysis, and other statistical techniques (Blanca et al., 2018).

Both novice and advanced users could access these functions through a menu-driven interface or syntax commands, offering flexibility. Visualization tools supported the creation of charts, graphs, and customizable reports, including bar charts, scatterplots, histograms, and pie charts (Loffing, 2022). These features simplified the analysis process and enabled clear presentation of findings.

SPSS version 30 also provided advanced options for data handling, including missing value imputation, data cleaning, and data transformation. Its functionality could be expanded by integrating with other statistical applications and programming languages. Overall, SPSS version 30 remained an effective tool for researchers and analysts, offering a comprehensive set of statistical methods, an intuitive interface, and versatile data management features (Loffing, 2022). It continues to be widely used in academic, social science, market research, and related fields where quantitative data analysis is essential.

Study Validity

In a quantitative correlational study, it is critical to consider potential threats to external validity. Because this study examined the relationships among network degradation, ransomware security attacks, and employee cyberloafing, several threats and strategies to address them were identified:

- Testing reactivity - This refers to the likelihood that participants' behavior is influenced by being observed or evaluated (Mshelbwala et al., 2020). To mitigate this threat, indirect measures of network degradation, ransomware security attacks, and employee cyberloafing were used, such as self-report surveys and archival data (Walentynowicz et al., 2018).
- Interaction effects of selection and experimental variables - This threat occurs when sample characteristics affect the observed associations between variables (Garofalo et al., 2022). To reduce this risk, efforts were made to obtain a representative sample reflective of the population of interest (Young, 2023). Random sampling techniques were also used to increase generalizability (Parsaeian et al., 2021).

- Specificity of variables - This threat arises when measurement methods do not fully capture all relevant aspects of constructs such as network degradation, security threats, and cyberloafing (Pennington et al., 2016). To address this issue, well-validated instruments were employed (Sham et al., 2021), and pilot testing was conducted to identify potential gaps (Pearson et al., 2020).
- Reactive effects of experimental arrangements - This refers to participants altering their behavior due to the experimental setting or circumstances (Wu, 2020). To minimize this threat, the study was designed to limit participants' awareness of observation, reducing the likelihood of deliberate behavior changes.
- Multiple-treatment interference - This threat occurs when exposure to multiple treatments or conditions influences participant responses (Lopez & Gutman, 2017). To counterbalance this risk, a within-subjects design was used, with each participant experiencing conditions in a different order (Sarkies et al., 2019).

When conducting research, it is important to consider not only external validity threats but also internal threats, such as:

- History - Internal validity can be compromised by outside events or circumstances that occur during a study and influence participant behavior (Mallinson & Hatemi, 2018). For example, network degradation, ransomware security attacks, and employee cyberloafing may be affected by policy changes or technological developments. To mitigate this risk, data were collected on major external events or policy changes that could influence the study variables and were included as control variables (Slocum et al., 2022).

- Maturation - Participants may change naturally over time, altering their exposure to network degradation, ransomware security threats, or cyberloafing behaviors (De Vries et al., 2021). To limit this effect, control groups or matched-pairs designs were considered (Cessie et al., 2008). Comparing participants with a control group helped isolate the effect of cyberloafing on network degradation and ransomware threats by reducing the influence of maturation.
- Testing - Prior experience with assessment tools or repeated testing may affect participant results (Nagler et al., 2021). To address this, alternative versions of instruments were used, instrument order was counterbalanced, or a control group that did not complete the instruments was included (Taber, 2017).
- Instrumentation - Bias or error introduced by inconsistent or poorly designed instruments may threaten internal validity (Mokkink et al., 2020). To reduce this risk, certified and reliable measurement tools were used (Mohajan, 2017). A pilot test evaluated the readability and comprehension of items measuring network degradation, ransomware security threats, and cyberloafing, with revisions made as needed (Srinivasan & Lohith, 2017).
- Statistical regression - Extreme scores on an initial assessment may naturally regress toward the mean on subsequent assessments, regardless of actual relationships among network degradation, ransomware threats, and cyberloafing (Cahit, 2015). To counter this, participants were selected across a broad range of

scores, multiple assessments were conducted over time, and baseline scores were statistically adjusted (Cahit, 2015).

After addressing external and internal validity threats, statistical conclusion validity was also considered. Statistical conclusion validity refers to the extent to which the results of a study accurately reflect the true relationships among variables (Ampatzoglou et al., 2019).

Potential threats to this form of validity and strategies to address them included:

- Violation of assumptions - Correlation analysis depends on certain assumptions, including normality, linearity, and homoscedasticity. Violating these assumptions can result in inaccurate findings (Bakdash & Marusich, 2017). To address this, nonparametric correlation methods such as Spearman's rank correlation were applied, or data were transformed to meet assumptions before conducting analyses (Janse et al., 2021).
- Outliers - Outliers can disproportionately influence correlation coefficients and distort results (Rousselet & Pernet, 2012). To mitigate this issue, analyses were conducted with and without outliers to determine their impact (Pernet et al., 2013). When appropriate, outliers were removed, or results were reported both ways to demonstrate their effect (Pernet et al., 2013).
- Restriction of range - When variables exhibit minimal variation, correlation coefficients may underestimate or overestimate associations (Janse et al., 2021). To prevent this, the range of scores for network degradation, ransomware threats,

and cyberloafing were examined prior to analysis. If the range was restricted, additional data were collected or partial correlation techniques were applied to account for confounding variables (Janse et al., 2021).

- Multiple comparisons - Running repeated tests without adjustment increases the risk of Type I errors (Menyhart et al., 2021). To control this risk, adjustments such as the Bonferroni correction were applied to maintain an appropriate significance level when evaluating multiple relationships (Haynes, 2013).
- Confounding variables - Uncontrolled confounding factors can inflate Type I error rates and produce spurious correlations (Busenbark et al., 2022). Relevant confounding factors affecting network degradation, ransomware threats, and cyberloafing were identified and included as control variables to isolate the true relationships (Westfall & Yarkoni, 2016).

Considering external validity in a quantitative correlational study on the relationships among network degradation, ransomware security threats, and employee cyberloafing is essential. External validity refers to the extent to which research results can be generalized to larger populations and applied in contexts beyond the study sample. To support the generalization of findings, several factors that influence external validity were carefully evaluated and addressed:

- Research context - The environment and circumstances of the study's execution were considered. Findings must be generalized with caution if they are unique to a specific group, industry, or location (Burchett et al., 2020).

- Measurement validity - To prevent bias, measurements such as survey questions and data collection procedures were ensured to be accurate and valid for the broader population (Tempelaar et al., 2020).
- Effect size - The relationships among network degradation, ransomware security threats, and employee cyberloafing were analyzed. If the effect size was minimal, the findings may have limited applicability in other contexts (Schäfer & Schwarz, 2019).
- Timeframe - The study timeline was examined to determine whether the phenomena may evolve over time (Bates & Glennerster, 2017). Shifts in the relationships among network degradation, ransomware threats, and cyberloafing could affect generalizability.
- Cultural and regional differences - Potential cultural or regional differences that might influence the relationships among the study variables were considered (Hanel et al., 2018).
- Similarity of settings - Generalizability increases when the circumstances of the study closely resemble those of the target population (Burchett et al., 2020).
- Researcher bias - To strengthen generalizability, potential biases in data collection and analysis were minimized (Baldwin et al., 2022).
- Replication - External validity is enhanced when other researchers can reproduce the study in different settings and obtain comparable results (Nosek & Errington, 2020).

Transition and Summary

This section has addressed multiple aspects of the study, including the researcher's role, population, sampling considerations, ethical research practices, data analysis methods, and study validity. The researcher's responsibilities encompassed developing the topic, formulating research questions and hypotheses, conducting a literature review, analyzing data, and presenting the findings. Ethical standards were emphasized throughout, ensuring that no personal identifiable information was collected and that all data was stored securely. In addition, the steps for performing statistical analyses were outlined, and potential threats to reliability and validity were identified along with strategies to mitigate them.

The following section presents the study's findings. It focuses on descriptive statistics, results of inferential analyses, and their placement within the theoretical framework. The findings are examined in relation to professional practice and their potential to drive social change. Recommendations for action, directions for future research, and reflections on the study are also discussed. Of particular interest is how the correlations among network degradation, ransomware security attacks, and employee cyberloafing can be applied within the field of information technology.

Section 4: Application to Professional Practice and Implications for Change

Presentation of the Findings

In this study, I employed a quantitative correlational research design to examine the relationship between network degradation, ransomware security attacks, and employee cyberloafing in K–12 public school districts.

Statistical Test

The primary statistical test used in this study was correlation analysis. Depending on data characteristics, either:

- Pearson's Correlation Coefficient (r) – if the data were continuous and normally distributed, or
- Spearman's Rank Correlation Coefficient (p) – if the data were ordinal or not normally distributed.

In addition, hypothesis testing was performed to assess the significance of the observed correlation coefficients, using p-values to determine whether relationships between variables were statistically significant.

Variables

Independent Variables

- Network degradation: Measured by bandwidth usage and latency metrics from NGFW logs.

- Ransomware security attacks: Measured by the number of detected ransomware attempts, intrusion attempts, and threat intelligence alerts from NGFWs.

Dependent Variable

- Employee cyberloafing: Assessed via URL access logs and application usage data, specifically time and frequency spent on non-work-related activities by employees during work hours.

Each variable was quantified in terms of counts (e.g., visits, ransomware hits) and usage volume (e.g., GB bandwidth consumed).

Purpose of the Test

The purpose of the correlation analysis was to:

- Determined the degree and direction of association between employee cyberloafing and both network degradation and ransomware attacks.
- Evaluated if increases in cyberloafing were associated with increased bandwidth usage or frequency of security alerts.

The *p*-values derived from correlation analysis informed whether the correlations were statistically significant, supporting or rejecting the null hypothesis.

Relationship with the Hypotheses

$H_0 1$: There is no statistically significant relationship between network degradation, ransomware security attacks, and employee cyberloafing.

H_a1: There is a statistically significant relationship between network degradation, ransomware security attacks, and employee cyberloafing.

The chosen statistical tests directly assessed these hypotheses by measuring the strength and significance of relationships among the variables. A significant positive correlation supported the alternative hypothesis indicating that cyberloafing may have contributed to degraded network performance and heightened security risks. Conversely, a lack of significant correlation supported the null hypothesis.

Variables Overview

This study investigated the relationship among:

- Network degradation (bandwidth usage in gigabytes, continuous variable)
- Ransomware security attacks (categorical variable, measured through firewall alerts)
- Employee cyberloafing (categorical variable, defined through firewall categories and messages)

Descriptive Statistics

A report of descriptive stats for variables like bandwidth use, ransomware alerts, and cyberloafing is presented in Table 2.

Table 2

Descriptive Statistics for Study Variables

Variable	*N*	Mean	*SD*
Bandwidth use (Gbps)	30	1,458.38	842.97
Ransomware alerts	30	8,277,397,953.6	3,311,612,175.3
Cyberloafing (visits)	30	1,893,874,468.8	1,120,451,753.1

Bandwidth Usage (Continuous Scale Variable)

The bandwidth usage, represented by network degradation quantitatively, measured in gigabytes (GB), is presented in Table 3.

- Mean bandwidth usage: Reported the average GB across the sample.
- *SD*: Reported on variability in GB usage.
- Range (Min-Max): The lowest and highest bandwidth usage was recorded.

Table 3

Descriptive Statistics for Bandwidth

Measure	Bandwidth (GB)
Mean	1,458.38
SD	842.97
Minimum	100.12
Maximum	2,348.19

Ransomware Security Attacks (Nominal Variable)

Ransomware security attacks were indicated by firewall alerts in the firewall log (category column). As shown in Table 4, the majority of high-confidence ransomware visits were categorized under Proxy avoidance.

- Frequency: Number of times each type of alert appeared.
- Percentage: Proportion of each alert type relative to the total number of alerts was calculated.

Table 4

Firewall Logs: Ransomware Category Frequency

Alert Type	Confidence	Frequency	Percentage (%)
Phishing	High	94,087	0.01%
Malicious websites	High	136,217	0.01%
Spam URLs	High	46,484	0.00%
Proxy avoidance	High	9,793,916	0.57%
Hacking	High	1,152,903	0.07%
Illegal or unethical	High	20,077	0.00%
File sharing and storage	Risk	10,439,421	0.61%
Peer-to-peer file sharing	Risk	4,375	0.00%
Freeware and software downloads	Risk	6,508,764	0.38%
Dynamic content	Risk	29,134	0.00%
Dynamic dns	Risk	13,091	0.00%
Newly observed domain	Risk	113,843	0.01%

Alert Type	Confidence	Frequency	Percentage (%)
Newly registered domain	Risk	12,765	0.00%
Web hosting	Risk	16,833,440	0.98%
Web-based applications	Risk	69,270,479	4.02%
Web-based email	Risk	8,617,181	0.05%
Remote access	Risk	39,418	0.00%
Information and computer security	Risk	12,885,680	0.75%
Information technology	Risk	1,469,367,790	85.21%
Instant messaging	Risk	14,705,510	0.85%
Content servers	Risk	102,393,504	5.94%
Unrated	Risk	1,979,952	0.11%

Employee Cyberloafing (Nominal Variable)

Employee cyberloafing was determined by the firewall categories visited. As shown in Table 5, the majority of cyberloafing visits were categorized as Streaming Media and Social Networking.

- Frequency: Visit count for each category was recorded.

- Percentage: Proportion of visits per category relative to total visits was calculated.

Table 5

Firewall Logs: Cyberloafing Category Frequency

Cyberloafing category	Visits (Count)	Percentage (%)
Social networking	105,660,228	26.78%
Web-based email	8,617,181	2.18%
Shopping	44,371,673	11.25%
Gambling	59,133	0.01%
Entertainment	3,516,019	0.89%
Streaming media and download	225,190,194	57.07%
Games	7,046,073	1.79%
Dating	53,695	0.01%
Pornography	42,968	0.01%
Nudity and risqué	21	0.00%

In this quantitative correlational study, several critical statistical assumptions underpinned the analysis of the relationship between network degradation, ransomware security attacks, and employee cyberloafing. Firstly, the assumption of linearity was essential, as the Pearson correlation coefficient, the primary analytical tool employed, required a linear relationship between variables (Das, 2023). This assumption ensured that the strength and direction of the relationships assessed were meaningful and accurately represented by a straight line. The assumption of normality in the distribution of variables was also considered, indicating that data collected on network usage, security incidents, and cyberloafing behaviors needed to approximate a normal distribution to validate correlation tests effectively. Tests such as the Shapiro-Wilk or Kolmogorov-Smirnov were reviewed to confirm normality, and potential transformations or non-parametric methods were considered if deviations were significant.

Assessment of Normality

To determine whether the continuous variables met the assumption of normality required for Pearson's correlation, a Shapiro-Wilk test was conducted. The results are presented in Table 6. The test indicated that all variables deviated significantly from a normal distribution ($p < .001$). However, due to the large sample size ($N = 30$), the central limit theorem suggests that the sampling distribution of the mean approximates normality, and Pearson's correlation is generally considered robust against such violations in large datasets.

Table 6

Shapiro-Wilk Test for Normality (N =30)

Variable	*W*	*df*	*p*
Bandwidth usage	0.686	30	$< .001$
Employee cyberloafing	0.717	30	$< .001$
Ransomware alerts	0.728	30	$< .001$

Note: All variables significantly deviated from normality; however, due to the large sample size, Pearson's correlation remains appropriate.

Another critical assumption addressed in this study was homoscedasticity, which implied that variances along the line of best fit remained constant. Homoscedasticity ensured that errors in prediction were uniform across all levels of independent variables, supporting the robustness and accuracy of correlation results (Baek et al., 2022). Graphical analyses, such as scatterplots and residual plots, were conducted to visually assess and confirm the stability of variance throughout the data range.

Additionally, independence of observations was an essential assumption, ensuring that each data point was independent of the others. This meant no data point systematically influenced or correlated with another, preserving the validity of inferential statistics (Salmond, 2023). Given the context of data collection from firewall logs and security alerts within K-12 public school districts, this assumption was carefully validated by ensuring data were collected and analyzed in distinct intervals without overlapping or repeated measurements influencing subsequent observations.

Lastly, the reliability and accuracy of instrumentation represented a crucial assumption, ensuring that the recorded data accurately reflected actual network usage and security incidents without systematic bias or error. By using standardized data collection processes inherent in NGFWs, I ensured consistency and replicability in measuring variables. The instrumentation's calibration, consistency checks, and adherence to industry standards further reinforced the study's methodological rigor, credibility, and reliability of the correlational findings (Sonntag & Loh, 2023).

Results of Correlation Analysis

For the inferential statistical analysis, I used Pearson's correlation coefficient (r) to examine relationships among the continuous study variables. Although the Shapiro-Wilk test indicated that the variables violated the assumption of normality ($p < .001$ for all variables), the sample size ($N = 30$) was considered sufficient for Pearson's r to remain robust to these deviations. An alpha level of .05 was used to determine statistical significance. As shown in Table 7, there was a significant positive correlation between network degradation (measured via bandwidth usage) and employee cyberloafing, r (30) = .69, $p < .001$, indicating a large effect size, suggesting that higher levels of cyberloafing are strongly associated with increased network degradation (as measured by bandwidth usage). The 95% confidence interval for this correlation ranged from .46 to .84, supporting the strength and reliability of the relationship.

Additionally, the correlation analysis revealed a significant positive correlation between ransomware security alerts and employee cyberloafing, r (30) = .72, $p < .001$, also indicating a large effect size under Cohen's guidelines, indicating a strong and meaningful relationship between increased cyberloafing activity and the frequency of ransomware-related alerts. The 95% confidence interval ranged from .52 to .86, further reinforcing the robustness of the finding. Together, these results support the alternative hypotheses, confirming statistically significant relationships between employee cyberloafing and both network degradation and ransomware security alerts.

For this analysis:

- Employee cyberloafing was measured as the daily count of visits to non-work-related website categories such as Streaming Media, Social Networking, and Games. This variable was treated as a continuous scale variable in SPSS.
- Ransomware alerts were measured as the daily frequency of firewall alert messages related to high-risk or suspicious activity categories (e.g., Phishing, Malicious Websites, Proxy Avoidance). This variable was also handled as a continuous scale variable in SPSS.
- Network degradation was represented by the average bandwidth usage (in Gbps) per day, which was likewise treated as a continuous variable.

Although the Shapiro-Wilk test for normality revealed that all three variables deviated from a normal distribution ($p < .001$), the use of Pearson's r remained appropriate given the robustness of the test with a moderate sample size ($N = 30$) and the approximately linear relationship observed in scatterplots. An alpha level of .05 was established as the threshold for determining statistical significance.

Power Analysis

Although a priori power analysis was not conducted before data collection, a post hoc review of the observed effect sizes provides justification for the adequacy of the sample size. The correlations between employee cyberloafing and the two key outcomes—network degradation (r = .69) and ransomware alerts (r = .72)—represent large effect sizes, as defined by Cohen (1988). According to guidelines provided by Faul et al. (2009) using G*Power 3.1, a sample size of 30 is sufficient to detect correlations of $r \geq .50$ with over 90% power at an alpha level of .05. Thus, the sample size used in this study was adequate to identify strong and meaningful relationships among the variables of interest.

Table 7

Pearson Correlation Coefficients Between Study Variables (N =30)

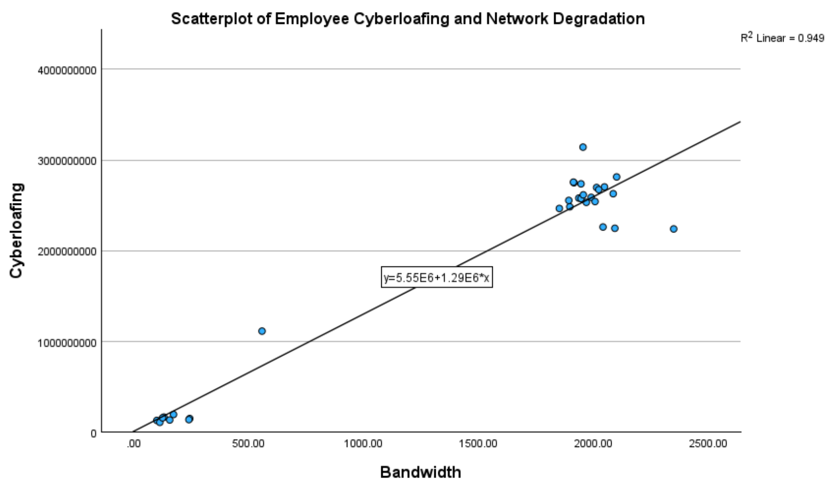
Variables	1	2
1. Network degradation	—	
2. Employee cyberloafing	.69***	—
	(.000)	
	[95% CI: .46, .84]	
3. Ransomware security attacks	—	.72***
		(.000)
		[95% CI: .52, .86]

Note: Values represent Pearson's *r*. p-values are in parentheses. Confidence intervals (CI) are 95%.***p* < .001.

A scatterplot illustrating the relationship between bandwidth usage and cyberloafing is presented in Figure 1. A positive linear trend supports the use of Pearson's correlation.

Figure 1

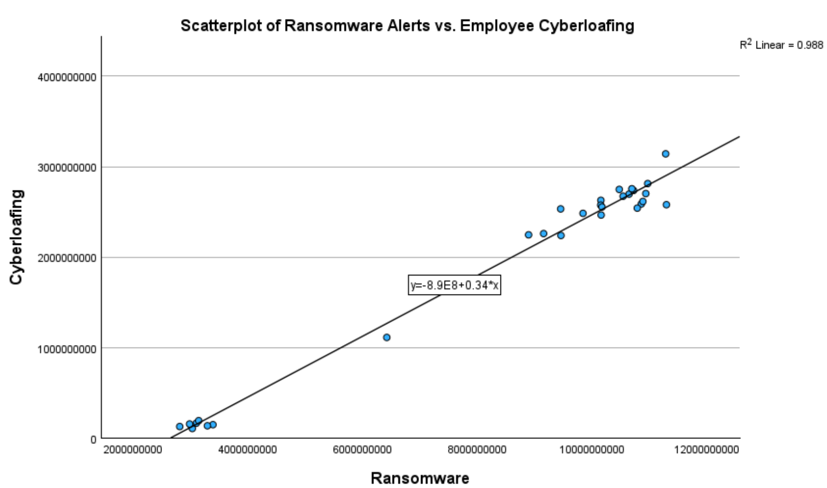
Scatterplot of Employee Cyberloafing and Network Degradation



Similarly, the relationship between ransomware alerts and cyberloafing is shown in Figure 2, which also reveals a strong linear association.

Figure 2

Scatterplot of Ransomware Alerts Versus Employee Cyberloafing



In summary, the research question addressed was:

RQ: What is the relationship between network degradation, ransomware security attacks, and employee cyberloafing?

The findings confirmed a significant positive correlation for both research questions, indicating that increased employee cyberloafing was associated with greater network degradation and heightened risk of ransomware security attacks. These results highlight the importance of monitoring and managing employee internet behaviors to enhance IT infrastructure security and performance. However, the results were interpreted within the study's defined scope and limitations, and no causal inferences were drawn from the observed correlations.

The findings also extended knowledge within the theoretical framework of activity theory, which emphasizes understanding the complex interactions between human behavior and technology in organizational contexts. Prior research, including Lim and Teo (2024) and Giordano and Mercado (2023), identified cyberloafing as a risk to information security and network performance, aligning with the results of this study. Similarly, Cremer et al. (2022) and Bhaskar (2022) underscored the importance of proactive cybersecurity policies and employee education, further supporting these findings. This study contributed to the literature by quantifying the relationships among the variables, offering empirical evidence to support strategies for IT professionals to mitigate risks associated with cyberloafing. At the same time, the results contrasted with findings by Liang et al. (2022), which suggested potential benefits of moderate cyberloafing for stress reduction and creativity. These contrasting results underscore the need for a balanced approach to policy formulation, acknowledging both the security risks and the possible organizational benefits of cyberloafing.

Interpreting the findings through the lens of activity theory provided deeper insights into the socio-technical dynamics at play. The theory posits that human activities are shaped by the tools used—in this case, digital technologies and internet access—and the cultural and organizational contexts in which they occur (Guo et al., 2024). Evidence from this study, showing that cyberloafing correlated with increased network degradation and ransomware risk, supports activity theory's assertion that misuse or under-regulated use of technological tools can disrupt the intended outcomes of an activity system. Within the school district network environment, the mediating tools (e.g., internet access) became sources of vulnerability when not aligned with the object (e.g., educational tasks).

The findings also affirmed activity theory's emphasis on the interconnectedness of individual actions and systemic outcomes (Rudolph et al., 2025). Cyberloafing, while seemingly minor at the individual level, when aggregated across the system, contributed to broader issues of infrastructure strain and security risks. These findings support system-level interventions—such as updating acceptable use policies and promoting cybersecurity education—as strategies to mediate behavior and align tool use with institutional objectives. Thus, the study validated the applicability of activity theory to this research context and demonstrated its utility in guiding IT governance and policy strategies that address both human and technological dimensions. Nonetheless, interpretations were limited to correlational data and the specific setting of K-12 public school district and should not be generalized beyond similar contexts without further research.

IT Contributions and Recommendations for Professional Practice

The findings of this study provided actionable insights for IT leaders and contributed to the research community by illustrating how employee internet behavior—specifically cyberloafing—affects network infrastructure and security posture. For IT professionals in educational institutions, the demonstrated correlations between cyberloafing, network degradation, and ransomware exposure highlight the need to reassess internet governance policies, firewall configurations, and end-user training protocols. As Lim and Teo (2024) and Giordano and Mercado (2023) emphasized, unmanaged digital behavior can compromise infrastructure integrity and expand the threat landscape. Therefore, IT leaders are encouraged to implement robust acceptable use policies that extend beyond access restrictions to include ongoing awareness programs that educate staff about security risks linked to nonwork-related browsing.

One practical recommendation is for IT departments to integrate firewall analytics with behavioral monitoring systems to identify patterns of bandwidth abuse or potential malicious access points in real time. Studies by Cremer et al. (2022) and Moustafa et al. (2021) support proactive monitoring as a preventive strategy that enhances IT operational readiness. Furthermore, integrating AI-based anomaly detection into next-generation firewall (NGFW) appliances can enable real-time alerts when user behavior deviates from baseline productivity patterns, containing threats before they escalate. These strategies align with current trends in cybersecurity and network management, where layered defense models and behavior-aware systems are increasingly standard (Bhaskar, 2022).

For the scholarly community, this study extended the application of activity theory in the IT domain by validating its usefulness in understanding behavioral influences on technology infrastructure performance and security. Quantitative evidence supported earlier conceptual work that identified human interaction with technology as a critical factor in system vulnerabilities (Dutta et al., 2021). Scholars are therefore encouraged to examine additional dimensions of cyberloafing across diverse sectors and apply alternative behavioral theories to expand understanding. Comparative studies across organizational types or geographic regions could yield broader insights and inform cross-sector cybersecurity frameworks.

Overall, this study reinforces the need for IT leaders to adopt a dual focus on technological controls and user behavior to strengthen system resilience. By combining technical safeguards with behavioral policy enforcement and ongoing training, educational institutions—and potentially other sectors—can mitigate the risks associated with employee cyberloafing and improve overall IT operational health.

Implications for Social Change

This study's findings hold significant implications for positive social change across educational institutions, IT departments, and broader societal contexts. By establishing a statistically significant relationship between cyberloafing, network degradation, and ransomware security attacks, the research supports interventions that promote responsible technology use. Such interventions can enhance digital literacy, create safer learning environments, and improve operational integrity.

For IT and organizational leaders, implementing preventive and educational strategies informed by this study can produce tangible improvements in employee awareness and behavior. When employees understand the consequences of their digital actions—such as how casual browsing may compromise security or disrupt network performance, they are more likely to adopt responsible online practices. Embedding cybersecurity education into institutional culture fosters a workforce that values digital ethics and prioritizes secure practices. Over time, these changes can result in fewer successful cyberattacks, reduced infrastructure strain, and increased system uptime, positively influencing institutional effectiveness and public trust.

At the community level, particularly within public education, strengthening the stability and security of digital infrastructure contributes to more equitable access to uninterrupted learning. Students, especially in underserved areas, benefit when digital resources remain consistently available and are not compromised by preventable issues stemming from employee misuse. These improvements support academic achievement, reduce digital inequality, and promote long-term empowerment through education.

For the scholarly community, the findings encourage further exploration of the behavioral dimensions of cybersecurity and network management. By advancing evidence-based recommendations for improving digital responsibility and linking them to educational outcomes, this study contributes to a growing body of research that views secure, equitable, and well-managed digital environments as essential foundations for social progress.

Overall, the study underscores the intersection of human behavior, technological infrastructure, and collective well-being. It reinforces the perspective that informed IT practices are not only operational necessities but also catalysts for meaningful and lasting social change.

Recommendations for Further Research

While this study offered critical insights into the correlations among cyberloafing, network degradation, and ransomware security threats, it also identified several limitations that should be addressed in future research to improve IT practice and strengthen scholarly understanding.

First, data collection was limited to K-12 public school districts with next-generation firewalls (NGFWs), potentially excluding districts lacking the infrastructure to participate. Future research should broaden the scope by including districts from other sectors (e.g., higher education, corporate IT) and by using alternative data-gathering technologies to accommodate institutions without NGFWs. This would enhance generalizability and expand the applicability of findings to a wider IT context.

Second, the use of nonprobability purposive sampling, while effective for targeting specific criteria, limits the ability to generalize findings across populations. Future studies should incorporate probability sampling methods to reduce sampling bias and improve external validity. For example, random sampling from a stratified pool of districts that vary in size, region, and demographics would provide more representative data.

Third, although this study followed a structured research design, it acknowledged the potential risk of unplanned post hoc analyses. Future researchers should mitigate this threat to internal validity by pre-registering their analysis plans and clearly distinguishing exploration from confirmatory analyses. This transparency would enhance the credibility and reproducibility of research outcomes.

Additionally, the findings were limited by the specific point in time when the data were collected. Longitudinal studies would better capture how patterns of cyberloafing and network degradation evolve in response to policy changes, technological upgrades, or cybersecurity awareness campaigns. Such approaches would help IT leaders assess the long-term effectiveness of interventions.

Further research should also incorporate qualitative or mixed methods approaches to explore the motivations underlying cyberloafing behavior. Understanding the human factors driving digital misuse could enable IT practitioners to design policies that are both effective and empathetic, balancing productivity with user satisfaction.

Finally, future research should investigate emerging technologies such as AI-based network monitoring, zero-trust architectures, and behavioral analytics for managing user behavior and identifying potential cyber threats. Examining how these tools can proactively detect and mitigate cyberloafing-related risks may transform reactive security models into predictive, adaptive systems that align with modern IT practices.

Addressing these limitations and research gaps will enable future scholars and IT professionals to build on this study's foundation, leading to stronger safeguards, more efficient network infrastructures, and more responsible use of digital resources across educational and organizational settings.

Conclusion

This quantitative correlational study examined the relationships among network degradation, ransomware security attacks, and employee cyberloafing within K–12 public school districts. The findings revealed statistically significant positive correlations between employee cyberloafing and both network degradation and ransomware security alerts. These results supported alternative hypotheses and reinforced the applicability of activity theory by illustrating the interconnectedness of individual behavior, technological tools, and institutional outcomes.

Using data collected from next-generation firewalls (NGFWs), the study enabled a comprehensive, real-world analysis of user behavior, bandwidth usage, and security events without compromising individual privacy. This approach provided a robust framework for evaluating how cyberloafing contributes to systemic vulnerabilities in educational IT infrastructure. The results underscore the importance of monitoring employee internet activity as a critical component of cybersecurity and network performance management.

From a professional practice perspective, the findings support the implementation of proactive, behavior-aware IT governance policies. These include refining acceptable use policies, embedding ongoing cybersecurity awareness training, and deploying analytics tools capable of identifying behavioral anomalies in real time. Such strategies are essential for protecting digital resources, maintaining secure learning environments, and ensuring equitable access to instructional technology.

While this study contributed meaningfully to the field, it was not without limitations. The reliance on nonprobability purposive sampling, the exclusion of districts without NGFW capabilities, and the constraints of cross-sectional data limited the generalizability of the findings. Future research should expand into other geographic regions, incorporate longitudinal methods, and integrate qualitative data to explore the underlying motivations for cyberloafing behaviors.

Ultimately, this study enhances scholarly understanding of socio-technical dynamics within educational institutions and provides practical insights for IT leaders and policymakers. The central conclusion is clear: employee cyberloafing is a measurable behavior that directly affects both network performance and cybersecurity risk. Addressing this challenge through informed, data-driven strategies will support safer, more efficient, and more equitable educational environments.

References

Aboramadan, M., Albashiti, B., Alharazin, H., & Zaidoune, S. (2019). Organizational culture, innovation, and performance: A study from a non-Western context. *Journal of Management Development, 39*(4), 437–451. https://doi.org/10.1108/jmd-06-2019-0253

Abu-Baker, N. N., AbuAlrub, S., Obeidat, R. F., & Assmairan, K. (2021). Evidence-based practice beliefs and implementations: a cross-sectional study among undergraduate nursing students. *BMC Nursing, 20*(1). https://doi.org/10.1186/s12912-020-00522-x

Abulela, M. A. A., & Harwell, M. (2020). Data analysis: Strengthening inferences in quantitative education studies conducted by novice researchers. *Educational Sciences: Theory & Practice, 20*(1), 59–78.

Aczel, B., Kovacs, M., van der Lippe, T., & Szaszi, B. (2021). Researchers working from home: Benefits and challenges. *PLOS ONE, 16*(3), e0249127. https://doi.org/10.1371/journal.pone.0249127

Alhasan, A. J., & Surantha, N. (2021). Evaluation of data center network security based on next-generation firewall. *International Journal of Advanced Computer Science and Applications, 12*(9). https://doi.org/10.14569/ijacsa.2021.0120958

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*. https://doi.org/10.3389/fcomp.2021.563060

Allen, M. (2017). *The SAGE Encyclopedia of Communication Research Methods*. Sage. https://doi.org/10.4135/9781483381411

Alqahtani, A., & Sheldon, F. T. (2022). A survey of crypto ransomware attack detection methodologies: An evolving outlook. *Sensors, 22*(5), 1837. https://doi.org/10.3390/s22051837

Amir, N., Jabeen, F., & Niaz, S. (2020). *A brief review of conditions, circumstances and applicability of sampling techniques in computer science domain*. 2020 IEEE 23rd International Multitopic Conference (INMIC). https://doi.org/10.1109/inmic50486.2020.9318209

Ampatzoglou, A., Bibi, S., Avgeriou, P., Verbeek, M., & Chatzigeorgiou, A. (2019). Identifying, categorizing and mitigating threats to validity in software engineering secondary studies. *Information and Software Technology, 106*, 201-230. https://doi.org/10.1016/j.infsof.2018.10.006

Andringa, S., & Godfroid, A. (2020). Sampling bias and the problem of generalizability in applied linguistics. *Annual Review of Applied Linguistics, 40*, 134–142. https://doi.org/10.1017/s0267190520000033

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J. M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making, 20*(1). https://doi.org/10.1186/s12911-020-01161-7

Aslan, O., & Yilmaz, A. A. (2021). A new malware classification framework based on deep learning algorithms. *IEEE Access, 9*. https://doi.org/10.1109/access.2021.3089586

Audulv, Å., Hall, E. O. C., Kneck, Å., Westergren, T., Fegran, L., Pedersen, M. K., Aagaard, H., Dam, K. L., & Ludvigsen, M. S. (2022). Qualitative longitudinal research in health research: a method study. *BMC Medical Research Methodology, 22*(1), Article 255. https://doi.org/10.1186/s12874-022-01732-4

Baba, A. M., Midi, H., Adam, M. B., & Abd Rahman, N. H. A. (2021). Detection of influential observations in spatial regression model based on outliers and bad leverage classification. *Symmetry, 13*(11), 2030. https://doi.org/10.3390/sym13112030

Babbie, E. R. (2016). *The practice of social research* (14th ed.). *Cengage Learning*

Baek, E. J., Jung, H. U., Chung, J. Y., Jung, H. I., Kwon, S. Y., Lim, J. E., Kim, H. K., Kang, J. O., & Oh, B. (2022). The effect of heteroscedasticity on the prediction efficiency of genome-wide polygenic score for body mass index. *Frontiers in Genetics*, *13*. https://doi.org/10.3389/fgene.2022.1025568

Bailey, C. M., Newton, J. M., & Hall, H. G. (2019). Telephone triage in midwifery practice: A cross-sectional survey. *International Journal of Nursing Studies, 91*, 110-118. https://doi.org/10.1016/j.ijnurstu.2018.11.009

Bakdash, J. Z., & Marusich, L. R. (2017). Repeated measures correlation. *Frontiers in Psychology, 8*. https://doi.org/10.3389/fpsyg.2017.00456

Bakker, E. A., Hartman, Y. A. W., Hopman, M. T. E., Hopkins, N. D., Graves, L. E. F., Dunstan, D. W., Healy, G. N., Eijsvogels, T. M. H., & Thijssen, D. H. J. (2020). Validity and reliability of subjective methods to assess sedentary behaviour in adults: a systematic review and meta-analysis. *International Journal of Behavioral Nutrition and Physical Activity, 17*(1) Article 75. https://doi.org/10.1186/s12966-020-00972-1

Baldwin, J. R., Pingault, J. B., Schoeler, T., Sallis, H. M., & Munafò, M. R. (2022). Protecting against researcher bias in secondary data analysis: Challenges and potential solutions. *European Journal of Epidemiology, 37*(1), 1–10. https://doi.org/10.1007/s10654-021-00839-0

Bansal, U. (2021, May 21/23). *A review on ransomware attack*. 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), Jalandhar, India. https://doi.org/10.1109/icsccc51823.2021.9478148

Barchard, K. A., Freeman, A. J., Ochoa, E., & Stephens, A. K. (2020). Comparing the accuracy and speed of fmy data-checking methods. *Behavior Research Methods, 52*(1), 97-115. https://doi.org/10.3758/s13428-019-01207-3

Barroga, E., & Matanguihan, G. J. (2022). A practical guide to writing quantitative and qualitative research questions and hypotheses in scholarly articles. *Journal of Korean Medical Science*, *37*(16). https://doi.org/10.3346/jkms.2022.37.e121

Basu, I., & Maji, S. (2022). Multicollinearity correction and combined feature effect in shapley values. *Lecture Notes in Computer Science*, 79-90. https://doi.org/10.1007/978-3-030-97546-3_7

Bates, M. A., & Glennerster, R. (2017). The generalizability puzzle. *Stanford Social Innovation Review, 15*(3), 50–54. https://doi.org/10.48558/EYY5-3S89

Batiibwe, M. S. K. (2019). Using cultural historical activity theory to understand how emerging technologies can mediate teaching and learning in a mathematics classroom: A review of literature. *Research and Practice in Technology Enhanced Learning, 14*(1), Article 6. https://doi.org/10.1186/s41039-019-0110-7

Bauer, G. R., & Scheim, A. I. (2019). Methods for analytic intercategorical intersectionality in quantitative research: Discrimination as a mediator of health inequalities. *Social Science & Medicine, 226*, 236–245. https://doi.org/10.1016/j.socscimed.2018.12.015

Beer, P., & Mulder, R. H. (2020). The effects of technological developments on work and their implications for continuous vocational education and training: A systematic review. *Frontiers in Psychology, 11,* Article 918. https://doi.org/10.3389/fpsyg.2020.00918

Bello, I., Chiroma, H., Abdullahi, U. A., Gital, A. Y. U., Jauro, F., Khan, A., Okesola, J. O., & Abdulhamid, S. I. M. (2021). Detecting ransomware attacks using intelligent algorithms: Recent developments and next directions from deep learning and big data perspectives. *Journal of Ambient Intelligence and Humanized Computing, 12*(9), 8699–8717. https://doi.org/10.1007/s12652-020-02630-7

Bennett, R. J., & Robinson, S. L. (2000). Development of a measure of workplace deviance. *Journal of Applied Psychology, 85*(3), 349–360. https://doi.org/10.1037/0021-9010.85.3.349

Bhandari, P. (2022b). Correlational research: When and how to use. *Scribbr.* https://www.scribbr.com/methodology/correlational-research/

Bhandari, P. (2022a). A note on survey research methods levels of measurement: Foundational basis for quantitative analysis of survey data. *Dhaulagiri Journal of Sociology and Anthropology, 16*(1), 122–126. https://doi.org/10.3126/dsaj.v16i01.50982

Bhandari, P. (2023a). Descriptive statistics: Definitions, types, examples. *Scribbr.* https://www.scribbr.com/statistics/descriptive-statistics/

Bhaskar, R. (2022). Better cybersecurity awareness through research. *ISACA Journal, 3.* https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/better-cybersecurity-awareness-through-research

Blanca, M. J., Alarcón, R., Arnau, J., Bono, R., & Bendayan, R. (2017). Effect of variance ratio on ANOVA robustness: Might 1.5 be the limit? *Behavior Research Methods, 50*(3), 937–962. https://doi.org/10.3758/s13428-017-0918-2

Blanca, M. J., Alarcón, R., & Bono, R. (2018). Current practices in data analysis procedures in psychology: What has changed? *Frontiers in Psychology, 9,* Article 2558. https://doi.org/10.3389/fpsyg.2018.02558

Bloch, M., Lave, J., & Wenger, E. (1994). Situated learning: Legitimate peripheral participation. *Man, 29*(2), 487–488. https://doi.org/10.2307/2804509

Bloomfield, J., & Fisher, M. (2019). Quantitative research design. *Journal of the Australasian Rehabilitation Nurses' Association, 22*(2), 27–30. https://doi.org/10.33235/jarna.22.2.27-30

Boise State University. (n.d.). *Guidelines on pilot studies.* https://www.boisestate.edu/research-compliance/irb/guidance/pilot-studies/

Boston University. (2013). *Introduction to correlation and regression analysis.* https://sphweb.bumc.bu.edu/otlt/MPH-Modules/BS/BS704_Multivariable/BS704_Multivariable5.html

Bozkus, K. (2024). Organizational culture change and technology: Navigating the digital transformation. *Business, Management and Economics.* https://doi.org/10.5772/intechopen.112903

Brinkman, B., Flick, C., Gotterbarn, D., Miller, K., Vazansky, K., & Wolf, M. J. (2017). Listening to professional voices: Draft 2 of the ACM code of ethics and professional conduct. *Communications of the ACM, 60*(5), 105–111. https://doi.org/10.1145/3072528

Burchett, H. E. D., Kneale, D., Blanchard, L., & Thomas, J. (2020). When assessing generalisability, focusing on differences in population or setting alone is insufficient. *Trials, 21,* Article 645. https://doi.org/10.1186/s13063-020-4178-6

Busenbark, J. R., Yoon, H. E., Gamache, D. L., & Withers, M. C. (2022). Omitted variable bias: Examining management research with the impact threshold of a confounding variable (ITCV). *Journal of Management, 48*(1), 17–48. https://doi.org/10.1177/01492063211006458

Busetto, L., Wick, W., & Gumbinger, C. (2020). How to use and assess qualitative research methods. *Neurological Research and Practice, 2,* Article 14. https://doi.org/10.1186/s42466-020-00059-z

Cahit, K. (2015). Internal validity: A must in research designs. *Educational Research and Reviews, 10*(2), 111–118. https://doi.org/10.5897/ERR2014.1835

Centers for Disease Control and Prevention. (2018). *Data collection methods for evaluation: Document review.* U.S. Department of Health & Human Services. https://www.cdc.gov/healthyyouth/evaluation/pdf/brief18.pdf

Cessie, S., Nagelkerke, N., Rosendaal, F., van Stralen, K., Pomp, E., & van Houwelingen, H. (2008). Combining matched and unmatched control groups in case-control studies. *American Journal of Epidemiology, 168*(10), 1204–1210. https://doi.org/10.1093/aje/kwn236

Chen, T., & Gopalan, A. (2021). Optimized online lecture for narrow-bandwidth network. In *Proceedings of the 2021 10th International Conference on Educational and Information Technology (ICEIT)* (pp. xxx–xxx). IEEE. https://doi.org/10.1109/ICEIT51700.2021.9375618

Cheng, J. (2022). The social and psychological consequences of ransomware attacks. *ISACA Journal.* https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/the-social-and-psychological-consequences-of-ransomware-attacks

Cichoń, M. (2020). Reporting statistical methods and outcomes of statistical analyses in research articles. *Pharmacological Reports, 72*(3), 481–485. https://doi.org/10.1007/s43440-020-00110-5

Cisco Systems. (2021). *Cisco web usage control filtering categories data sheet.* Cisco. https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/datasheet_C78-718442.html

Clifton-Sprigg, J., James, J., & Vujić, S. (2020). Freedom of information (FOI) as a data collection tool for social scientists. *PLOS ONE, 15*(2), e0228392. https://doi.org/10.1371/journal.pone.0228392

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum Associates. https://doi.org/10.4324/9780203771587

Cooksey, R. W. (2020). Descriptive statistics for summarising data. In *Illustrating statistical procedures: Finding meaning in quantitative data* (pp. 61–139). Springer. https://doi.org/10.1007/978-981-15-2537-7_5

Cooper, C., Booth, A., Varley-Campbell, J., Britten, N., & Garside, R. (2018). Defining the process to literature searching in systematic reviews: A literature review of guidance and supporting studies. *BMC Medical Research Methodology, 18*(1), Article 85. https://doi.org/10.1186/s12874-018-0545-3

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance – Issues and Practice, 47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Dalglish, S. L., Khalid, H., & McMahon, S. A. (2020). Document analysis in health policy research: The READ approach. *Health Policy and Planning, 35*(10), 1424–1431. https://doi.org/10.1093/heapol/czaa064

Das, J. (2023). Pearson's correlation in predictive analytics and machine learning: Applications and limitations. *International Journal for Multidisciplinary Research, 5*(3), Article 48969. https://doi.org/10.36948/ijfmr.2023.v05i03.48969

Dearing, J. W., & Cox, J. G. (2018). Diffusion of innovations theory, principles, and practice. *Health Affairs, 37*(2), 183–190. https://doi.org/10.1377/hlthaff.2017.1104

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness. In *Proceedings of the 15th International Academic MindTrek*

Conference: Envisioning Future Media Environments (pp. xxx–xxx). ACM. https://doi.org/10.1145/2181037.2181040

De Vries, J. H., Spengler, M., Frintrup, A., & Mussel, P. (2021). Personality development in emerging adulthood: How the perception of life events and mindset affect personality trait change. *Frontiers in Psychology, 12,* Article 671421. https://doi.org/10.3389/fpsyg.2021.671421

Dhamija, P., Chiarini, A., & Shapla, S. (2023). Technology and leadership styles: A review of trends between 2003 and 2021. *The TQM Journal, 35*(1), 210–233. https://doi.org/10.1108/tqm-03-2021-0087

Duppa, G. I. P., & Surantha, N. (2019). Evaluation of network security based on next-generation intrusion prevention system. *TELKOMNIKA (Telecommunication Computing Electronics and Control), 17*(1), 39–47. https://doi.org/10.12928/telkomnika.v17i1.9191

Dutta, A., Steiner, E., Proulx, J., Berisha, V., Bliss, D. W., Poole, S., & Corman, S. (2021). Analyzing the relationship between productivity and human communication in an organizational setting. *PLOS ONE, 16*(7), e0250301. https://doi.org/10.1371/journal.pone.0250301

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2019). Re-examining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model. *Information Systems Frontiers, 21*(3), 719–734. https://doi.org/10.1007/s10796-017-9774-y

Easa, N. F., & Orra, H. E. (2021). HRM practices and innovation: An empirical systematic review. *International Journal of Disruptive Innovation in Government, 1*(1), 15–35. https://doi.org/10.1108/ijdig-11-2019-0005

Eberhard, K. (2021). The effects of visualization on judgment and decision-making: A systematic literature review. *Management Review Quarterly, 73*(1), 167–214. https://doi.org/10.1007/s11301-021-00235-8

Edwards, J. R. (2020). The peaceful coexistence of ethics and quantitative research. *Journal of Business Ethics, 167*(1), 31–40. https://doi.org/10.1007/s10551-019-04197-6

Egbert, J., & Plonsky, L. (2020). Bootstrapping techniques. In *A practical handbook of corpus linguistics* (pp. 593–610). Springer. https://doi.org/10.1007/978-3-030-46216-1_24

Einy, S., Oz, C., & Navaei, Y. D. (2021). The anomaly and signature-based IDS for network security using hybrid inference systems. *Mathematical Problems in Engineering, 2021,* Article 6639714. https://doi.org/10.1155/2021/6639714

Eisend, M., & Kuss, A. (2019). Obtaining data for theory testing: Operationalization, measurement, and data collection. In *Research methodology in marketing* (pp. 123–150). Springer. https://doi.org/10.1007/978-3-030-10794-9_6

Eisend, M., van Reijmersdal, E. A., Boerman, S. C., & Tarrahi, F. (2020). A meta-analysis of the effects of disclosing sponsored content. *Journal of Advertising, 49*(3), 344–366. https://doi.org/10.1080/00913367.2020.1765909

Engeström, Y. (2015). *Learning by expanding: An activity-theoretical approach to developmental research*. Cambridge University Press. https://doi.org/10.1017/CBO9781139814744

Erceg-Hurn, D. M., & Mirosevich, V. M. (2008). Modern robust statistical methods: An easy way to maximize the accuracy and power of your research. *American Psychologist, 63*(7), 591–601. https://doi.org/10.1037/0003-066X.63.7.591

Fancourt, D., Garnett, C., Spiro, N., West, R., & Müllensiefen, D. (2019). How do artistic creative activities regulate my emotions? Validation of the Emotion Regulation Strategies for Artistic Creative Activities Scale (ERS-ACA). *PLOS ONE, 14*(2), e0211362. https://doi.org/10.1371/journal.pone.0211362

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods, 41*(4), 1149–1160. https://doi.org/10.3758/BRM.41.4.1149

Favaretto, M., De Clercq, E., Gaab, J., & Elger, B. S. (2020). First do no harm: An exploration of researchers' ethics of conduct in big data behavioral studies. *PLOS ONE, 15*(11), e0241865. https://doi.org/10.1371/journal.pone.0241865

Feng, C., Li, L., & Sadeghpour, A. (2020). A comparison of residual diagnosis tools for diagnosing regression models for count data. *BMC Medical Research Methodology, 20*(1), 288. https://doi.org/10.1186/s12874-020-01055-2

Fernandez, M., Mowatt, R. A., Shinew, K. J., Stodolska, M., & Stewart, W. (2021). Going the extra mile: Building trust and collaborative relationships with study participants. *Leisure Sciences, 43*(3–4), 418–435. https://doi.org/10.1080/01490400.2020.1830901

Fernando, J. (2023). The correlation coefficient: What it is, what it tells investors. *Investopedia.* https://www.investopedia.com/terms/c/correlationcoefficient.asp

Field, A. P. (2019). *Discovering statistics using IBM SPSS statistics* (5th ed.). Sage Publications.

Flora, D. B., LaBrish, C., & Chalmers, R. P. (2012). Old and new ideas for data screening and assumption testing for exploratory and confirmatory factor analysis. *Frontiers in Psychology, 3,* 55. https://doi.org/10.3389/fpsyg.2012.00055

Foutsitzi, S., & Caridakis, G. (2019). ICT in education: Benefits, challenges and new directions. In *Proceedings of the 2019 10th International Conference on Information, Intelligence, Systems and Applications (IISA)* (pp. 1–4). IEEE. https://doi.org/10.1109/iisa.2019.8900666

Freedman, M. (2023). Spying on your employees? Better understand the law first. *Business News Daily.* https://www.businessnewsdaily.com/6685-employee-monitoring-privacy.html

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

Gao, J. (2020). P-values – a chronic conundrum. *BMC Medical Research Methodology, 20*(1), 167. https://doi.org/10.1186/s12874-020-01051-6

Garofalo, S., Giovagnoli, S., Orsoni, M., Starita, F., & Benassi, M. (2022). Interaction effect: Are you doing the right thing? *PLOS ONE, 17*(7), e0271668. https://doi.org/10.1371/journal.pone.0271668

Gegan, R., Mao, C., Ghosal, D., Bishop, M., & Peisert, S. (2020). Anomaly detection for Science DMZs using system performance data. In *Proceedings of the 2020 International Conference on Computing, Networking and Communications (ICNC)* (pp. 695–699). IEEE. https://doi.org/10.1109/icnc47757.2020.9049695

Giacalone, M., Panarello, D., & Mattera, R. (2017). Multicollinearity in regression: An efficiency comparison between LP-norm and least squares estimators. *Quality & Quantity, 52*(4), 1831–1859. https://doi.org/10.1007/s11135-017-0571-y

Gianfrancesco, M. A., & Goldstein, N. D. (2021). A narrative review on the validity of electronic health record-based research in epidemiology. *BMC Medical Research Methodology, 21*(1), 147. https://doi.org/10.1186/s12874-021-01416-5

Giordano, C., & Mercado, B. K. (2023). Cyberloafing: Investigating the importance and implications of new and known predictors. *Collabra: Psychology, 9*(1), Article 57391. https://doi.org/10.1525/collabra.57391

Goel, I. (2021). Cybersecurity: A shared responsibility. *ISACA Journal.* https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/the-social-and-psychological-consequences-of-ransomware-attacks

Granić, A. (2022). Educational technology adoption: A systematic review. *Education and Information Technologies, 27*(7), 9725–9744. https://doi.org/10.1007/s10639-022-10951-7

Grant, C., & Osanloo, A. (2014). Understanding, selecting, and integrating a theoretical framework in dissertation research: Creating the blueprint for your "house." *Administrative Issues Journal: Education, Practice, and Research, 4*(2), 12–26. https://doi.org/10.5929/2014.4.2.9

Grant, S. C. (2021). Informed consent—I can and should do better. *JAMA Network Open, 4*(4), e2110848. https://doi.org/10.1001/jamanetworkopen.2021.10848

Gravetter, F., & Wallnau, L. (2017). *Statistics for the behavioral sciences* (10th ed.). Cengage Learning.

Greenland, S., Senn, S. J., Rothman, K. J., Carlin, J. B., Poole, C., Goodman, S. N., & Altman, D. G. (2016). Statistical tests, p values, confidence intervals, and power: A guide to misinterpretations. *European Journal of Epidemiology, 31*(4), 337–350. https://doi.org/10.1007/s10654-016-0149-3

Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: Redefining human-centric cyber security. *Frontiers in Big Data, 4,* 583723. https://doi.org/10.3389/fdata.2021.583723

Guetterman, T. C. (2019). Basics of statistics for primary care research. *Family Medicine and Community Health, 7*(2), e000067. https://doi.org/10.1136/fmch-2018-000067

Guo, R., Poquet, O., & Dawson, S. (2024). Exploring sociocultural influences on generative AI engagement in higher education: An activity theory perspective. *Smart Learning Environments, 11*(1), Article 24. https://doi.org/10.1186/s40561-024-00352-3

Hadlington, L., & Parsons, K. (2017). Can cyberloafing and internet addiction affect organizational information security? *Cyberpsychology, Behavior, and Social Networking, 20*(9), 567–571. https://doi.org/10.1089/cyber.2017.0239

Hair, J., Babin, B., Anderson, R., & Black, W. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning.

Hallström, J. (2022). Embodying the past, designing the future: Technological determinism reconsidered in technology education. *International Journal of Technology and Design Education, 32*(1), 17–31. https://doi.org/10.1007/s10798-020-09600-2

Hanel, P. H. P., Maio, G. R., Soares, A. K. S., Vione, K. C., de Holanda Coelho, G. L., Gouveia, V. V., Patil, A. C., Kamble, S. V., & Manstead, A. S. R. (2018). Cross-cultural differences and similarities in human value instantiation. *Frontiers in Psychology, 9,* 849. https://doi.org/10.3389/fpsyg.2018.00849

Haneuse, S., Arterburn, D., & Daniels, M. J. (2021). Assessing missing data assumptions in EHR-based studies: A complex and underappreciated task. *JAMA Network Open, 4*(2), e210184. https://doi.org/10.1001/jamanetworkopen.2021.0184

Harris, S., & Houser, S. (2018). Double trouble—Using health informatics to tackle duplicate medical record issues. *Journal of AHIMA, 89*(8), 20–23. https://library.ahima.org/doc?oid=302567

Hayat, M. J., Powell, A., Johnson, T., & Cadwell, B. L. (2017). Statistical methods used in the public health literature and implications for training of public health professionals. *PLOS ONE, 12*(6), e0179032. https://doi.org/10.1371/journal.pone.0179032

Hayati Rezvan, P., Lee, K. J., & Simpson, J. A. (2015). The rise of multiple imputations: A review of the reporting and implementation of the method in medical research. *BMC Medical Research Methodology, 15*(1), 30. https://doi.org/10.1186/s12874-015-0022-1

Haynes, W. (2013). Bonferroni correction. In W. Dubitzky, O. Wolkenhauer, K.-H. Cho, & H. Yokota (Eds.), *Encyclopedia of systems biology* (pp. 154–154). Springer. https://doi.org/10.1007/978-1-4419-9863-7_1213

Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). Cybersecurity practices for social media users: A systematic literature review. *Journal of Cybersecurity and Privacy, 2*(1), 1–18. https://doi.org/10.3390/jcp2010001

Huebner, M., Vach, W., Cessie, S., Schmidt, C. O., & Lusa, L. (2020). Hidden analyses: A review of reporting practice and recommendations for more transparent reporting of initial data analyses. *BMC Medical Research Methodology, 20*(1), 125. https://doi.org/10.1186/s12874-020-00942-y

Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: Views from a predictive model and human responses. *Crime Science, 8*(1), 2. https://doi.org/10.1186/s40163-019-0097-9

Humayun, M., Jhanjhi, N., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal, 22*(1), 105–117. https://doi.org/10.1016/j.eij.2020.05.003

Hung, M., Bounsanga, J., & Voss, M. W. (2017). Interpretation of correlations in clinical research. *Postgraduate Medicine, 129*(8), 902–906. https://doi.org/10.1080/00325481.2017.1383820

Hussain, M. I., He, J., Zhu, N., Ali Zardari, Z., Razque, F., Hussain, S., & Pathan, M. S. (2021). An archetype for mitigating the security threats in multi-cloud environment by implementing tree-based next-generation firewalls. *Journal of Intelligent & Fuzzy Systems, 41*(1), 125–136. https://doi.org/10.3233/jifs-200835

Ibrahim, A., Thiruvady, D., Schneider, J. G., & Abdelrazek, M. (2020). The challenges of leveraging threat intelligence to stop data breaches. *Frontiers in Computer Science, 2,* 36. https://doi.org/10.3389/fcomp.2020.00036

Ishaq, E., Bashir, S., Zakariya, R., & Sarwar, A. (2021). Technology acceptance behavior and feedback loop: Exploring reverse causality of TAM in post-COVID-19 scenario. *Frontiers in Psychology, 12,* 682507. https://doi.org/10.3389/fpsyg.2021.682507

Jack, L., Jr. (2021). Advancing health equity, eliminating health disparities, and improving population health. *Preventing Chronic Disease, 18,* E95. https://doi.org/10.5888/pcd18.210264

Jacquier, E., Laurent-Puig, P., Badoual, C., Burgun, A., & Mamzer, M. F. (2021). Facing new challenges to informed consent processes in the context of translational research: The case in CARPEM consortium. *BMC Medical Ethics, 22*(1), 117. https://doi.org/10.1186/s12910-021-00592-9

Jaggernauth, E., & Rocke, S. (2021). Effectiveness of paired next generation firewalls in securing industrial automation and control systems: A case study. *West Indian Journal of Engineering, 44*(1), 4–10. https://doi.org/10.47412/marq2173

Jakobsen, J. C., Gluud, C., Wetterslev, J., & Winkel, P. (2017). When and how should multiple imputation be used for handling missing data in randomised clinical trials: A practical guide with flowcharts. *BMC Medical Research Methodology, 17*(1), 162. https://doi.org/10.1186/s12874-017-0442-1

Jammalamadaka, S. R., Taufer, E., & Terdik, G. H. (2021). On multivariate skewness and kurtosis. *Sankhya A, 83*(2), 607–644. https://doi.org/10.1007/s13171-020-00211-6

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: Towards an effective anti-phishing training—A comparative literature review. *Human-Centric Computing and Information Sciences, 10*(1), 33. https://doi.org/10.1186/s13673-020-00237-7

Jan, J., Alshare, K. A., & Lane, P. L. (2022). Hofstede's cultural dimensions in technology acceptance models: A meta-analysis. *Universal Access in the Information Society, 22*(2), 249–270. https://doi.org/10.1007/s10209-022-00930-7

Janse, R. J., Hoekstra, T., Jager, K. J., Zoccali, C., Ripepi, G., Dekker, F. W., & van Diepen, M. (2021). Conducting correlation analysis: Important limitations and pitfalls. *Clinical Kidney Journal, 14*(11), 2332–2337. https://doi.org/10.1093/ckj/sfab085

Johnson, J. L., Adkins, D., & Chauvin, S. (2020). A review of the quality indicators of rigor in qualitative research. *American Journal of Pharmaceutical Education, 84*(1), 7120. https://doi.org/10.5688/ajpe7120

Jordan, C. Y. (2018). Population sampling affects pseudoreplication. *PLOS Biology, 16*(10), e2007054. https://doi.org/10.1371/journal.pbio.2007054

Kaliyadan, F., & Kulkarni, V. (2019). Types of variables, descriptive statistics, and sample size. *Indian Dermatology Online Journal, 10*(1), 82–86. https://doi.org/10.4103/idoj.idoj_468_18

Kaptelinin, V., & Nardi, B. (2018). Activity theory as a framework for human-technology interaction research. *Mind, Culture, and Activity, 25*(1), 3–5. https://doi.org/10.1080/10749039.2017.1393089

Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. *Information & Computer Security, 30*(3), 382–401. https://doi.org/10.1108/ICS-06-2021-0073

Kennison, S. M., & Chan-Tin, E. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. *Frontiers in Psychology, 11,* 546546. https://doi.org/10.3389/fpsyg.2020.546546

Keserlioglu, K., Kilicoglu, H., & ter Riet, G. (2019). Impact of peer review on discussion of study limitations and strength of claims in randomized trial reports: A before and after study. *Research Integrity and Peer Review, 4,* 9. https://doi.org/10.1186/s41073-019-0078-2

Kim, H. Y. (2017). Statistical notes for clinical researchers: Chi-squared test and Fisher's exact test. *Restorative Dentistry & Endodontics, 42*(2), 152–155. https://doi.org/10.5395/rde.2017.42.2.152

Kim, T. K. (2017). Understanding one-way ANOVA using conceptual figures. *Korean Journal of Anesthesiology, 70*(1), 22–26. https://doi.org/10.4097/kjae.2017.70.1.22

Kline, P. (2013). *Handbook of psychological testing* (2nd ed.). Routledge. https://doi.org/10.4324/9781315812274

Knief, U., & Forstmeier, W. (2021). Violating the normality assumption may be the lesser of two evils. *Behavior Research Methods, 53*(6), 2576–2590. https://doi.org/10.3758/s13428-021-01587-5

Konikiewicz, W., & Markowski, M. (2017). Analysis of performance and efficiency of hardware and software firewalls. *Journal of Applied Computer Science Methods, 9*(1), 49–63. https://doi.org/10.1515/jacsm-2017-0003

Koomson, J. (2021). Rise of ransomware attacks on the education sector during the COVID-19 pandemic. *ISACA Journal, 5.* Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/rise-of-ransomware-attacks-on-the-education-sector-during-the-covid-19-pandemic

Kulas, J., Roji, R. G. P. P., & Smith, A. (2021). *IBM SPSS essentials: Managing and analyzing social sciences data* (2nd ed.). Wiley. https://doi.org/10.1002/9781119417453

Kulkarni, R. U., Wang, C. L., & Bertozzi, C. R. (2022). Analyzing nested experimental designs—A user-friendly resampling method to determine experimental significance. *PLOS Computational Biology, 18*(5), e1010061. https://doi.org/10.1371/journal.pcbi.1010061

Kwak, S. K., & Kim, J. H. (2017). Statistical data preparation: Management of missing values and outliers. *Korean Journal of Anesthesiology, 70*(4), 407–411. https://doi.org/10.4097/kjae.2017.70.4.407

Lakens, D. (2013). Calculating and reporting effect sizes to facilitate cumulative science: A practical primer for t-tests and ANOVAs. *Frontiers in Psychology, 4,* 863. https://doi.org/10.3389/fpsyg.2013.00863

Langner, R., Scharnowski, F., Ionta, S., Salmon, C. E. G., Piper, B. J., & Pamplona, G. S. P. (2023). Evaluation of the reliability and validity of computerized tests of attention. *PLOS ONE, 18*(1), e0281196. https://doi.org/10.1371/journal.pone.0281196

Lau, J. D., Kleiber, D., Lawless, S., & Cohen, P. J. (2021). Gender equality in climate policy and practice hindered by assumptions. *Nature Climate Change, 11*(3), 186–192. https://doi.org/10.1038/s41558-021-00999-7

Lee, T., & Shi, D. (2021). A comparison of full information maximum likelihood and multiple imputation in structural equation modeling with missing data. *Psychological Methods, 26*(4), 466–485. https://doi.org/10.1037/met0000381

Lenger, A. (2019). The rejection of qualitative research methods in economics. *Journal of Economic Issues, 53*(4), 946–965. https://doi.org/10.1080/00213624.2019.1657748

Leont'ev, A. N. (1978). *Activity, consciousness, and personality.* Prentice-Hall.

Le-Rademacher, J., & Wang, X. (2021). Time-to-event data: An overview and analysis considerations. *Journal of Thoracic Oncology, 16*(7), 1067–1074. https://doi.org/10.1016/j.jtho.2021.04.004

Lester, J. N., Cho, Y., & Lochmiller, C. R. (2020). Learning to do qualitative data analysis: A starting point. *Human Resource Development Review, 19*(1), 94–106. https://doi.org/10.1177/1534484320903890

Levin, D. (2021). *The state of K-12 cybersecurity: 2020 year in review.* EdTech Strategies/K-12 Cybersecurity Resource Center and the K12 Security Information Exchange. Retrieved from https://k12cybersecure.com/year-in-review/

Li, J., Wu, N., & Xiong, S. (2021). Sustainable innovation in the context of organizational cultural diversity: The role of cultural intelligence and knowledge sharing. *PLOS ONE, 16*(5), e0250878. https://doi.org/10.1371/journal.pone.0250878

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior.

International Journal of Information Management, 45, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, Q. (2020). Overview of data visualization. In *Embodying data* (pp. 17–47). Springer. https://doi.org/10.1007/978-981-15-5069-0_2

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *Energy Reports, 7,* 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Liang, X., Guo, G., Gong, Q., Li, S., & Li, Z. (2022). Cyberloafing to escape from the “devil”: Investigating the impact of abusive supervision from the third-party perspective. *Frontiers in Psychology, 12,* 722063. https://doi.org/10.3389/fpsyg.2021.722063

Lim, V. K. G. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior, 23*(5), 675–694. https://doi.org/10.1002/job.161

Lim, V. K. G., & Teo, T. S. H. (2024). Cyberloafing: A review and research agenda. *Applied Psychology, 73*(1), 441–484. https://doi.org/10.1111/apps.12452

Lin, W. C., & Tsai, C. F. (2020). Missing value imputation: A review and analysis of the literature (2006–2017). *Artificial Intelligence Review, 53*(2), 1487–1509. https://doi.org/10.1007/s10462-019-09709-4

Liu, L., Jones, B. F., Uzzi, B., & Wang, D. (2023). Data, measurement and empirical methods in the science of science. *Nature Human Behaviour, 7*(7), 1046–1058. https://doi.org/10.1038/s41562-023-01562-4

Loffing, F. (2022). Raw data visualization for common factorial designs using SPSS: A syntax collection and tutorial. *Frontiers in Psychology, 13,* 808469. https://doi.org/10.3389/fpsyg.2022.808469

Lopez, M. J., & Gutman, R. (2017). Estimation of causal effects with multiple treatments: A review and new ideas. *Statistical Science, 32*(3), 322–339. https://doi.org/10.1214/17-sts612

Lunde, L. K., Fløvik, L., Christensen, J. O., Johannessen, H. A., Finne, L. B., Jørgensen, I. L., Mohr, B., & Vleeshouwers, J. (2022). The relationship between telework from home and employee health: A systematic review. *BMC Public Health, 22*(1), 47. https://doi.org/10.1186/s12889-021-12481-2

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity, 3*(1), 1–12. https://doi.org/10.1186/s42400-020-00050-w

MacColl, J., Husch, P., & Nurse, J. (2022). Beyond the bottom line: The societal impact of ransomware. *Royal United Services Institute.* Retrieved from https://rusi.org/explore-our-research/publications/commentary/beyond-bottom-line-societal-impact-ransomware

Mallinson, D. J., & Hatemi, P. K. (2018). The effects of information and social conformity on opinion change. *PLOS ONE, 13*(5), e0196600. https://doi.org/10.1371/journal.pone.0196600

Mamat, N., & Baqutayan, S. (2021). Differential perspectives of cyberloafing activities about computer ethics among employees. *Journal of Science, Technology and Innovation Policy, 5*(1), 22–33. https://doi.org/10.11113/jostip.v5n1.39

Mason, N. (2022). Using social cyberloafing to cope with workplace ostracism. *Nature Reviews Psychology, 1*(10), 557–557. https://doi.org/10.1038/s44159-022-00108-1

Mat Roni, S., & Djajadikerta, H. G. (2021). Non-parametric tests. In *Data analysis with SPSS for survey-based research* (pp. 219–260). Springer. https://doi.org/10.1007/978-981-16-0193-4_10

Mazzetti, G., & Schaufeli, W. B. (2022). The impact of engaging leadership on employee engagement and team effectiveness: A longitudinal, multi-level study on the mediating role of personal- and team resources. *PLOS ONE, 17*(6), e0269433. https://doi.org/10.1371/journal.pone.0269433

Mcleod, S. (2023). P-value and statistical significance: What it is & why it matters. *Simply Psychology.* Retrieved from https://www.simplypsychology.org/p-value.html

Menyhart, O., Weltz, B., & Győrffy, B. (2021). MultipleTesting.com: A tool for life science researchers for multiple hypothesis testing correction. *PLOS ONE, 16*(6), e0245824. https://doi.org/10.1371/journal.pone.0245824

Midway, S. R. (2020). Principles of effective data visualization. *Patterns, 1*(9), 100141. https://doi.org/10.1016/j.patter.2020.100141

Mishra, P., Pandey, C., Singh, U., Keshri, A., & Sabaretnam, M. (2019). Selection of appropriate statistical methods for data analysis. *Annals of Cardiac Anaesthesia, 22*(3), 297–301. https://doi.org/10.4103/aca.aca_248_18

Mohajan, H. K. (2017). Two criteria for good measurements in research: Validity and reliability. *Annals of Spiru Haret University. Economic Series, 17*(4), 59–82. https://doi.org/10.26458/1746

Mohammad, J., Quoquab, F., Halimah, S., & Thurasamy, R. (2019). Workplace internet leisure and employees' productivity: The mediating role of employee satisfaction. *Internet Research, 29*(4), 725–748. https://doi.org/10.1108/intr-05-2017-0191

Mokkink, L. B., Boers, M., van der Vleuten, C. P. M., Bouter, L. M., Alonso, J., Patrick, D. L., de Vet, H. C. W., & Terwee, C. B. (2020). COSMIN risk of bias tool to assess the quality of studies on reliability or measurement error of outcome measurement instruments: A Delphi study. *BMC Medical Research Methodology, 20*(1), 293. https://doi.org/10.1186/s12874-020-01179-5

Momani, A. M. (2020). The unified theory of acceptance and use of technology: A new approach in technology acceptance. *International Journal of Sociotechnology and Knowledge Development, 12*(3), 79–98. https://doi.org/10.4018/ijskd.2020070105

Morrison-Smith, S., & Ruiz, J. (2020). Challenges and barriers in virtual teams: A literature review. *SN Applied Sciences, 2*(6), 1096. https://doi.org/10.1007/s42452-020-2801-5

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology, 12,* 561011. https://doi.org/10.3389/fpsyg.2021.561011

Mshelbwala, F. S., Hugenberg, D. W., & Kreutz, R. P. (2020). Impact of routine platelet reactivity testing with VerifyNow assay on antiplatelet choice after percutaneous coronary intervention. *Clinical Pharmacology: Advances and Applications, 12,* 35–41. https://doi.org/10.2147/cpaa.s242675

Nadkarni, S., & Prügl, R. (2020). Digital transformation: A review, synthesis and opportunities for future research. *Management Review Quarterly, 71*(2), 233–341. https://doi.org/10.1007/s11301-020-00185-7

Nagler, R. H., Vogel, R. I., Gollust, S. E., Yzer, M. C., & Rothman, A. J. (2021). Effects of prior exposure to conflicting health information on responses to subsequent unrelated health messages: Results from a population-based longitudinal experiment. *Annals of Behavioral Medicine, 56*(5), 498–511. https://doi.org/10.1093/abm/kaab069

Nardi, B. A. (1995). Studying context: A comparison of activity theory, situated action models, and distributed cognition. In *Context and consciousness: Activity theory and human-computer interaction* (pp. 69–102). MIT Press. https://doi.org/10.7551/mitpress/2137.003.0008

National Institute for Health and Care Excellence. (2022). *Developing NICE guidelines: The manual.* Retrieved from https://www.nice.org.uk/process/pmg20/chapter/identifying-the-evidence-literature-searching-and-evidence-submission

Nguyen, M., Fujioka, J., Wentlandt, K., Onabajo, N., Wong, I., Bhatia, R. S., Bhattacharyya, O., & Stamenova, V. (2020). Using the technology acceptance model to explore health provider and administrator perceptions of the usefulness and ease of using technology in palliative care. *BMC Palliative Care, 19*(1), Article 138. https://doi.org/10.1186/s12904-020-00644-8

Nosek, B. A., & Errington, T. M. (2020). What is replication? *PLOS Biology, 18*(3), e3000691. https://doi.org/10.1371/journal.pbio.3000691

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.

Odoi, B., Samita, S., Al-Hassan, S., & Twumasi-Ankrah, S. (2019). Efficiency of Bartlett and Levene's tests for testing homogeneity of variance under varying number of replicates and groups in one–way ANOVA. *International Journal of Innovative Technology and Exploring Engineering, 8*(6), 1219–1223.

Ohana, M., Murtaza, G., Haq, I. U., Al-Shatti, E., & Chi, Z. (2024). Why and when can CSR toward employees lead to cyberloafing? The role of workplace boredom and moral disengagement. *Journal of Business Ethics, 189*(1), 133–148. https://doi.org/10.1007/s10551-023-05358-4

O'Sullivan, L., Feeney, L., Crowley, R. K., Sukumar, P., McAuliffe, E., & Doran, P. (2021). An evaluation of the process of informed consent: Views from research participants and staff. *Trials, 22*(1), Article 304. https://doi.org/10.1186/s13063-021-05493-1

Paradis, E., O'Brien, B., Nimmon, L., Bandiera, G., & Martimianakis, M. A. T. (2016). Design: Selection of data collection methods. *Journal of Graduate Medical Education, 8*(2), 263–264. https://doi.org/10.4300/jgme-d-16-00098.1

Parker, R., Thomsen, B. S., & Berry, A. (2022). Learning through play at school – A framework for policy and practice. *Frontiers in Education, 7,* Article 751801. https://doi.org/10.3389/feduc.2022.751801

Parsaeian, M., Mahdavi, M., Saadati, M., Mehdipour, P., Sheidaei, A., Khatibzadeh, S., Farzadfar, F., & Shahraz, S. (2021). Introducing an efficient sampling method for national surveys with limited sample sizes: Application to a national study to determine quality and cost of healthcare. *BMC Public Health, 21*(1), Article 1462. https://doi.org/10.1186/s12889-021-11441-0

Patwardhan, A. A., Pandey, N., & Dhume, S. M. (2017). Integrated model for understanding Indian physicians' internet usage pattern: An empirical approach. *International Journal of Healthcare Management, 10*(1), 19–33. https://doi.org/10.1080/20479700.2016.1270385

Pearson, N., Naylor, P. J., Ashe, M. C., Fernandez, M., Yoong, S. L., & Wolfenden, L. (2020). Guidance for conducting feasibility and pilot studies for implementation trials. *Pilot and Feasibility Studies, 6*(1), Article 167. https://doi.org/10.1186/s40814-020-00634-w

Pennington, C. R., Heim, D., Levy, A. R., & Larkin, D. T. (2016). Twenty years of stereotype threat research: A review of psychological mediators. *PLOS ONE, 11*(1), e0146487. https://doi.org/10.1371/journal.pone.0146487

Penn State University. (n.d.). *12.4 - Detecting multicollinearity using variance inflation factors.* Retrieved from https://online.stat.psu.edu/stat501/lesson/12/12.4

Perkins, N. J., Cole, S. R., Harel, O., Tchetgen Tchetgen, E. J., Sun, B., Mitchell, E. M., & Schisterman, E. F. (2017). Principled approaches to missing data in epidemiologic studies. *American Journal of Epidemiology, 187*(3), 568–575. https://doi.org/10.1093/aje/kwx348

Pernet, C. R., Wilcox, R., & Rousselet, G. A. (2013). Robust correlation analyses: False positive and power validation using a new open-source MATLAB toolbox. *Frontiers in Psychology, 3,* Article 606. https://doi.org/10.3389/fpsyg.2012.00606

Petrazzini, B. O., Naya, H., Lopez-Bello, F., Vazquez, G., & Spangenberg, L. (2021). Evaluation of different approaches for missing data imputation on features associated to genomic data. *BioData Mining, 14*(1), Article 17. https://doi.org/10.1186/s13040-021-00274-7

Petticrew, M., & Roberts, H. (2006). *Systematic reviews in the social sciences: A practical guide.* Blackwell. https://doi.org/10.1002/9780470754887

Phillips, S. M., Summerbell, C., Ball, H. L., Hesketh, K. R., Saxena, S., & Hillier-Brown, F. C. (2021a). The validity, reliability, and feasibility of measurement tools used to assess sleep of pre-school aged children: A systematic rapid review. *Frontiers in Pediatrics, 9,* Article 770262. https://doi.org/10.3389/fped.2021.770262

Phillips, S. M., Summerbell, C., Hobbs, M., Hesketh, K. R., Saxena, S., Muir, C., & Hillier-Brown, F. C. (2021b). A systematic review of the validity, reliability, and feasibility of measurement tools used to assess the physical activity and sedentary behaviour of pre-school aged children. *International Journal of Behavioral Nutrition and Physical Activity, 18*(1), Article 17. https://doi.org/10.1186/s12966-021-01132-9

Qotba, H. A., Al Nuaimi, A. S., Al Mujalli, H., Zainel, A. A., Khudadad, H., Marji, T., Veettil, S. T., & Syed, M. A. (2021). COVID-19 surveillance in the primary health care population of Qatar: Experience of prioritizing timeliness over representativeness when sampling the population. *Frontiers in Public Health, 9,* 654734. https://doi.org/10.3389/fpubh.2021.654734

Quader, F., & Janeja, V. P. (2021). Insights into organizational security readiness: Lessons learned from cyber-attack case studies. *Journal of Cybersecurity and Privacy, 1*(4), 638–659. https://doi.org/10.3390/jcp1040032

Ramezani, N., Bhati, A., Murphy, A., Routh, D., & Taxman, F. S. (2022). Assessing the reliability and validity of the risk-need-responsivity (RNR) program tool. *Health & Justice, 10*(1), Article 1. https://doi.org/10.1186/s40352-022-00182-w

Raymaekers, J., & Rousseeuw, P. J. (2021). Transforming variables to central normality. *Machine Learning.* https://doi.org/10.1007/s10994-021-05960-5

Razali, N. A. (2020). Study on personal internet use and cyberloafing activities in workplace. *European Proceedings of Social and Behavioural Sciences.* https://doi.org/10.15405/epsbs.2020.12.05.96

Reisinger, H., & Fetterer, D. (2021, November 5). Forget flexibility. Your employees want autonomy. *Harvard Business Review.* https://hbr.org/2021/10/forget-flexibility-your-employees-want-autonomy

Reizer, A., Galperin, B. L., Chavan, M., Behl, A., & Pereira, V. (2022). Examining the relationship between fear of COVID-19, intolerance for uncertainty, and cyberloafing: A mediational model. *Journal of Business Research, 145,* 660–670. https://doi.org/10.1016/j.jbusres.2022.03.037

Reshmi, T. R. (2021). Information security breaches due to ransomware attacks: A systematic literature review. *International Journal of Information Management Data Insights, 1*(2), 100013. https://doi.org/10.1016/j.jjimei.2021.100013

Roczniewska, M., Smoktunowicz, E., Calcagni, C. C., von Thiele Schwarz, U., Hasson, H., & Richter, A. (2022). Beyond the individual: A systematic review of the effects of unit-level demands and resources on employee productivity, health, and well-being. *Journal of Occupational Health Psychology, 27*(2), 240–257. https://doi.org/10.1037/ocp0000311

Rogers, G., Szomszor, M., & Adams, J. (2020). Sample size in bibliometric analysis. *Scientometrics, 125*(1), 777–794. https://doi.org/10.1007/s11192-020-03647-7

Ronchetti, E. (2021). The main contributions of robust statistics to statistical science and a new challenge. *METRON, 79*(2), 127–135. https://doi.org/10.1007/s40300-020-00185-3

Ross, P. T., & Zaidi, N. L. B. (2019). Limited by my limitations. *Perspectives on Medical Education, 8*(4), 261–264. https://doi.org/10.1007/s40037-019-00530-x

Ross, R. K., Breskin, A., & Westreich, D. (2020). When is a complete-case approach to missing data valid? The importance of effect-measure modification. *American*

Journal of Epidemiology, 189(12), 1583–1589. https://doi.org/10.1093/aje/kwaa124

Rosseel, R. (2021). Correlation analysis: All the basics you need to know. *365 Data Science.* Retrieved from https://365datascience.com/trending/correlation-analysis/

Rousselet, G. A., & Pernet, C. R. (2012). Improving standards in brain–behavior correlation analyses. *Frontiers in Human Neuroscience, 6,* Article 119. https://doi.org/10.3389/fnhum.2012.00119

Rudolph, M., Sato, K., & Loewen, P. (2025). Rethinking the evaluation of educational intervention effectiveness through an activity theory lens: A holistic systems approach. *Frontiers in Education, 10,* 1532376. https://doi.org/10.3389/feduc.2025.1532376

Salmerón, R., García, C., & García, J. (2020). Overcoming the inconsistencies of the variance inflation factor: A redefined VIF and a test to detect statistical troubling multicollinearity. *arXiv.* https://doi.org/10.48550/arxiv.2005.02245

Salmond, E. (2023). A cautionary note on calculating correlations on combined data sets: When observations are non-independently and non-identically distributed. *Frontiers in Systems Biology, 5,* Article 1042156. https://doi.org/10.3389/fsysb.2023.1042156

Saltos-Rivas, R., Novoa-Hernández, P., & Serrano Rodríguez, R. (2021). On the quality of quantitative instruments to measure digital competence in higher education: A systematic mapping study. *PLOS ONE, 16*(9), e0257344. https://doi.org/10.1371/journal.pone.0257344

Sandjakoska, L., & Stojanovska, F. (2020). How initialization is related to deep neural networks generalization capability: Experimental study. *2020 55th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)*. https://doi.org/10.1109/icest49890.2020.9232882

Sanislav, T., Zeadally, S., Mois, G. D., & Folea, S. C. (2018). Wireless energy harvesting: Empirical results and practical considerations for internet of things. *Journal of Network and Computer Applications, 121,* 149–158. https://doi.org/10.1016/j.jnca.2018.08.002

Sao, R., Chandak, S., Patel, B., & Bhadade, P. (2020). Cyberloafing: Effects on employee job performance and behavior. *International Journal of Recent Technology and Engineering (IJRTE), 8*(5), 1509–1515. https://doi.org/10.35940/ijrte.e4832.018520

Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. *SN Computer Science, 2*(3), Article 160. https://doi.org/10.1007/s42979-021-00592-x

Sarkies, M. N., Skinner, E. H., Bowles, K. A., Morris, M. E., Williams, C., O’Brien, L., Bardoel, A., Martin, J., Holland, A. E., Carey, L., White, J., & Haines, T. P. (2019). A novel counterbalanced implementation study design: Methodological description and application to implementation research. *Implementation Science, 14,* Article 45. https://doi.org/10.1186/s13012-019-0896-0

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *International Cybersecurity Law Review, 3*(1), 7–34. https://doi.org/10.1365/s43439-021-00045-4

Schäfer, T., & Schwarz, M. A. (2019). The meaningfulness of effect sizes in psychological research: Differences between sub-disciplines and the impact of potential biases. *Frontiers in Psychology, 10,* Article 813. https://doi.org/10.3389/fpsyg.2019.00813

Schaffer, A. L., Dobbins, T. A., & Pearson, S. A. (2021). Interrupted time series analysis using autoregressive integrated moving average (ARIMA) models: A guide for evaluating large-scale health interventions. *BMC Medical Research Methodology, 21,* Article 58. https://doi.org/10.1186/s12874-021-01235-8

Schemer, C., Masur, P. K., Geiß, S., Müller, P., & Schäfer, S. (2021). The impact of internet and social media use on well-being: A longitudinal analysis of adolescents across nine years. *Journal of Computer-Mediated Communication, 26*(1), 1–21. https://doi.org/10.1093/jcmc/zmaa014

Schober, P., Boer, C., & Schwarte, L. A. (2018). Correlation coefficients: Appropriate use and interpretation. *Anesthesia & Analgesia, 126*(5), 1763–1768. https://doi.org/10.1213/ane.0000000000002864

Schober, P., & Vetter, T. R. (2019). Chi-square tests in medical research. *Anesthesia & Analgesia, 129*(5), 1193. https://doi.org/10.1213/ane.0000000000004410

Schofield, G., Dittborn, M., Selman, L. E., & Huxtable, R. (2021). Defining ethical challenge(s) in healthcare research: A rapid review. *BMC Medical Ethics, 22,* Article 115. https://doi.org/10.1186/s12910-021-00700-9

Schuster, N. A., Rijnhart, J. J. M., Twisk, J. W. R., & Heymans, M. W. (2022). Modeling non-linear relationships in epidemiological data: The application and interpretation of spline models. *Frontiers in Epidemiology, 2,* Article 975380. https://doi.org/10.3389/fepid.2022.975380

Seeram, E. (2019). An overview of correlational research. *Radiologic Technology, 91*(2), 176–179. https://pubmed.ncbi.nlm.nih.gov/31685592/

Sekaran, U., & Bougie, R. J. (2016). *Research methods for business: A skill building approach* (7th ed.). John Wiley & Sons.

Sener, G. (2020). Opinions of vocational school students regarding in-class cyberloafing activities. *International Online Journal of Educational Sciences, 12*(4). https://doi.org/10.15345/iojes.2020.04.017

Sham, W. W. L., Yeung, G. T. Y., Mak, W. W. S., & Powell, C. L. Y. M. (2021). Comprehensive well-being scale: Development and validation among Chinese in recovery of mental illness in Hong Kong. *BMC Psychology, 9,* Article 156. https://doi.org/10.1186/s40359-021-00686-4

Sharton, B. (2021). Ransomware attacks are spiking: Is your company prepared? *Harvard Business Review.* https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared

Shrestha, A. K., Vassileva, J., Joshi, S., & Just, J. (2021). Augmenting the technology acceptance model with trust model for the initial adoption of a blockchain-based system. *PeerJ Computer Science, 7,* e502. https://doi.org/10.7717/peerj-cs.502

Shrestha, N. (2020). Detecting multicollinearity in regression analysis. *American Journal of Applied Mathematics and Statistics, 8*(2), 39–42. https://doi.org/10.12691/ajams-8-2-1

Shukla, S., Hassan, M. F., Tran, D. C., Akbar, R., Paputungan, I. V., & Khan, M. K. (2023). Improving latency in internet-of-things and cloud computing for real-time data transmission: A systematic literature review (SLR). *Cluster Computing, 26*(5), 2657–2680. https://doi.org/10.1007/s10586-021-03279-3

Siegel, J. T., & Navarro, M. (2019). A conceptual replication examining the risk of overtly listing eligibility criteria on Amazon's Mechanical Turk. *Journal of Applied Social Psychology, 49*(4), 239–248. https://doi.org/10.1111/jasp.12580

Siegle, D. (2021). Confidence intervals and levels. *University of Connecticut.* Retrieved from https://researchbasics.education.uconn.edu/confidence-intervals-and-levels/

Simsek, A., & Elciyar, K. (2021). An investigation of cyberloafing in a large-scale technology organization from the perspective of the theory of interpersonal behavior. *Online Journal of Communication and Media Technologies, 11*(2), e202106. https://doi.org/10.30935/ojcmt/10823

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Slocum, T. A., Pinkelman, S. E., Joslyn, P. R., & Nichols, B. (2022). Threats to internal validity in multiple-baseline design variations. *Perspectives on Behavior Science, 45*(3), 619–638. https://doi.org/10.1007/s40614-022-00326-1

Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity, 7*(1), tyab019. https://doi.org/10.1093/cybsec/tyab019

Song, M., Ugrin, J., Li, M., Wu, J., Guo, S., & Zhang, W. (2021). Do deterrence mechanisms reduce cyberloafing when it is an observed workplace norm? A moderated mediation model. *International Journal of Environmental Research and Public Health, 18*(13), 6751. https://doi.org/10.3390/ijerph18136751

Sonntag, O., & Loh, T. P. (2023). Calibration: An underappreciated component in the analytical process of medical laboratories. *Clinical Chemistry and Laboratory Medicine, 61*(1), e1–e8. https://doi.org/10.1515/cclm-2023-xxxx

Soon Chew, T. (2023). Considerations for developing cybersecurity awareness training. *ISACA Journal, 2.* Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for-developing-cybersecurity-awareness-training

Spacey, A., Harvey, O., & Casey, C. (2021). Postgraduate researchers' experiences of accessing participants via gatekeepers: 'Wading through treacle!'. *Journal of Further and Higher Education, 45*(4), 433–450. https://doi.org/10.1080/0309877x.2020.1774051

Spineli, L. M., Kalyvas, C., & Papadimitropoulou, K. (2021). How robust are findings of pairwise and network meta-analysis in the presence of missing participant outcome data? *BMC Medicine, 19,* Article 107. https://doi.org/10.1186/s12916-021-02195-y

Sridhar, R., & Nandhini, M. (2021). Ensemble human movement sequence prediction model with Apriori based probability tree classifier (APTC) and bagged J48 on machine learning. *Journal of King Saud University – Computer and Information Sciences, 33*(4), 408–416. https://doi.org/10.1016/j.jksuci.2018.04.002

Srinivasan, R., & Lohith, C. P. (2017). Pilot study—Assessment of validity and reliability. In *India Studies in Business and Economics* (pp. 43–49). Springer. https://doi.org/10.1007/978-981-10-3590-6_6

Streiner, D. L., Norman, G. R., & Cairney, J. (2015). *Health measurement scales.* Oxford University Press. https://doi.org/10.1093/med/9780199685219.001.0001

Sulaiman, N., Fauzi, M., Wider, W., Rajadurai, J., Hussain, S., & Harun, S. (2022). Cyber–information security compliance and violation behaviour in organisations: A systematic review. *Social Sciences, 11*(9), 386. https://doi.org/10.3390/socsci11090386

Sullivan, L. (n.d.). Hypothesis testing – Analysis of variance (ANOVA). *Boston University School of Public Health.* Retrieved from https://sphweb.bumc.bu.edu/otlt/MPH-Modules/BS/BS704_HypothesisTesting-ANOVA/BS704_HypothesisTesting-Anova_print.html

Syed, S. (2020). The impact of cyberloafing on employees' job performance: A review of literature. *Journal of Advances in Management Sciences & Information Systems, 6,* 16–28. https://doi.org/10.6000/2371-1647.2020.06.02

Taber, K. S. (2017). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in Science Education, 48*(6), 1273–1296. https://doi.org/10.1007/s11165-016-9602-2

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. *Electronics, 11*(14), 2181. https://doi.org/10.3390/electronics11142181

Talavera-Velasco, B., Luceño-Moreno, L., Martín García, J., & Vázquez-Estévez, D. (2018). DECORE-21: Assessment of occupational stress in police. Confirmatory factor analysis of the original model. *PLOS ONE, 13*(10), e0205028. https://doi.org/10.1371/journal.pone.0205028

Tamilmani, K., Rana, N. P., Wamba, S. F., & Dwivedi, R. (2021). The extended unified theory of acceptance and use of technology (UTAUT2): A systematic literature review and theory evaluation. *International Journal of Information Management, 57,* 102269. https://doi.org/10.1016/j.ijinfomgt.2020.102269

Tan, P. T., Cro, S., Van Vogt, E., Szigeti, M., & Cornelius, V. R. (2021). A review of the use of controlled multiple imputation in randomised controlled trials with missing outcome data. *BMC Medical Research Methodology, 21,* Article 46. https://doi.org/10.1186/s12874-021-01261-6

Tandon, A., Kaur, P., Ruparel, N., Islam, J. U., & Dhir, A. (2022). Cyberloafing and cyberslacking in the workplace: Systematic literature review of past achievements and future promises. *Internet Research, 32*(1), 55–89. https://doi.org/10.1108/intr-06-2020-0332

Tempelaar, D., Rienties, B., & Nguyen, Q. (2020). Subjective data, objective data and the role of bias in predictive modelling: Lessons from a dispositional learning analytics application. *PLOS ONE, 15*(6), e0233977. https://doi.org/10.1371/journal.pone.0233977

Tennant, J. P., & Ross-Hellauer, T. (2020). The limitations to our understanding of peer review. *Research Integrity and Peer Review, 5,* Article 6. https://doi.org/10.1186/s41073-020-00092-1

Thabane, L., Mbuagbaw, L., Zhang, S., Samaan, Z., Marcucci, M., Ye, C., Thabane, M., Giangregorio, L., Dennis, B., Kosa, D., Debono, V. B., Dillenburg, R., Fruci, V., Bawor, M., Lee, J., Wells, G., & Goldsmith, C. H. (2013). A tutorial on sensitivity analyses in clinical trials: The what, why, when and how. *BMC Medical Research Methodology, 13,* Article 92. https://doi.org/10.1186/1471-2288-13-92

Thelwall, M., & Mas-Bleda, A. (2020). How common are explicit research questions in journal articles? *Quantitative Science Studies,* 1–19. https://doi.org/10.1162/qss_a_00041

Theofanidis, D., & Fountouki, A. (2019). Limitations and delimitations in the research process. *Perioperative Nursing (GORNA), 7*(3), 155–162. http://doi.org/10.5281/zenodo.2552022

Thrun, M. C., Gehlert, T., & Ultsch, A. (2020). Analyzing the fine structure of distributions. *PLOS ONE, 15*(10), e0238835. https://doi.org/10.1371/journal.pone.0238835

Tiersma, K., Reichman, M., Popok, P. J., Nelson, Z., Barry, M., Elwy, A. R., Flores, E. J., Irwin, K. E., & Vranceanu, A. M. (2022). The strategies for quantitative and qualitative remote data collection: Lessons from the COVID-19 pandemic. *JMIR Formative Research, 6*(4), e30055. https://doi.org/10.2196/30055

Tomšik, R. (2019). Power comparisons of Shapiro–Wilk, Kolmogorov–Smirnov and Jarque–Bera tests. *Scholars Journal of Research in Mathematics and Computer Science, 3*(3), 238–243. https://www.researchgate.net/publication/333133367

Tsai, H. Y. (2023). Do you feel like being proactive today? How daily cyberloafing influences creativity and proactive behavior: The moderating roles of work environment. *Computers in Human Behavior, 138,* 107470. https://doi.org/10.1016/j.chb.2022.107470

United States Department of Health and Human Services. (1979). *The Belmont Report*. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html

U.S. Bureau of Labor Statistics. (2023). *American time use survey – 2022 results (USDL-23-1364)*. https://www.bls.gov/news.release/atus.htm

van den Boogaart, K. G., Filzmoser, P., Hron, K., Templ, M., & Tolosana-Delgado, R. (2020). Classical and robust regression analysis with compositional data.

Mathematical Geosciences, 53(5), 823–858. https://doi.org/10.1007/s11004-020-09895-w

van den Broeck, J., Argeseanu Cunningham, S., Eeckels, R., & Herbst, K. (2005). Data cleaning: Detecting, diagnosing, and editing data abnormalities. *PLoS Medicine, 2*(10), e267. https://doi.org/10.1371/journal.pmed.0020267

Van der Voordt, T., & Jensen, P. A. (2023). The impact of healthy workplaces on employee satisfaction, productivity and costs. *Journal of Corporate Real Estate, 25*(1), 29–49. https://doi.org/10.1108/jcre-03-2021-0012

Varbanova, V., & Beutels, P. (2020). Recent quantitative research on determinants of health in high income countries: A scoping review. *PLOS ONE, 15*(9), e0239031. https://doi.org/10.1371/journal.pone.0239031

Veazie, S., Peterson, K., Bourne, D., Anderson, J., Damschroder, L., & Gunnar, W. (2022). Implementing high-reliability organization principles into practice: A rapid evidence review. *Journal of Patient Safety, 18*(1), e320–e328. https://doi.org/10.1097/pts.0000000000000768

Vigneshwaran, E., Madineni, M., Sake, K., Alakhali, K., Sirajudeen, S., & Khan, N. (2017). Comparative analysis of cost and efficacy for mono and dual therapy of antiepileptics among children. *Drug Development and Therapeutics, 8*(1), 25. https://doi.org/10.4103/ddt.ddt_16_16

Vorm, E. S., & Combs, D. J. Y. (2022). Integrating transparency, trust, and acceptance: The Intelligent Systems Technology Acceptance Model (ISTAM). *International*

Journal of Human-Computer Interaction, 38(18–20), 1828–1845. https://doi.org/10.1080/10447318.2022.2070107

Vygotsky, L. S. (1978). *Mind in society: The development of higher psychological processes.* Harvard University Press. https://doi.org/10.2307/j.ctvjf9vz4

Wada, K. (2020). Outliers in official statistics. *Japanese Journal of Statistics and Data Science, 3*(2), 669–691. https://doi.org/10.1007/s42081-020-00091-y

Walentynowicz, M., Schneider, S., & Stone, A. A. (2018). The effects of time frames on self-report. *PLOS ONE, 13*(8), e0201655. https://doi.org/10.1371/journal.pone.0201655

Wallisch, C., Bach, P., Hafermann, L., Klein, N., Sauerbrei, W., Steyerberg, E. W., Heinze, G., Rauch, G., & on behalf of topic group 2 of the STRATOS initiative. (2022). Review of guidance papers on regression modeling in statistical series of medical journals. *PLOS ONE, 17*(1), e0262918. https://doi.org/10.1371/journal.pone.0262918

Westfall, J., & Yarkoni, T. (2016). Statistically controlling for confounding constructs is harder than you think. *PLOS ONE, 11*(3), e0152719. https://doi.org/10.1371/journal.pone.0152719

White House. (2021). *Fact sheet: Ongoing public U.S. efforts to counter ransomware.* https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of Medical Internet Research, 22*(9), e23692. https://doi.org/10.2196/23692

Wiśniowski, A., Sakshaug, J. W., Perez Ruiz, D. A., & Blom, A. G. (2020). Integrating probability and nonprobability samples for survey inference. *Journal of Survey Statistics and Methodology, 8*(1), 120–147. https://doi.org/10.1093/jssam/smz051

Wlosinski, L. (2020). Ransomware response, safeguards and countermeasures. *ISACA Journal, 4*. https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/ransome-response-safeguards-and-countermeasures

Wolff, J. (2021). How is technology changing the world, and how should the world change technology? *Global Perspectives, 2*(1). https://doi.org/10.1525/gp.2021.27353

Wu, H. (2020). *Introduction to difference in differences (DID) analysis.* CFDR Workshop Series. https://www.bgsu.edu/content/dam/BGSU/college-of-arts-and-sciences/center-for-family-and-demographic-research/documents/Workshops/2020-Difference-in-Difference-analysis.pdf

Wu, J., Mei, W., Liu, L., & Ugrin, J. C. (2020). The bright and dark sides of social cyberloafing: Effects on employee mental health in China. *Journal of Business Research, 112,* 56–64. https://doi.org/10.1016/j.jbusres.2020.02.043

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research, 39*(1), 93–112. https://doi.org/10.1177/0739456x17723971

Xie, Y., & DeVellis, R. F. (1992). Scale development: Theory and applications. *Contemporary Sociology, 21*(6), 876. https://doi.org/10.2307/2075704

Xiong, H., Payne, D., & Kinsella, S. (2016). Peer effects in the diffusion of innovations: Theory and simulation. *Journal of Behavioral and Experimental Economics, 63,* 1–13. https://doi.org/10.1016/j.socec.2016.04.017

Yadav, D. (2022). Criteria for good qualitative research: A comprehensive review. *The Asia-Pacific Education Researcher, 31*(6), 679–689. https://doi.org/10.1007/s40299-021-00619-0

Yang, K., Tu, J., & Chen, T. (2019). Homoscedasticity: An overlooked critical assumption for linear regression. *General Psychiatry, 32*(5), e100148. https://doi.org/10.1136/gpsych-2019-100148

Yazdanmehr, A., & Wang, J. (2023). Can peers help reduce violations of information security policies? The role of peer monitoring. *European Journal of Information Systems, 32*(3), 508–528. https://doi.org/10.1080/0960085x.2021.1980444

Yip, J. A., Levine, E. E., Brooks, A. W., & Schweitzer, M. E. (2020). Worry at work: How organizational culture promotes anxiety. *Research in Organizational Behavior, 40,* 100124. https://doi.org/10.1016/j.riob.2020.100124

Young, J. (2023). Representative sample: Definition, importance, and examples. *Investopedia.* https://www.investopedia.com/terms/r/representative-sample.asp

Yurekten, O., & Demirci, M. (2021). Citadel: Cyber threat intelligence assisted defense system for software-defined networks. *Computer Networks, 191,* 108013. https://doi.org/10.1016/j.comnet.2021.108013

Yuryna Connolly, L., Wall, D. S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity, 6*(1). https://doi.org/10.1093/cybsec/tyaa023

Zhang, Y., Wang, J., Akhtar, M. N., & Wang, Y. (2022). Authoritarian leadership and cyberloafing: A moderated mediation model of emotional exhaustion and power distance orientation. *Frontiers in Psychology, 13.* https://doi.org/10.3389/fpsyg.2022.1010845

Zhong, J., Chen, Y., Yan, J., & Luo, J. (2022). The mixed blessing of cyberloafing on innovation performance during the COVID-19 pandemic. *Computers in Human Behavior, 126,* 106982. https://doi.org/10.1016/j.chb.2021.106982

Zimmerman, C., Mak, J., Pocock, N. S., & Kiss, L. (2021). Human trafficking: Results of a 5-year theory-based evaluation of interventions to prevent trafficking of women from South Asia. *Frontiers in Public Health, 9.* https://doi.org/10.3389/fpubh.2021.645059

Zohrabi, M. (2013). Mixed method research: Instruments, validity, reliability and reporting findings. *Theory and Practice in Language Studies, 3*(2), 254–262. https://doi.org/10.4304/tpls.3.2.254-262

Appendix A - Firewall Category SQL Query and Result Summary

This appendix provides the SQL query used to extract category-level browsing data from the firewall logs and the corresponding summary of the results. The table includes the category name, the count of unique visits, the number of detected ransomware alerts, the number of ransomware risk alerts, and the total bandwidth used in gigabytes (GB).

SQL Query

```
SELECT
  CAST(f.Category AS VARCHAR(255)) AS Category,
  COUNT(DISTINCT CAST(f.Hostname AS VARCHAR(255))) AS Visits,
  COUNT(CASE
    WHEN CAST(f.Category AS VARCHAR(255)) IN (
      'Phishing',
      'Malicious Websites',
      'Spam URLs',
      'Proxy Avoidance',
      'Hacking',
      'Illegal or Unethical'
```

```
    ) THEN 1
END) AS Ransomware_Alerts,
COUNT(CASE
    WHEN CAST(f.Category AS VARCHAR(255)) IN (
        'File Sharing and Storage',
        'Peer-to-peer File Sharing',
        'Freeware and Software Downloads',
        'Dynamic Content',
        'Dynamic DNS',
        'Newly Observed Domain',
        'Newly Registered Domain',
        'Web Hosting',
        'Web-based Applications',
        'Web-based Email',
        'Remote Access',
        'Information and Computer Security',
        'Information Technology',
```

```
            'Instant Messaging',
            'Content Servers',
            'Unrated'
        ) THEN 1
    END) AS Ransomware_Risk_Alerts,
    ROUND(SUM(b.Bandwidth) / 1024.0, 2) AS Bandwidth_GB
FROM
    BrowsingData f
FULL OUTER JOIN
    BandwidthData b ON f.DateTime = b.Time
WHERE
    CAST(f.Category AS VARCHAR(255)) IS NOT NULL
GROUP BY
    CAST(f.Category AS VARCHAR(255))
ORDER BY
    CAST(f.Category AS VARCHAR(255));
```

Table 8

Firewall Categories and Result Summary

Category	Visits	Ransomware_Alerts	Ransomware_Risk_Alerts	Bandwidth_GB
Abortion	16	0	0	NULL
Advertising	814,083	0	0	2,005,543
Advocacy organizations	137	0	0	30.7
Alcohol	525	0	0	180.64
Alternative beliefs	64	0	0	22.46
Armedf	488	0	0	518.71
Arts and culture	4,216	0	0	5,663.98
Auction	344	0	0	8,402.04
BAN	138	0	0	NULL
Brokerage and trading	405	0	0	1,678.92
Business	115,572	0	0	990,461.2
Charitable organizations	482	0	0	308.32

Category	Visits	Ransomware_Alerts	Ransomware_Risk_Alerts	Bandwidth_GB
Child education	1,097	0	0	33,648.32
Content servers	110,956	0	102,477,993	782,043.2
Dating	234	0	0	400.78
Digital postcards	101	0	0	225.87
Domain parking	2,532	0	0	6,903.56
Drug abuse	2	0	0	NULL
Dynamic content	72	0	29,152	182.41
Dynamic dns	47	0	13,101	71.91
Education	124,365	0	0	1,380,657
Entertainment	15,055	0	0	29,153.68
Explicit violence	26	0	0	NULL
Extremist groups	1	0	0	NULL
File sharing and storage	16,884	0	10,448,176	67,568.71
Finance and banking	10,095	0	0	26,279.35

Category	Visits	Ransomware_Alerts	Ransomware_Risk_Alerts	Bandwidth_GB
Folklore	167	0	0	95.11
Freeware and software downloads	1,447	0	6,514,367	41,592.7
Gambling	459	0	0	348.53
Games	9,685	0	0	54,055.63
General organizations	4,311	0	0	30,982.79
Global religion	2,916	0	0	1,789.73
Government and legal organizations	6,344	0	0	20,133.29
Hacking	1,321	1,154,222	0	11,949.03
Health and wellness	13,819	0	0	12,295.57
Illegal or unethical	575	20,108	0	329.47
Information and computer security	692	0	12,896,724	78,145.26
Information technology	2,110,436	0	1,470,685,135	7,878,588
Instant messaging	516	0	14,717,546	118,105.2

Category	Visits	Ransomware_Alerts	Ransomware_Risk_Alerts	Bandwidth_GB
Internet radio and tv	1,928	0	0	32,584.71
Internet telephony	88	0	0	15,595.76
Job search	2,187	0	0	1,968.65
Lingerie and swimsuit	198	0	0	578.21
Malicious websites	1,102	136,537	0	2,820.95
Marijuana	107	0	0	NULL
Meaningless content	12,387	0	0	89,235.57
Medicine	232	0	0	67.57
Newly observed domain	7,209	0	114,064	2,598.98
Newly registered domain	883	0	12,775	80.26
News and media	11,429	0	0	160,537.8
Newsgroups and message boards	1,012	0	0	15,905.15
Nudity and risque	3	0	0	NULL
Online meeting	186	0	0	535.23
Other adult materials	478	0	0	224.64

Category	Visits	Ransomware_Alerts	Ransomware_Risk_Alerts	Bandwidth_GB
Peer-to-peer file sharing	322	0	4,375	NULL
Personal vehicles	5,250	0	0	10,053.93
Personal websites and blogs	12,000	0	0	8,731.25
Phishing	1,232	94,174	0	863.32
Plagiarism	155	0	0	91.95
Political organizations	744	0	0	623.13
Pornography	1,722	0	0	318.13
Proxy avoidance	2,470	9,802,347	0	78,095.7
Real estate	2,923	0	0	30,810.64
Reference	10,793	0	0	41,042.55
Remote access	3,221	0	39,445	164.39
Restaurant and dining	5,517	0	0	10,694.28
Search engines and portals	32,369	0	0	1,379,234
Secure websites	691	0	0	11,346.58
Sex education	13	0	0	11.34
Shopping	25,208	0	0	342,789.3

Category	Visits	Ransomware_Alerts	Ransomware_Risk_Alerts	Bandwidth_GB
Social networking	498,036	0	0	867,004
Society and lifestyles	4,604	0	0	5,062.99
Spam urls	550	46,522	0	366.92
Sports	8,930	0	0	44,003.66
Sports hunting and war games	31	0	0	NULL
Streaming media and download	9,033	0	0	1,861,134
Tobacco	107	0	0	NULL
Travel	10,037	0	0	57,811.24
Unrated	6,303	0	1,981,229	11,757.45
Weapons (sales)	375	0	0	89.25
Web analytics	216,947	0	0	389,836
Web chat	86	0	0	803.85
Web hosting	26,257	0	16,849,423	129,913.1

Category	Visits	Ransomware_Alerts	Ransomware_Risk_Alerts	Bandwidth_GB
Web-based applications	1,953	0	69,331,620	466,699.8
Web-based email	717	0	8,624,220	59,713.05

Appendix B - Descriptive Statistics for Bandwidth Usage

This appendix presented the SQL query and resulting descriptive statistics for the bandwidth data used in the study. The statistical measures included the mean, standard deviation, minimum, and maximum bandwidth values (in gigabytes) collected from the BandwidthData table.

SQL Query

```
SELECT
    ROUND(AVG(Bandwidth), 2) AS Mean_Bandwidth_MB,
    ROUND(STDEV(Bandwidth), 2) AS Standard_Deviation_MB,
    ROUND(MIN(Bandwidth), 2) AS Minimum_MB,
    ROUND(MAX(Bandwidth), 2) AS Maximum_MB
FROM
    BandwidthData;
```

Table 9

Bandwidth Usage Summary

Mean_Bandwidth_MB	Standard_Deviation_MB	Minimum_MB	Maximum_MB
1,458.38	2,167.49	34.1	8,530

Appendix C - Ransomware Alert Types and Risk Classification

This appendix presented the SQL query and results used to classify and analyze different ransomware-related categories based on their confidence level, frequency, and proportional representation in the dataset. Categories were grouped into High Confidence (indicative of known ransomware behavior) and Risk (associated with higher risk of ransomware delivery or hosting).

SQL Query

```
SELECT

  Category AS Alert_Type,

  CASE

    WHEN Category IN ('Phishing', 'Malicious Websites', 'Spam URLs', 'Proxy
      Avoidance', 'Hacking', 'Illegal or Unethical')

      THEN 'High'

    WHEN Category IN ('File Sharing and Storage', 'Peer-to-peer File Sharing',
      'Freeware and Software Downloads', 'Dynamic Content',

              'Dynamic DNS', 'Newly Observed Domain', 'Newly Registered Domain',
      'Web Hosting', 'Web-based Applications',

              'Web-based Email', 'Remote Access', 'Information and Computer
      Security', 'Information Technology',
```

```
                'Instant Messaging', 'Content Servers', 'Unrated')
            THEN 'Risk'
        ELSE 'Other'
    END AS Confidence_Level,
    COUNT(*) AS Frequency,
    ROUND(COUNT(*) * 100.0 / SUM(COUNT(*)) OVER(), 2) AS Percentage
FROM BrowsingData
WHERE Category IN (
    'Phishing', 'Malicious Websites', 'Spam URLs', 'Proxy Avoidance', 'Hacking', 'Illegal or
        Unethical',
    'File Sharing and Storage', 'Peer-to-peer File Sharing', 'Freeware and Software
        Downloads', 'Dynamic Content',
    'Dynamic DNS', 'Newly Observed Domain', 'Newly Registered Domain', 'Web
        Hosting', 'Web-based Applications',
    'Web-based Email', 'Remote Access', 'Information and Computer Security',
        'Information Technology',
    'Instant Messaging', 'Content Servers', 'Unrated'
)
```

```
GROUP BY Category

ORDER BY Confidence_Level, Category;
```

Table 10

Ransomware Alert Summary

Alert_Type	Confidence_Level	Frequency	Percentage
Hacking	High	1,152,903	0.07
Illegal or unethical	High	20,077	0
Malicious websites	High	136,217	0.01
Phishing	High	94,087	0.01
Proxy avoidance	High	9,793,916	0.57
Spam urls	High	46,484	0
Content servers	Risk	102,393,504	5.94
Dynamic content	Risk	29,134	0
Dynamic dns	Risk	13,091	0
File sharing and storage	Risk	10,439,421	0.61
Freeware and software downloads	Risk	6,508,764	0.38
Information and computer security	Risk	12,885,680	0.75
Information technology	Risk	1,469,367,790	85.21
Instant messaging	Risk	14,705,510	0.85
Newly observed domain	Risk	113,843	0.01

Alert_Type	Confidence_Level	Frequency	Percentage
Newly registered domain	Risk	12,765	0
Peer-to-peer file sharing	Risk	4,375	0
Remote access	Risk	39,418	0
Unrated	Risk	1,979,952	0.11
Web hosting	Risk	16,833,440	0.98
Web-based applications	Risk	69,270,479	4.02
Web-based email	Risk	8,617,181	0.5

Appendix D - Cyberloafing Categories and Visit Frequency

This appendix included the SQL query and output used to identify categories of cyberloafing—non-work-related internet activity—based on browsing data. Cyberloafing was operationalized through visits to sites related to social networking, shopping, entertainment, and similar non-instructional categories. The data included total visits and percentage distribution across all observed cyberloafing traffic.

SQL Query

```
SELECT
    Category AS Cyberloafing_Category,
    COUNT(*) AS Visits,
    ROUND(COUNT(*) * 100.0 / SUM(COUNT(*)) OVER(), 2) AS Percentage
FROM BrowsingData
WHERE Category IN (
    'Social Networking',
    'Web-based Email',
    'Shopping',
    'Gambling',
    'Entertainment',
```

```
    'Streaming Media and Download',
    'Games',
    'Dating',
    'Pornography',
    'Nudity and Risque'
)
GROUP BY Category
ORDER BY Visits DESC;
```

Table 11

Cyberloafing Activity Summary

Cyberloafing_Category	Visits	Percentage
Streaming media and download	22,519,0194	57.07
Social networking	105,660,228	26.78
Shopping	44,371,673	11.25
Web-based email	8,617,181	2.18
Games	7,046,073	1.79
Entertainment	3,516,019	0.89
Gambling	59,133	0.01
Dating	53,695	0.01
Pornography	42,968	0.01
Nudity and risque	21	0