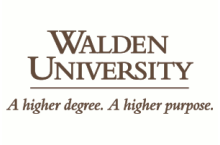

2019

Strategies That Mitigate IT Infrastructure Demands Produced by Student BYOD Usa

Martha Dunne
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Martha Jane Dunne

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. Gail Miles, Committee Chairperson, Information Technology Faculty
Dr. Steven Case, Committee Member, Information Technology Faculty
Dr. Gary Griffith, University Reviewer, Information Technology Faculty

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

Walden University
2019

Abstract

Strategies That Mitigate IT Infrastructure Demands Produced by Student BYOD Usage

by

Martha Jane Dunne

MS, University of Phoenix, 2009

BS, University of Phoenix, 2006

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2019

Abstract

The use of bring your own devices (BYOD) is a global phenomenon, and nowhere is it more evident than on a college campus. The use of BYOD on academic campuses has grown and evolved through time. The purpose of this qualitative multiple case study was to identify the successful strategies used by chief information officers (CIOs) to mitigate information technology infrastructure demands produced by student BYOD usage. The diffusion of innovation model served as the conceptual framework. The population consisted of CIOs from community colleges within North Carolina. The data collection process included semistructured, in-depth face-to-face interviews with 9 CIOs and the analysis of 25 documents, all from participant case organizations. Member checking was used to increase the validity of the findings. During the data analysis phase, the data were coded, sorted, queried, and analyzed obtained from semistructured interviews and organizational documentation with NVivo, a qualitative data analysis computer software package. Through methodological triangulation, 3 major themes emerged from the study: the importance of technology management tools, the importance of security awareness training, and the importance of BYOD security policies and procedures. These themes highlight successful strategies employed by CIOs. The implications for positive social change as a result of this study include creating a more positive experience for students interacting with technology on campus. Effects on social change will also arise by increasing a student's mindfulness through security awareness programs, which will empower the student to take more control of their online presence and as they pass that information along to family and friends.

Strategies That Mitigate IT Infrastructure Demands Produced by Student BYOD Usage

by

Martha Jane Dunne

MS, University of Phoenix, 2009

BS, University of Phoenix, 2006

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2019

Dedication

I dedicate this work to my husband, Edward, the tall blond British guy who means the world to me. Thank you for helping me achieve my dream. We might be from two countries, but we share one heart. Thank you.

I also dedicate this work to our daughter, Jennifer Rose, the heart of my heart. I know there were times that I was unavailable, and yet you forgave me – every time. Your understanding and support mean the world to me. Leah, it took a long time to find you and we are so very happy that you have joined our family.

To friends and family that have offered support and words of encouragement over the years – thank you.

Acknowledgments

Thank you, Dr. Gail Miles, my committee chair and mentor, for all of her help along this journey. Your encouragement came when I needed it, and the gentle pushes were invaluable. I would also like to thank Dr. Steven Case for all of his help along the way. The length of time this journey took is probably longer than any of us expected. So thank you, Drs. Miles and Case for helping me achieve a dream. Dr. Gary Griffith, thank you for serving as my URR. Thank you all for your feedback; it helped make the final product better. Thank you, Dr. Alison Wiers for being the mentor you are.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Background of the Problem

The bring your own device (BYOD) movement came into being as the cost of a smartphone became an acceptable expense, and the proliferation of smartphones became widespread among teens and adults. As of 2016, 72% of U.S. adults owned a smartphone (Poushter, 2016). For this study, the definition of *BYOD* is bringing one's personally owned device to class and connecting to the educational institution's information technology (IT) resources to facilitate classwork, research, and other tasks associated with education. BYOD use by students addresses several of their needs: mobility, engagement, and retention. The transition from the information age to the connected age has allowed for unprecedented opportunities regarding connectivity via smartphones, iPads, laptops, tablets, and watches (Bichsel, 2015).

In addition, BYOD has created an atmosphere that is conducive to learning, working, and collaborating on a scale never seen before (Bichsel, 2015). However, BYOD does bring its own set of IT challenges regarding security, support, and IT infrastructure-related concerns. The IT infrastructure issues associated with BYOD include adapting local infrastructure to accommodate more devices, different types of devices, and predicting new technology and its demands and growing current infrastructure to allow institutional systems to work on a wide-range of user-provided technology (Jarrahi, Crowston, Bondar, & Katzy, 2017). In addition, there is a need to ensure the integrity and security of the network, institutional data, and educational assets.

The tech-savvy college student is actively embracing the BYOD phenomenon as many carry multiple devices (Bichsel, 2015), and as the number of mobile digital devices grows on college campuses, so do the associated demands (Jarrahi et al., 2017). On most campuses, the individual charged with mitigating the demands associated with BYOD is typically the senior IT person whose title may be the chief information officer (CIO) or the chief technology officer (CTO).

Problem Statement

Approximately 2.5 billion mobile digital devices were expected to ship during 2015 (Hsiao & Chen, 2016). The combination of digital devices and communication technologies have brought about an information revolution on college campuses that requires addressing (Chitanana, & Govender, 2015). Student use of BYOD has affected network architectures as students typically carry multiple devices that naturally are always powered on, attempting to access campus Wi-Fi and simultaneously transferring data (Chitanana, & Govender, 2015). Always online and always connected is the new norm (Vorderer, Krömer, & Schneider, 2016). The general IT problem that I addressed in this study was the increased consumer usage of multiple mobile devices on campuses continued to expand with little to impede its progress, straining IT infrastructure. The specific IT problem that I addressed in this study is that some community college CIOs lack strategies to successfully address the challenges of increasing mobile usage demands by student devices.

Purpose Statement

My purpose in this qualitative multiple case study was to explore the strategies used by community college CIOs to successfully address the challenges of increasing mobile usage demands by students and their devices. The population for this case study was composed of community college CIOs within North Carolina who have strategies to address the challenges of increasing mobile usage demands. CIOs are accountable for implementing the appropriate stratagems to ensure the college's IT infrastructure remains operational while meeting institutional requirements. For this research study, community colleges in North Carolina were the individual cases, and the North Carolina community college system was the single collective study. The inferences for future IT practice include the potential to impact how future IT innovations are managed by community college CIOs. The implication for positive social change centers around the potential for increased student engagement resulting from the enhanced capabilities necessary to access and complete coursework, anywhere, anytime, on any device.

Nature of the Study

A review of current literature indicates that the selection of a methodology, which can facilitate research, is of paramount importance to a researcher as the method chosen provides direction while also standardizing the investigation (Harland, 2014). Qualitative research is an exploration of the essence of a phenomenon coupled with the real-life experiences of individuals and their interaction with a phenomenon in a natural environment (Cronin, 2014). I chose qualitative research as I wanted to discover, from research participants, what were their motivations for selecting the strategies they did,

their opinions of the approach they did put into place and how the stratagems helped them to meet the challenge of increasing mobile usage demands on their campus. Quantitative research is used to test hypotheses and observe the transformation brought about by a change between variables based on altered values (Lynch, Barrett, Stretesky, & Long, 2017). I did not choose the use of quantitative methods for this research study because this study did not involve testing a theory or hypothesis, nor was the collection of numerical data a primary factor in this study. Kachouie and Sedighadeli (2015) noted that a mixed methods study includes both quantitative and qualitative approaches in a concurrent, yet independent, method to generalize findings and to understand a phenomenon. A mixed-methods methodology was inappropriate for this study because it involved a quantitative approach, and I was not seeking to test a theory or hypothesis. After identifying the major themes in research, qualitative, quantitative, and mixed methods and how each could be to study my topic, I chose to use qualitative research methodology as my research platform. Qualitative research permitted me to explore the strategies of North Carolina Community Colleges CIOs/CTOs as they implement protocols to strategically address the challenges brought about by the increasing mobile device usage demands associated with BYOD.

After reviewing qualitative research methods, I chose a case study methodology as the most appropriate design for this research study. As a researcher, I wanted to delve beneath the surface of BYOD to identify the successful strategies used by CIOs to address and meet the requirements of BYOD on campus as well as ascertain their opinions and motivations. According to Yin (2014), a classic case study is an inquiry of a

phenomenon within its real-world context. A researcher using the case study format does not seek to manipulate the behavior of research participants, but case study methodology can be used to explore answers regarding the how and why of the phenomenon (Baxter, & Jack, 2008). A multiple case study format forms the basis of this study. Fletcher, MacPhee, and Dickson (2015) asserted that a multiple case study often reveals characteristic features of the phenomenon under investigation, whereas Gaikwad (2017) argued that a multiple case study allows a researcher to analyze each case individually and then across the cases. Cross case analysis may provide additional complexity as the overall argument uses a variety of empirical evidence (Gaikwad, 2017). For this study, the community colleges of NC were the individual cases, and the NC community college system was the single collective study. Harland (2014) maintained that in a higher education setting, a case study may have additional beneficiaries such as students and colleagues as well as potentially influencing practices in higher education. A qualitative multiple case study was chosen as the most appropriate for this research because a case study will allow greater insight into the strategies being employed by CIOs to successfully manage the BYOD phenomenon and its impact on community college IT infrastructure.

For this study, CIOs of community colleges serve as a cultural group, and the CIOs share a common language; however, it would be impractical to execute an immersion opportunity. Lichterman (2017) observed that an integral part of ethnography design is to study people and their culture to discover the shared patterns of behavior, beliefs, and language within a culture. Therefore, I did not choose ethnography as the design of this

study. Adams, Yin, Vargas Madriz, and Mullen (2014) identified a phenomenological approach as one that would elicit responses regarding lived or shared experiences instead of rationalizing the experience after it has taken place. However, with this study I sought answers to the how and why questions of the phenomenon, not the shared experiences, phenomenology was not the right choice for this study, my focus was on the identification and exploration of strategies used by community college CIOs to ensure the college's IT infrastructure could support the BYOD demands of students.

Research Question

The research question for this study was: What strategies do community college CIOs use to strategically address the challenges of increasing mobile usage demands directly related to BYOD on campus?

Interview/Survey Questions?

1. Overall, what do you see as challenges resulting from individuals bringing multiple digital devices with them to campus?
2. Which of these challenges is affecting your campus network? What steps have been taken to mitigate the challenges?
3. What successful strategies are you using to reduce the effects of mobile usage demands on campus?
4. How did you identify and select the successful strategies for reducing the effects of mobile usage demands on campus?
5. How did you implement the successful strategies for minimizing the effects of mobile usage demands within your campus network?

6. What challenges did you encounter in implementing the strategies to reduce the consequences of mobile usage demands?
7. How did you manage the challenges faced in implementing the strategies to minimize the effects of mobile usage demands?
8. What strategies are most effective in reducing the effects of mobile usage demands on campus?
9. What factors influence the implementation of strategies to minimize the effects of mobile usage demands on campus?
10. What additional information, documentation, or processes would you like to share that may help in this research study?

Conceptual Framework

The theoretical underpinning my study was Rogers's (2003) diffusion of innovations (DOI) theory. Rogers's DOI theory has been and is widely used in the social sciences (Matthews, 2017). As a change model, DOI theory uses communication across peer groups can accelerate the acceptance of the innovation, how the innovation spreads, and at what rate (Rogers, 2003). Researchers on IT adoption have used the DOI theory to understand the propagation of information (Zhang, Yu, Yan, & Spil, 2015), the diffusion process rarely varies across disciplines (Mehmood, Barbieri, & Bonchi, 2015; Rogers, 2003; Uchida, 2015).

Rogers (2003) determined that DOI theory was the "process by which an innovation is communicated through certain channels over time among members of a social system" (p. 5). Within the diffusion process, four primary attributes occur,

including innovation, communication, channels in the course of time, and social system (Rogers, 2003). In addition, DOI primarily contends with categories of adopters, characteristics of an innovation, and the innovation decision process (Rogers, 2003). Rogers's (2003) model includes five types of adopters: innovators, early adopters, early majority, later majority, and laggards. Rogers's DOI theory also consists of five characteristics of innovation: observability, relative advantage, compatibility, trialability, and complexity (Rogers, 2003; Zhang et al., 2015). These characteristics, as perceived by members of a social system, can help determine an innovation's rate of adoption and explain why some changes are very successful and others less so (Rogers, 2003).

Rogers (2003) asserted that the two major communication channels, mass media channels, and interpersonal channels, had an impact on the diffusion process (Rogers, 2003). In addition, time factors within the innovation-diffusion process, innovation adopter categories, and the subsequent rate of adoption (Rogers, 2003). A social system is made up of a group of people or business units that are involved in a joint problem-solving exercise to realize a common goal. As such, DOI theory will help provide the necessary insight to investigate the strategies that CIOs use to manage adequately the student BYOD demands that are being placed on community college IT infrastructure.

Definition of Terms

Bring your own device (*BYOD*). Refers to individuals bringing their personally owned mobile device (smartphone, laptop, or tablet), which has applications and embedded features that allow the individual to engage in learning, anywhere, anytime (Song, 2016).

Chief information officer (*CIO*). The CIO "oversees the people, processes, and technologies within a company's IT organization to ensure they deliver outcomes that support the goals of the business. CIO plays a key leadership role in the critical strategic, technical, and management initiatives" (Gartner, CIO, 2018).

Chief technology officer (*CTO*). The CTO has the overall responsibility of "managing the physical and personnel technology infrastructure including technology deployment, network, and system management, integration testing, and developing technical operations personnel" (Gartner, CTO, 2018).

Diffusion of innovation (*DOI*). A methodology created by Rogers (2003) to understand the factors of communication, innovation attributes and awareness of an innovation that contribute to the acceptance or rejection of the innovation within a cultural group (Mannan, Nordin, Rafik-Galea, & Rizal, (2017).

Mobile device. A laptop, personal digital assistant, smart phone, or tablet (Briz-Ponce, Pereira, Carvalho, Juanes-Méndez, & García-Peñalvo, 2017; Sung, Chang, & Liu, 2016).

Mobile learning. The use of a mobile device to access information when it was needed, when the individual wanted to access the information, often referred to as anywhere, anytime learning (Alhassan, 2016; Briz-Ponce et al., 2017).

Smart mobile devices (*SMD*). Smartphones and tablets which combine computing and communication features into one device (Shraim & Crompton, 2015).

Assumptions, Limitations, and Delimitations

Researchers, in the course of their research, make assumptions, and these assumptions are thought to be accurate but research as yet to verify the hypothesis (Hollinger, Yerramalli, Singh, Mitra, & Sukhatme, 2015). Assumptions, once made, provide researchers with the framework that subsequently influences the research process itself as well as aiding researchers in protecting themselves against their prejudices (Hollinger et al., 2015). Researchers can build new ideas and concepts from assumptions. This study included several assumptions.

Assumptions

My first assumption was that the CIOs or CTOs of North Carolina community colleges have already decided to adopt BYOD on their respective campuses. My second assumption was that the North Carolina Community College System Office was aware of and provided input into the decision by individual community colleges to implement BYOD. The third assumption was that the target sample sought for this study were representative of organizational decision-makers as a population regarding their attitudes toward the adoption and implementation of BYOD. Each member of the target sample had an equal opportunity to complete the survey, thus ensuring the randomness of the target sample. The fourth assumption was that the survey participants would give complete and honest answers as there was no fear of reprisal and collection of their personally identifiable information (PII). The fifth assumption was that the individual community colleges allow students to bring their individually owned digital devices to campus and access the community college network or IT infrastructure.

Limitations

Limitations are weaknesses that may have an undesirable impact on the study and which not under the control of the researcher (Berbary, 2014). The study was geographically limited as it will only include community college CIOs or CTOs from North Carolina. Selecting only individuals from community colleges within North Carolina could result in findings that might not be generalizable beyond the specific area where I conducted the study. This study was limited explicitly to the successful strategies used by community college CIOs to manage student BYOD demands being placed on community college IT infrastructure. Should a participant not have any expertise in BYOD, that would be reflected in the semistructured interview and could ultimately negatively affect this study.

Delimitations

Delimitations, as well as limitations and assumptions, were reflected in the development of this study. Delimitations are boundaries imposed by the researcher to limit the scope of a research study (Bhat, Gijo, & Jnanesh, 2014). A researcher uses scope to establish the parameters of a study while narrowing its focus (Berbary, 2014). The scope of this study included CIOs of North Carolina community colleges, whose campuses permitted the student use of BYOD on campus and who had successful BYOD strategies in place. The first delimitation for this study was the identification of strategic approaches put into place by community college CIOs to successfully address the challenges of increasing mobile usage demands brought to bear on campus networks by the increasing number of mobile devices on campus. The second restriction was that the

study participants were limited to the geographical area of North Carolina and, more specifically, community college CIOs or CTOs. Other delimitations include the problem under study and how data was collected. Data collection was accomplished via an initial survey, recorded semistructured interviews, and documentation provided by CIO or retrieved from the campus websites that related to BYOD on campus.

Significance of the Study

Contribution to Information Technology Practice

This study was significant as it has the potential to impact how CTOs and CIO successfully address the BYOD phenomena and its associated issues on their campus. This research may assist in the identification of areas on campus where BYOD has yet to be addressed by CIOs and CTOs. The information gathered by this study allows other institutions and companies to become better prepared to face the same challenges as college students' transition from student to employee in a commercial world. Identifying best practices on a college campus can easily translate into viable solutions for other educational entities or companies, possibly leading to cost reductions while encouraging reinvesting in future IT environments.

Implications for Social Change

Today's educational institutions are coping in a world that is very different from the more traditional one of years past. Traxler (2016) argued that students and colleges alike are undergoing an identity transformation, in that the norms no longer exist for an increasingly mobile and connected society. The current student population, which is rife with non-traditional students who expect the experience to be on their terms, not

mandated by classroom structures and college policies that are outdated. With the influx of student devices onto campuses, CTOs and CIOs are looking into how much visibility into the devices is necessary and do they know which student devices are connecting to the institution's network and for what purpose. Another avenue of investigation is the support available for which mobile devices and operating systems. This research may also be beneficial to students in that the successful strategies put into play by CIOs may lead to increased personalized student-centered learning. This activity could then lead, in turn, to increased motivation by students to succeed at their coursework, which, in turn, could improve the student's economic future.

A Review of the Professional and Academic Literature

The objective of this qualitative research study was to identify what strategies are used by CIOs and CTOs to manage the BYOD phenomena successfully on community college campuses. I used a qualitative collective case study to study the successful stratagems employed by CIOs and CTOs at community colleges within North Carolina. As such, I focused specifically on the strategies community colleges use to successfully address the challenges of increased mobile use demands on campuses. I identified the literature compiled for this review through comprehensive online library search methods. Among the journal, databases searched, one generating the most relevant results were ProQuest, ACM, IEEE, AIS, Science Direct, Emerald, EBSCOhost, Google Scholar, SAGE, and Walden University Library and included articles within the last five years. The search included the following keywords: BYOD, Diffusion of Innovation theory, security, infrastructure, mobile devices, and mobile learning. The researcher accessed a

multitude of other databases in the search process, as well. Before generating the returns, the peer-reviewed feature was selected, ensuring that all of the literature viewed would fit this designation. I reviewed current literature containing empirical research in the relevant areas, which appeared in a wide range of publications, such as Research in Learning Technology, Information and Knowledge Management, Journal of Management Information Systems, The Global E-Learning Journal, and Information Systems Education Journal. Additionally, once I identified primary authors, the corpus of their work was reviewed for other relevant research, an examination of other works cited by those authors' revealed topics that could further support my research, and the process continued. At this point, 96% of the references used in the literature review of this doctoral study are peer-reviewed, and 93% are within five years of my expected graduation date of 2019.

Table 1

Summary of Research Articles Consulted in Literature Review

Sources from a review of the professional and academic literature	Number
Total references in literature review	101
Total peer-reviewed references in literature review	97
Total peer-reviewed in literature w/in 5 years	90
% peer-reviewed references in literature review	96%
% peer-reviewed references in literature review % w/in 5 years	93%

The literature review begins with the conceptual framework chosen for use during this study, Rogers's (2003) diffusion of innovation theory. What follows is an examination of the current research regarding BYOD. Within the literature review regarding current research on BYOD, I discuss the following topics; BYOD and education, BYOD risks, network overload, IT purchasing, security, security frameworks, and BYOD strategies.

Diffusion of Innovation (DOI) Theory

The conceptual framework selected for the study was Rogers's diffusion of innovation (DOI) theory, which he developed in 1962 and, as such, is one of the oldest social science theories. Rogers (2003) defined diffusion of innovation as a "process by which an innovation is communicated through certain channels over time among the members of a social system," and "is a special type of communication, in that the messages are concerned with new ideas" (p. 5). Within Rogers's DOI theory, there are five facets: the change model, communication, adopter categories, attributes, and the innovation-decision process.

Change Model

Rogers's (2003) DOI theory is considered a change model in that communication, especially within peer groups, can accelerate the acceptance of the innovation, how the innovation spreads, and at what rate. As such, the use of DOI can play a role in the adoption of new behaviors that may aid the development of the strategies necessary to manage BYOD. Within DOI theory, Rogers (2003) asserted that a product or idea could increase in popularity and acceptance by the use of group communication within a

specific population or social system. The goal at the end of the diffusion process is that the populace or social group will adopt the new idea or product. Doyle, Garrett, and Currie (2014) noted that DOI theory is particularly useful in that DOI offers support in the planning and adoption of new technologies.

Given that DOI uses word of mouth and personal experiences to assist in the diffusion of knowledge and applications, this applies to the proposed study. Within community colleges in North Carolina, the student populations at these campuses vary from 2,000 to over 50,000 students per year. As such, the technology varies as does the technical expertise of the colleges' IT staff.

Communication

Rogers (2003) described two forms of communication: mass media and interpersonal. Cheboi and Mberia (2014) referred to these channels as localite and cosmopolite. The term mass media communication can be used to describe those avenues that reach out to numerous individuals at one time, such as the Internet, television, newspapers, blogs, and radio (Cheboi & Mberia, 2014; Rogers, 2003). Rogers (2003) posited that interpersonal communication is communication that is directed to individuals and is more effective in influencing one to adopt an innovation, especially from someone deemed to be on par with themselves. Communication takes place between individuals who discuss the innovation, which can then be used to inform other potential adopters as well as share information about the change to reach a common understanding (Rogers, 2003). According to Rogers (2003), the process of diffusion between individuals or groups takes place under the following conditions; a) an innovation exists; b) when

someone wishes to impart knowledge of or about the innovation; c) when someone unaware of the change discovers it; and d) a means of communication exists between the two individuals. Ferreira and Lee (2014) noted this diffusion should be on track with increases in satisfaction or dissatisfaction within the group. Interpersonal communications have more impact when imparting disappointment with innovation rather than satisfaction with it (Ferreira & Lee, 2014). Rogers's (2003) Diffusion of Innovation is quite clear on the importance of communication. Voicing an opinion is a part of human nature; we discuss what we like and what we do not like sometimes without realizing the impact of such discussions.

Rogers (2003) found that the diffusion process rarely varied even across disciplines. Works by Doyle et al. (2014) and Franceschinis et al. (2017) support Rogers's (2003) concept of diffusion. Doyle et al., (2014) sought to explore the validity of using Rogers's DOI theory as a guide to implementing the use of mobile devices into a nursing curriculum, while Franceschinis et al., (2017) used Rogers's approach to inform regarding renewable heating systems. As such, this concept may apply to BYOD strategies, as there are CIOs who keep up to date with technology and its implementation and uses as well as those who are less familiar. Spreading information about BYOD strategies may serve to inform those individuals less familiar with its concepts and applications.

Adopter Categories

Crucial to communication is what Rogers (2003) describes as the five adopter categories. The first group of adopters is the innovators. These are the individuals who

are risk-takers willing to seek out new technologies, new methods, and often propose a change for the sake of change (Rogers, 2003). Second, the early adopters, who habitually function as the opinion leaders of the social group, like leadership roles and may have already recognized that the change or innovation is necessary (Rogers, 2003). These individuals are willing to move forward with change as to them the innovation seems better than the product or process currently being used. The third group is the early majority, which typically adopts new ideas before the average person but will look for evidence that the proposed innovation works before they wholeheartedly accept the change (Rogers, 2003). The fourth group, the late majority, are the doubters who will not adopt change until the majority of the social group has done so (Rogers, 2003). The fifth segment of the social group is the hardest to influence. This group is often comprised of individuals who are very conservative, skeptical of change, and may never adopt the innovation (Rogers, 2003). Rogers (2003) argued that the willingness of each adopter and their inclination to implement a change would depend on his or her awareness of the innovation, their interest in and their evaluation of the change, trial of change, and ends with his or her adoption or non-adoption of the innovation. Xiong, Payne, and Kinsella (2016) studied the unique effect that one's peers played in the adoption of innovation and discovered three areas where the influence of peers have an impact on the diffusion: information, experience, and externality which underscores the precepts of Rogers's (2003) theory. Often individuals use peers as a resource when contemplating adopting innovation, and what experience the individual may personally have with the change will play a role in the decision-making process. Jahanmir and Lages (2016) sought out a

different perspective of Rogers's (2003) adopter categories when they explored the attributes of late adopters and why they might not adopt an innovation. The group dynamics that come into play within the five types of adopters, coupled with the communication that manifests itself between the groups performs a distinct role in the adoption process.

An S-shaped curve or Bell curve has often been used to depict Rogers's (2003) adopter categories over time within a cultural group. These categories of individuals each have a specific point on the S-shaped curve relating to a definite period (Peine, van Cooten, & Neven, 2017). The first segment on the S-curve is known as the innovators at 2.5%, which are then followed by early adopters at 13.5% (Peine et al., 2017). Following next is the early majority at 34% and then the late majority at 34% and finally the laggards at the final 16% (Peine et al., 2017). The use of an S-shaped curve clearly defines the natural progression of categories from innovators to laggards.

Each category of potential adopters can serve as both an adopter and as an influencer to the group behind them (Nan, Zmud, & Yetgin, 2014). The progression of influence within adopter groups and from one group to another is demonstrated via the S-shaped curve that Peine et al., (2017) used to identify the five categories of adopters. Before a potential adopter can decide on adoption, he or she must be aware of the innovation and its potential benefits (Nan et al., 2014). Sometimes becoming aware of the innovation is accomplished through communication with peers or someone who influences the prospective adopters. By using DOI to inform CIOs of strategies of

BYOD, the CIOs/CTOs will internalize the material, decide if it is right for them, and then ultimately make a decision regarding use a strategy or not.

Attributes

Attributes consist of one of the critical facets of DOI theory and often tie in with communication and the change model aspects. Innovations that are thought of as successful and are quickly adopted typically have five attributes, including a) relative advantage, b) compatibility, c) trialability, d) observability and e) complexity (Rogers, 2003). Change agents, as determined by Rogers (2003), are either someone or something supporting the innovation, are critical to the promotion of and diffusion of new technologies.

Regarding relative advantage, Rogers (2003) noted that an individual must think that innovation is better than the process or product that is currently in use. Hoehle, Zhang, and Venkatesh (2015) seconded Rogers's assertion by noting that the perceived ease of use of innovation will attract users as long as the perceived ease of use is at least equal to the ease of use of the current method. Hoehle et al., (2015), also agreed that the ease-of-use is a significant factor that can be used to assess the innovation. Redza, Nordin, and Saad, (2017) noted that communication leads to an understanding of information, which leads to comparing the relative advantage of the innovation over what is already in place. Without gaining a comparative advantage or perceived benefits from adoption, it is challenging to encourage the adoption of a change.

Compatibility comes into play as individuals consider the innovation to the existing values and needs of the individual and of the group (Rogers, 2003). Pashaeypoor,

Ashktorab, Rassouli, and Alavi-Majd (2016) found that identifying predictors that influence the acceptance of change should be done before implementing the change and that in doing so, the adoption rate increases. Xiong et al., (2016) added that the effect of peer engagement, the individual's experience with the innovation, as well as the organizational attitude and the culture, could prove to be significant in encouraging others to adopt the change, which aids in the subsequent diffusion of said innovation. Potential adopters seek out compatibility aspects of a change, ones that most closely match the adopter's needs and wants with features of the innovation. The more elements of an innovation that an individual sees as compatible with their own needs increases the likelihood of its adoption.

The third attribute of DOI theory is the complexity of the innovation (Rogers, 2003). The complexity of an innovation or the difficulty that individuals have in understanding or using the change does play a role in its acceptance and subsequent diffusion (Rogers, 2003). Both Mannan et al., (2017) and Smith et al., (2018) concurred with Rogers that perceived difficulty in understanding and using an innovation will influence a potential adopter's decision. Adopters are more likely to embrace a change if they expect it to be better than what is currently in use. Otherwise, there is no need to adopt. If an individual sees the innovation as being more complicated, it is unlikely that the individual would be able to justify a change (Rogers, 2003). When an adopter becomes aware of an innovation, they begin to assess its level of complexity and whether it will aid them. The complexity level will lead to the potential adopter taking either a positive or negative stance regarding the innovation.

Trialability is a significant part of DOI theory, in that the trialability of innovation is similar to the 'try it before you buy it' business concept (Rogers, 2003). Wang, Li, H. T., Li, C. R., and Zhang, (2016) concurred with Rogers (2003) in that if an individual or group is permitted to try or experiment with the innovation on a limited basis, there is less uncertainty surrounding the change. Trialability ensures that the individual is more likely to embrace the innovation (Rogers, 2003; Wang et al., 2016). Within the context of the proposed study, the trialability of BYOD strategies does not necessarily have to take place on every community college campus in North Carolina for it to influence the diffusion.

Observability is the fifth attribute of DOI theory and pertains to the visible results of an innovation (Rogers, 2003). Rogers (2003) noted that individuals who saw the effects of a change found it easier to adopt. Scott and McGuire (2017) also stated that when an individual can observe the results and outcomes, it increases the likelihood of the innovation's adoption. Such activity also contributes to the communication aspect of DOI theory. Seeing the results of a new process or project increases the talk (diffusion) surrounding the innovation, which increases its chance of adoption (Rogers, 2003; Xiong et al., 2016). If potential adopters can observe a trial of an innovation under consideration for approval the viability of the change is increased as well as its probability of adoption.

An organization's top management can create a positive environment that will affect the diffusion of innovation, and this comfort level may affect the organization's ability as well as an individual's ability to recognize the positive attributes of a change (Wang et al., 2016). As such, the effect of the comfort level on the positive characteristics

of an innovation has the potential to prevent the individual from accepting the change until he or she has no other recourse (Rogers, 2003). The personal innovativeness of late majority and laggards is such that they will wait to accept innovation. Furthermore, in the case of laggards, some individuals may never adopt the innovation (Rogers, 2003). However, innovators and early adopters move quickly to accept an innovation once they see the innovation as having positive attributes. An individual's inclination towards change within their domain may affect how they view and adopt change at the organizational level.

Rogers's (2003) DOI theory and case study research work well together for several reasons. The DOI theory does not manipulate any behaviors but seeks to examine the process through which a cultural group accepts an innovation (Rogers, 2003). The use of DOI theory in this study allows for more in-depth research into determining what strategies CIOs have used to manage BYOD on their campus successfully and if or how this information reaches their counterparts across the state. The diffusion process recognizes the role that someone's personal power plays in innovation acceptance (Rogers, 2003). DOI theory is knowledge-driven; it is about knowing who has the knowledge, the valued individual's opinion, and whether or not the individual's judgment is enough to overcome the uncertainty of something new (Rogers, 2003). Diffusion of innovations also takes into account that some individuals within the social group may choose not to seek information about the change, thereby ignoring the innovation (Rogers, 2003). This study with CIOs as the cultural group used DOI theory's primary

components to seek answers to the research question while not manipulating any behaviors of individuals or the innovation.

Innovation Decision Process

According to Rogers (2003), the innovation-decision process involves knowledge, persuasion, decision, implementation, and confirmation. These steps cover the entire process of diffusion of innovation and account for every step in the process. The logical progression includes where an individual discovered the innovation, formed an opinion of the change, decided to adopt the innovation or not, implemented that decision, and finally confirmed the decision (Rogers, 2003). Cheboi and Mberia (2014) found that interpersonal channels of communication play a significant role during the persuasion stage, while the cosmopolite (mass media) channels of communication were more useful in the knowledge stage. The process of diffusion of innovation is an active one as individuals must decide to adopt the change, postpone the choice or reject the innovation.

During the knowledge phase, individuals attempt to answer "what the innovation is and how and why it works" (Rogers, 2003, p. 21). Finding the answers to these three questions leads an individual to develop three forms of knowledge: awareness-knowledge, hot-to-knowledge, and principles-knowledge (Rogers, 2003). Once an individual has gathered knowledge, he or she forms either a positive or negative attitude towards the innovation. It should be noted, however, that the stance, good or bad, does not necessarily lead to adoption or rejection (Cheboi & Mberia, 2014). Now that the individual knows to move forward, he or she looks for social reinforcement from others within the social group; these opinions can affect an individual's views regarding the

innovation (Cheboi & Mberia, 2014). Although an individual may personally seek out information to answer whatever questions they have regarding an innovation, he or she will also seek input from members of their social group before making that final step to adopt.

Once the individual reaches the decision state, he or she will choose whether or not to adopt the innovation (Cheboi & Mberia, 2014). Cheboi and Mberia (2014) concurred with Rogers (2003) that if the change has a trial period, it is usually adopted quicker by individuals who want to test the innovation in their particular circumstances before making a final decision. Decisions by members of the social group are ongoing during the implementation phase, and it is essential for the individual implementing the innovation to know who among the change agents to go to for technical assistance (Rogers, 2003). Knowing who to go to for support will serve to dampen the uncertainty surrounding the innovation and may improve the innovation's chance of adoption (Rogers, 2003). The ability to approach someone within the social group who may have some experience with the change under consideration is beneficial. If this individual is willing to provide answers to questions or to show someone how the change is better the outcome can have positive results.

During the confirmation phase of the innovation-decision process, the individual is looking for encouraging support mechanisms for his decision to implement the innovation (Ferreira & Lee, 2014). However, according to Rogers (2003), a decision to adopt can be reversed if the individual is the recipient of conflicting messages. Attitudes are more critical at this juncture as late adoptions, and discontinuances occur during this

phase (Cheboi & Mberia, 2014). During this stage, an individual still has the opportunity to continue with acceptance or discontinue the use of the innovation (Cheboi & Mberia, 2014). Table 2 displays the innovation-decision stages of DOI theory and examples of the communication channels used in each.

Table 2

Communication Channels Used in Each Stage of Innovation-Decision

Innovation-decision stage	**Communication channel**
Knowledge	Mass media (internet, interpersonal, and demonstrations)
Persuasion	Interpersonal (members of same cultural group)
Decision	Trial period using innovation, mass media, interpersonal
Implementation	Interpersonal (change agents within the cultural group and early adopters)
Confirmation	Interpersonal (others within a cultural group who had already adopted the innovation (i.e., like-minded individuals) and mass media (demonstrations)

Note. Based on Rogers (2003).

Supporting and Contrasting Theories

Choosing diffusion of innovation theory for the conceptual framework of this study provides an avenue to help understand the BYOD phenomena and to uncover the strategies used by CIOs to address the challenges of increasing mobile usage demands

directly related to student use of BYOD on campus. The following section identifies theories that support and contrast the diffusion of innovation theory.

Although there are numerous theories from which a researcher can select to use, care must be taken to identify the one which will help answer the primary research question. The Unified Theory of Acceptance and Use of Technology (UTAUT) is a supporting theory. UTAUT addresses how intention and behavior towards technology evolve (Oye, Aiahad, & Abrahim, 2014; Venkatesh, Morris, Davis, G., & Davis, F., 2003). UTAUT is a valid instrument for predicting adoption behavior and addresses voluntariness and performance expectancy (Oye et al., 2014). The simplicity of UTAUT, along with its robustness, has let to UTAUT becoming a favorite used in research regarding technology adoption (Oye et al., 2014). Examples of UTAUT being employed in researching the adoption by users include: predicting multigenerational tablet adoption (Magsamen-Conrad, Upadhyaya, Joa, & Dowd, 2015); Internet banking (Tarhini, El-Masri, Ali, & Serrano, 2016); and investigating the perspectives of internet access device users (Lee, Lin, Ma, & Wu, 2017). UTAUT differs from DOI theory in that UTAUT does not include the communication stages through which technology passes before its adoption (Kiwanuka, 2015). In this study, I am interested in how information regarding successful strategies flows through the cultural group of CIOs. I chose to use DOI instead of UTAUT as DOI can be used to explain on an individual level as well as an organizational level how innovation and its subsequent adoption occur.

Another theory that was considered but ultimately rejected for this study was the Information Systems Success Model (ISSM), which was developed by DeLone and

McLean in 1992 to highlight a dependent variable known as Information System (IS) success within IS research (DeLone, & McLean, 2003). ISSM is a top-down process model which is then pushed down from the organizational level to users, this exposure to the IS product has an impact either positive or negative on the user's work product which can then impact the organization (DeLone, & McLean, 2003). ISSM incorporates system usage as a factor in user satisfaction and vice versa (Gan & Balakrishnan, 2017). This study was not seeking information on user satisfaction. In contrast to DOI, the ISSM theory lacks a holistic approach as it offers a more autocratic method of technology acceptance (Gan & Balakrishnan, 2017). Examples of ISSM used in researching adoption by users include online group-buying (Hsu, Chang, Chu, & Lee, 2014); and e-commerce in Kuwait (Rouibah, Lowry, & Almutairi, 2015). The ISSM model was not appropriate for this study as an evaluation of the IS systems of North Carolina Community Colleges is not the desired outcome.

The Diffusion of Innovation (DOI) theory has been widely used over the past several decades within empirical research, thus proving its functional value to a myriad of disciplines. Examples of DOI theory used in other fields include; addressing education instruction (Scott & McGuire, 2017), Danish eldercare (Langergaard, 2017), sustainable energy technologies (Hyysalo, Johnson, & Juntunen, 2017), and farming in Malaysia (Redza et al., 2017). After reviewing some theories, I selected Rogers's (2003) diffusion of innovation theory as the underlying framework for this study. It presents a more holistic manner in which to look at BYOD strategies used by CIOs/CTOs to address the challenges of increasing mobile usage demands directly related to student use of BYOD

on campus. The questions that DOI raises; how, why, and at what rate new ideas spread through cultures remain both current and timely. The next section includes a discussion of the themes discovered during a review of the literature surrounding the BYOD on campus phenomena.

Bring Your Own Device

BYOD has become a favorite buzzword on the campuses of many educational institutions. Students have brought the phenomenon of BYOD to educational institutions by students bringing their personally owned digital devices, such as smartphones, tablets, or e-Readers, to campus to expedite their personalized learning experiences (Farley et al., 2015). BYOD can result in the need for an educational entity to review its technology support plans as well as policies involving internet access. It takes a significant amount of commitment by an institution to take on the BYOD challenges needed at the infrastructural and pedagogical levels (Farley et al., 2015).

Understanding the roots of BYOD requires an examination of the role and effect of history on BYOD. The father of radio is considered by many to be Guglielmo Marconi (Smith-Rose, 1967). Marconi was the first to produce and prove that radio waves were capable of traveling over long distances (Smith-Rose, 1967). Such technological advances were instrumental in the subsequent development of the first wireless network, built in Germany in 1958 (Smith-Rose, 1967). In 1899, Marconi sent a radio telegraph transmission across the English Channel, and in 1901 a subsequent broadcast traveled from England to St. John's, Newfoundland, Canada (Smith-Rose, 1967). The next several

decades brought about many changes that would ultimately herald the phenomenon of BYOD.

The early 1980s introduced the first cellular network, based on narrowband analog systems, and it was used primarily for cars (Andersen, 2017; Fettweis & Alamouti, 2014). In 1982, the Groupe Special Mobile (GSM) began as a working group, where it approved the 900 MHz band for mobile communications (Andersen, 2017). By1993, mobile communications has received approval to operate on the 1800MHz band, which led to the first cellular 2G call connection (Andersen, 2017). The second generation allowed the use of both digital audio signals and text messaging (Fettweis & Alamouti, 2014). During the third generation, a different protocol was used to scale the network to accommodate the increasing number of users demanding both voice communication and text messaging (Fettweis & Alamouti, 2014). However, users would discover imaging and video content, which further taxed the networks, leading to the fourth generation (4G) of mobile communication (Fettweis & Alamouti, 2014). As the world becomes more engaged in 4G discussions and beyond, there is a need for technology organizations to provide capacity as well as an efficient and smart architecture that can accommodate today's demands and those of the future (Fettweis & Alamouti, 2014). The advent of users adopting voice communication, text messaging, imaging, and video content is a clear demonstration of the diffusion of innovation theory in action.

Marconi's scientific and technological breakthroughs set the stage for subsequent advancements in wireless connectivity, networks, and in the field of communications.

Mobile communications and mobile computing have evolved from the age of being able to communicate over short distances via electromagnetic waves to the digital era (Andersen, 2017). Individuals are now able to communicate via smartwatches, smartphones, or other digital devices by connecting to wireless networks allowing access to the Internet or a private virtual network (VPN) (Andersen, 2017). Other consequences of mobile devices include the meshing of social, business, and educational aspects of individuals' lives and the shrinking of the world's virtual space (Ally & Prieto-Blázquez, 2014). The furtherance of technology continues to affect businesses, social structures, and education.

BYOD and Education

The advancement of mobile technology offers institutions of higher education opportunities to access to a broader student population (Al-Emran, Elsherif, & Shaalan, 2016). The assimilation of technology media and its associated services into colleges are leading to significant changes that are impacting how both students and teachers study and learn (Song & Kong, 2017). No longer are students required to reside on campus or commute to school to fulfill their educational dreams (Al-Emran et al., 2016). The introduction of portable, mobile technologies is changing the educational landscape, wherein students are now using their mobile devices to access coursework anywhere and anytime (Ally & Prieto-Blázquez, 2014). Educational entities are merging technology with education to offer classes to students online, benefiting not only those students who may live near campus but thousands of miles away. Improvements in mobile

technologies have students bringing laptops, notebooks, and cell phones to their campuses. The associated impact of BYOD was the underlying construct of this study.

One of the benefits most often attributed to BYOD in conjunction with education is the assessability to content for students at any time from anyplace (Sundgren, 2017). Accessing content anytime from anyplace is known as opportunistic learning, and it takes advantage of the requirement for learning anywhere, anytime, anyplace by permitting students to use those short, fundamentally unproductive segments of time (commuting, waiting to see physician, etc.) to access class content (Sundgren, 2017). Which, in turn, allows the student to be in control of when and where they learn rather than waiting to attend class to learn (Sundgren, 2017). Studies by Dündar and Akçayır (2014), as well as Cheng, Guan, and Chau (2016) point out that students' use of BYOD may encourage the user in the development of their digital literacy skills. Students' use of BYOD may provide opportunities to increase individual skills in such areas as critical thinking, problem-solving, and collaboration (Cheng et al., 2016; Dündar & Akçayır, 2014). The increased cognitive skills arising from learning anywhere, anytime, anyplace may have far-reaching benefits for students in their school, work, and social lives. The convenience of retrieving information when it is needed, the accessibility of such information, and the overall utility of a mobile device itself that can offer communication and computing capabilities to its user, improves acceptance (Briz-Ponce et al., 2017; Shraim & Crompton, 2015). BYOD offers control of where, when, and how one learns to students, and both students and educational entities are embracing the practice. Students who chose

to use BYOD have a range of devices, smartphones, laptops, netbooks, and tablets from which to choose.

The use of a smartphone or other smart mobile device (SMD) allows a student to easily switch from accessing personal or private websites to the more public sites associated with their institution of higher education (Ilic, 2015). Smart devices often come with some interactive software applications pre-installed, or these types of software applications are readily available for free or a nominal fee. Such applications make SMDs a highly customizable yet personalized device that can access the internet for browsing, social media engagement, or communicating with friends and family. Students use such an SMD to collaborate with classmates, which in turn enhances both formal and informal learning (Shraim & Crompton, 2015). A dedicated device such as a desktop computer is no longer the only way to access family, friends, school, or business associates. Mobile devices have changed the technology landscape.

Ally and Prieto-Blázquez (2014) assert that learning via mobile technologies will change the learning dynamic from the traditional classroom to one that is more in tune with the learners' environments and become more situational, personal, foster increased collaboration, and continue throughout their lifetime. However, in contrast, Fielding's (2016) study indicates there is some disillusionment with the rhetoric surrounding BYOD's anytime, anyplace, anywhere paradigm due in part to a feeling of isolation on behalf of students. As a counterpoint, Fielding (2016) suggests BYOD courses be modified to incorporate an opportunity for students to document, with others, how the course fits into their lives while improving student engagement. Although mobile

learning has proven to offer benefits relating to students' engagement and retention of information, educators have shown reluctance to implement mobile learning initiatives within their courses (Alrasheedi & Capretz, 2015). As a counterpoint, Adhikari, Scogings, Mathrani, and Sofat (2017) noted that as teachers obtain and become familiar with emerging digital technologies, they become more comfortable with the technology. It is at this point educators will then begin to integrate the technology into their classes, which could then enable a change in the pedagogical practice at their institution (Adhikari et al., 2017). A scenario where educators integrating digital technology into their classes become innovators to their colleagues who, subsequently the technology into their courses is an example of diffusion of innovation theory in action.

A campus BYOD environment is not stagnant; it can be affected by several issues. Infrastructure, campus culture, perception, as well as institutional and organizational problems, can influence the use of BYOD on campus (Spangler, Rodi, & Kiernan, 2016). As educational entities try to adapt and adopt new technologies, an additional financial burden is being placed on already trimmed operating budgets (Spangler et al., 2016). This financial burden also increases the drain on resources both in technology and people. With wireless networks, Higher Education institutions can cut costs related to cable infrastructure while offering improved flexibility to its networks, and also, the wireless network can be scaled rather quickly compared to the typical cabled network (Liao, Luo, Gurung, & Shi, 2015). As campus wireless networks grow and allow personally owned digital devices to connect, the opportunities for cyberattacks also increase.

Mobile devices, without appropriate security measures in place, are vulnerable to attacks and, if infected, may pass along an attack when the device attempts to connect to a network. Educational entities are prime targets for cyber threats (King & Evans, 2016). Higher education entities are in a *catch-22* situation in that their networks are expected to be accessible by students, their parents, and the institution's staff and faculty, while striving to protect their business assets from the same threats that apply to the commercial and government sectors (King & Evans, 2016). According to a study released by Symantec, in 2016 the education sector rose to the second-highest spot of most targeted threat areas due in part to the amount of personal information retained by educational entities on both staff and students (King & Evans, 2016). As this study was conducted on community college campuses and involves identifying successful strategies for mitigating BYOD demands, it is essential to know and address potential vulnerabilities.

Connectivity

A variety of networks, such as Local Area Networks (LAN), Metropolitan Area Networks (MAN), Wide Area Network (WAN), Wireless Local Area Networks (WLAN) and Dense WLANs) may peacefully coexist on an educational campus (Debele, Meo, Renga, Ricca, & Zhang, 2015; Jothi, Rashid, & Husain, 2015). A computer network must have at least two computers and a communication channel that would allow computers to share resources and information (Jothi et al., 2015). As the network expands, so do the requirements for communicating. These requirements are known as networking protocols and use a standard format and a set of rules to define how to exchange messages between devices (Medhi & Ramasamy, 2017). Bandwidth becomes necessary for all of the devices

within the network to communicate with each other (Paredes & Hernandez, 2018). Bandwidth represents the capacity of the connection and the supported data rate of the network connection or interface. A higher capacity bandwidth is necessary to achieve greater communication performance (Jothi et al., 2015).

There are network-specific techniques for bandwidth management that are in use in higher education institutions that are both expensive and resource intensive (Chitanana & Govender, 2015). Examples of bandwidth management techniques include bandwidth allocation and scheduling (Paredes & Hernandez (2018). Chitanana and Govender (2015) suggest that higher education institutions should develop IT policies to include an internet access policy that promotes and refines bandwidth access and usage. Chitanana and Govender (2015) also noted that such a strategy has no value or standing unless the course of action is communicated and enforced.

Typically, on college campuses, individuals have two ways to connect; wired or wireless. The purpose of this study was to successfully address the challenges of increasing mobile usage demands directly related to BYOD on-campus wireless networks become an integral part of the conversation. The data carried over wireless networks has seen a tremendous amount of growth in recent years, and a 1,000 fold increase in data traffic for 2020 and beyond is expected (Al-Falahy & Alani, 2017). IEEE Standard 802.11xx continues to set the stage for the development of wireless LAN (Wi-Fi). Approximately 70 percent of traffic from mobile devices occurs indoors using small cells/hotspots (Al-Falahy & Alani, 2017). To meet the demands of such hefty data increases, many are looking to 5G mobile networks as part of the solution. A 5G mobile

network is expected to have higher capacity and higher data rates than a 4G mobile network (Al-Falahy & Alani, 2017). An access point provides a connection to the campus network through a WIFI connection point. Increasing the number of APs can improve connectivity and overall throughput of the networks' signal if the APs are positioned correctly to enhance coverage, not just mirror what is already covered (Ali, Razak, Amran, Salim, & Tahir, 2016). Increases in the amount of data being carried on wireless topology and the further development of wireless networks mean new topologies such as 5G and improved performance from APs are a must if the momentum is to be supported.

Although an individual may be using a digital device with a 3G/4G supported network, the device may attempt to connect to a Wi-Fi AP (Al-Falahy & Alani, 2017). Insufficient bandwidth can cause WLAN accessibility issues for students, staff, and faculty alike. Bandwidth management can offer faster applications, a reduction in the number of chokepoints or bottlenecks, and compressing traffic, thus increasing better control of the network (Noughabi, Far, & Raahemi, 2016; Paredes & Hernandez, 2018). Increasing bandwidth will provide better speed performance. Determining the amount of broadband connectivity that is needed by an organization requires; 1) analyzation of the current network usage; 2) identifying which applications are necessary, and 3) evaluating the network workload (Alhassan, 2016; Ali et al., 2016). An integral part of identifying the amount of connectivity necessary involves determining the number of students accessing the network within a predetermined amount of time (Ali et al., 2016). One must monitor network performance before, during, and after a broadband implementation to ensure the network capabilities are right-sized (Alhassan, 2016). While taking steps to

ensure that a network is right-sized for the population accessing the system, it is imperative to plan for and build in growth potential. Garba, Abdulmalik, and Tekanyi (2015) proposed a different model for wireless campus area networks that involves the use of dynamic nodes monitored by a software program to organize a queuing system of both real-time packets and non-interactive packets. This software is capable of slowing down or stopping transmission if it notices congestion, and it will resume transmitting when the buffer is free of congestion (Garba et al., 2015). These nodes are capable of monitoring an APs status remotely and provide real-time alerts as necessary (Ali et al., 2016). Alhassan (2016) suggests educational institutions ensure the wireless network coverage is expanded to encompass all parts of the school, thus allowing students access to Internet resources anywhere on campus. Alhassan (2016) also supports educational institutions partnering with Internet Service Providers to provide high-speed services at a reasonable cost. One of the accessibility issues of WLANs is directly related to bandwidth and how to manage it. Recent advances in topologies for use with WLANs include dynamic nodes capable of monitoring the performance of APs (Alhassan, 2016). Making use of these types advances to increase the footprint of a campus' WLAN offers greater freedom on campus to access material anyplace, anytime, and anywhere on campus with a myriad of digital devices.

Network access controls (NAC) is a networking solution designed to include a set of protocols to both define and implement a policy that will allow network resources to be accessed by devices as they join the network (Downer & Bhattacharya, 2015; Vignesh & Asha, 2015). NAC can include firewalls, antivirus software, and even spyware

detection or intrusion detection. These applications and devices are meant to protect the network from external attacks (Flauzac, Gonzalez, and Nolot, 2016). Access is accomplished by limiting the availability of network resources to endpoint devices that conform to an organization's security policy. The process begins by authenticating login information. Some NAC programs require coordination between an agent on the endpoint itself, devices that deliver network access, servers that provide authentication, systems responsible for policy decisions regarding health and compliance, and elements that help enforce those decisions and remediate failures (Downer & Bhattacharya, 2015; Vignesh & Asha, 2015).

Devices

Previous generations of mobile phones offered little besides the ability to make a phone call. Today's digital device provides much more. A study by Vorderer et al. (2016) found that the smartphone now serves as a primary interface for interacting with others. The current generation of smartphones are more desirable due to its; perceived ease of use, portability, ability to make a phone call, access the Internet, access social networking sites, games free or for a fee, and a host of other applications (Tossell, Kortum, Shepard, Rahmati, & Zhong, 2015). Song (2016) notes that mobile devices are less available than television sets in homes and that this is changing due to improved accessibility gained through the use of smart mobile devices through which individuals can access the Internet. The diffusion of mobile devices has proven to be an indispensable tool for students in higher education. Put into the context of Rogers's (2003) diffusion of innovation the use of a mobile device has reached through the innovators, the early

adopters, the early majority, the late majority and into the category known as laggards, the last 16% of the population. (Dennen & Hao, 2014; Hao, Cui, Dennen, Türel, & Mei, 2017). Student's adoption of mobile devices as innovation continues to spur change. Students and their digital devices travel all over campuses, and students expect the same access, everywhere they go. Like many other colleges, North Carolina Community College CIOs are identifying and implementing strategies to meet the demands.

Smartphones are not just for making phone calls but have become a daily instrument used in an individual's personal, work, and student life. Liao et al. (2015) suggest that the use of the desktop computer has fallen behind mobile devices such as laptops, tablets, and smartphones, which offer computing flexibility and mobility. As a result of this, interweaving mobile technology has grown in importance for students' academic pursuits (Liao et al., 2015). Mobile technologies have advanced in recent years, and that advancement has led to improvements in computer software applications which has allowed many applications to transition from a desktop only app to one capable of being accessed from mobile devices such as smartphone, tablets, and notebooks (Schindler, Burkholder, Morad, & Marsh, 2017). The use of mobile technologies permits learners to reach out across boundaries to learn and engage (Schindler et al., 2017). As the demand for improvements to digital devices and associated applications continue to rise, manufacturers will strive to meet consumer demand.

BYOD Risks

With the growing trend of BYOD reaching to many campuses, it becomes incumbent upon educational entities to develop appropriate policies. One such strategy

would be to allow students to use their own devices to access information and applications associated with their coursework, wirelessly. The convenience of using BYOD and wireless services are symbiotic; the perceived ease of use of BYOD leads to increased demands for more such services (Kao, Chang, Y. C. & Chang, R. S., 2015). Although BYOD has become increasingly popular on campus, the downside is that its use may affect the security of the institution's network (Chou, Chang, & Lin, 2017). While striving to meet student demand for BYOD, secure access must be maintained. In a study conducted by Kao et al. (2015), it was discovered that over seventy percent of all wireless network usage on campus was coming from personal digital devices such as smartphones and tablets. The challenge facing IT managers is to improve the accessibility of services for students with maintaining a security posture that thwarts security attacks (Chou et al., 2017; Kao et al., 2015). Encryption of data is one method used as a risk control measure for insecure connections; however, to be effective, data encryption must also occur when bits of data are in transit and at rest (Shumate & Ketel, 2014). One of the easiest ways to hamper a student's access is through the loss of their device. There are several ways to prevent mobile devices from being lost or stolen. First, establishing a passcode would prevent anyone, not knowing the passcode, from using the device. Secondly, setting up a remote lock function would enable the owner to lock down all features of the device if the device is lost or stolen (Shumate & Ketel, 2014). There is a fine line between improving student accessibility via digital devices and ensuring the network remains secure, and CIOs must find a balance.

Malware has been an issue for mobile device owners and IT personnel alike. The growth in malicious software has paralleled the increase in mobile device usage (Briz-Ponce, & Juanes-Méndez, (2015). Many individuals and organizations perform a baseline scan before the first use of a digital device. Some organizations use white-listing to specify the resources, websites, and what actions the device can take (Shumate & Ketel, 2014). Others use anti-malware software to reduce malware on the device (Shumate & Ketel, 2014). Wireless networks are more vulnerable to attacks than a wired network, and the risks associated with BYOD include insecure connections, lost or stolen devices, malware, access, and permissions (Shumate & Ketel, 2014). The implementation of a campus wireless network requires appropriate planning and the identification of successful strategies that permit the student use of BYOD without affecting the IT infrastructure.

Network Overload

IEEE standard 802.11 guides the design of wireless local area network (LAN) protocols and has been influential in the successful operation in wireless communication systems (Kim & Lee, 2015). The adoption of IEEE standard 802.11 in 1997 has led to Wireless Local Area Network (WLAN) technology and its evolution. IEEE standard 802.11 covers band usage from 2.4GHz to 5GHz (Shi, Liu, Y., Liu, W., & Zhang, 2015). As a result of this standard being in place, improvements in transmission rates, areas of coverage, reliability, and quality of service are noticeable. For example, IEEE 802.11ac seeks to deliver gigabit rates to wireless users (Siddiqui, Zeadally, & Salah, 2015). Other areas also experiencing improvements are mobility and security (Shi et al., 2015). The

802.11ac standard contains enhancements to the physical layer of the Open System Interconnection (OSI) model, which have resulted in better reliability and a more robust 5-GHz band. The 802.11ac amendment allows for better user experience as data rates move up to 7Gbps in the 5-GHz band, which is up to 10 times the speed achieved under the previous standard (Siddiqui et al., 2015). A study performed by Rimal, Van, & Maier, (2017) found that using both IEEE 802.11n and IEEE 802.3ah for integrated fiber-wireless access produced an effective solution for both broadband and mobile backhaul. In this scenario, IEEE 802.3ah offers reliability, and IEEE 802.11n provides extended coverage and flexibility (Rimal et al., 2017). The amendments to the IEEE standard 802.11 seek to keep pace with improved technologies involving data rates, reliability along with mobility and security.

Global mobile data traffic continues growing steadily. Yang and Winter, (2015) cite a 2013 Cisco report indicating during 2012 mobile data traffic was at 884,906 Terabytes per month, and this is projected to reach 11,155,531 Terabytes per month in 2017. As the mobile data traffic continues to grow network architecture is being examined to see how it can be improved to handle the enormous amounts of data. As a result, a new network architecture comprised of both LTE-A and IEEE 802.11ac is a possible way forward for institutions of higher education (Yang & Winter, 2015). Both can achieve gigabyte per second (Gbps) speeds and when used together shows promise not only campus coverage but for student access also in the form of seamless and automatic handovers (Yang & Winter, 2015). A study into new network technology asserts that the use of IEEE 802.11 and LTE-A will offer enhanced support for 5G core

networks (Rost et al., 2016). The demands of increasing mobile data traffic have led to the development of new network architecture and enhancements of the current architecture. In some cases, this will lead to IT department purchasing hardware. However, in many cases, the IT department is losing its purchasing power for digital tools.

IT Purchasing

By 2017, over 50% of IT purchases by organizations focused on digital tools; these purchases were made by human resources, finance, marketing, and departments in the hopes of finding a competitive edge (Russell, 2016). For IT departments, this loss of control over the purchase of IT applications which has been compounded even further by BYOD, the cloud, and the Internet (Russell, 2016). The purchase of an application without bringing the IT department into the discussion may jeopardize the installation or result in network vulnerabilities. Before the advent of BYOD, IT departments maintained restrictive use policies and typically denied requests for the use of digital devices that were not owned and managed by IT personnel (Russell, 2016). Students also have IT purchasing power. With mobile devices, students can access educational entities such as Khan Academy and Harvard/MIT edX, which offer low cost or free instruction to supplement face-to-face classwork (Zahadat, Blessner, Blackburn, & Olson, 2015). Within a company or organization, it can be beneficial to bring IT departments into discussions regarding purchases that require a connection to the network; otherwise, unsecured or unauthorized products may create vulnerabilities within the network.

Security

The introduction of BYOD into organizational entities and educational institutions left many managers and IT decision-makers with the insufficient knowledge to make the judgment calls relating to information security and privacy (Bello, Murray, & Armarego, 2017). Organizations which adopt BYOD without the appropriate security protocols or protective policies in place regarding information security may experience an increased risk of losing confidential information (Bello et al., 2017). NIST suggests the use of a five-phase life cycle of initiation, development, implementation, operations, and maintenance, and disposal to assist in organizations in determining a BYOD or remote access strategy (NIST, 2016). The security of BYOD remains a challenge with the estimated compound annual growth rate of mobile traffic from 2013 to 2018 at 61 percent per annum (Sama et al., 2015). Students are bringing their devices to campus in record numbers, yet, IT staff must manage the access of such devices to campus resources. Besides, there are the regulatory requirements imposed by FERPA, HIPPA, and PCI, regarding data storage within a network and how the data is accessed (Kiernan, 2016). Each of these plays a role in BYOD security. Innocenzi et al. (2018), noted that educating students in the area of information security improves the information security posture of the entire institution.

The emergence of new digital devices and their associated technologies have ensured that BYOD has become an integral part of students' lives, and with this acceptance comes the challenges of security (Dang-Pham and Pittayachawan, 2015). Manufacturers frequently release new versions of their devices. What happens to the no

longer used devices can be a security risk. Ali et al., (2016) assert that 50% of used cellphones still contain some data from the previous owner. The owner's unfamiliarity with the device and/or poor security practices may be contributing factor to data remaining on disused cellphones. Dang-Pham, Pittayachawan, and Bruno, (2017) reference a 2015 Gartner study suggesting that developing a group culture within a workplace that provides security education while also informing about the dangers of inappropriate behaviors may improve security practices. In addition to carelessness, there are several BYOD threats to consider, such as malicious applications, an escalation of privilege attack, physical access, along with disgruntled students or employees (Ali et al., 2016). A more detailed discussion of these topics follows in the security risks section.

Security Risks

Organizations and Higher Education institutions that permit BYOD have a responsibility to address the security issues associated with BYOD and how those security issues will affect the IT infrastructure. Singh, Chan, and Zulkefli (2017) note that malware and spear-phishing are two of the top four ways to attack via BYOD. A study conducted in an academic community by Diaz, Sherman, and Joshi (2019) showed that 59% of the study participants, including those who self-identified as technology savvy would open a phishing email and click on the phishing link. To address the security issues facing institutions regarding BYOD Bello et al., (2017) suggest the use of a multifaceted policy-based management model that includes: security standards and procedures, technical controls, security awareness and training, user perception, and user behavior. Innocenzi et al. (2018), suggest implementing a campus-wide campaign that

promotes cyber security. It is incumbent upon institutions to regularly review their security and privacy controls for BYOD as a method to address technology changes as well as further mitigating the security and privacy demands associated with BYOD. As there are potential security issues that can affect BYOD, it is up to both the device owner and the CIO to be aware of the threats and take appropriate action.

Although mobile devices such as smartphones, laptops, and tablets are small enough to be easily carried they are also easily forgotten, misplaced or even stolen if an individual's attention is focused elsewhere (Tu, Turel, Yuan, & Archer, 2015). Almarhabi, Jambi, Eassa, and Batarfi (2017), indicate that over 9 million smartphones are lost or stolen each year per study produced by PricewaterhouseCoopers (PWC). Such devices, if lost or stolen, may then pose a new set of problems for their owner in the form of expected and unexpected consequences. Should a mobile device owner lose the device, he or she is without the device and may experience the loss of data that was on the device while providing others with potential access to data residing on the device (Tu et al., 2015). There are also unexpected consequences with lost or stolen devices. For example; many users fail to realize that when they delete information from a device, the data may still exist on the device.

In some cases, the device's operating system only marks the data's location as deleted meaning the information is not wholly expunged from the device (Almarhabi et al., 2017). The owner or user of a lost/stolen mobile device may experience an inability to remotely access applications that were on the device while providing others with the potential to access those same applications (Tu et al., 2015). In many instances, owners of

smart mobile devices store personal data on the device. Types of data may include the following; passwords to email accounts as well as social media accounts, documents related to school or work, and even passwords to bank accounts all of which are risky to the devices' owner (Tu et al., 2015). In the Innocenzi et al. (2018) study, the authors noted there is a lack of knowledge regarding how having a weak password and the effect it has on an individual's overall cyber security. According to Peker, Ray, Da Silva, Gibson, and Lamberson (2016), many internet users, including college students are unaware of the risks they pose to themselves by using digital devices in insecure ways. As it pertains to this study the loss of a student's digital device that he or she uses to access the campus network can potentially be dangerous in the wrong hands as the security of the system could be breached.

As BYOD has grown in popularity with employees and students, educational institutions have experienced an increase in the number of security and privacy attacks as hackers or cyber attackers seek to gain access to the educational network as well as student's personal information (Singh et al., 2017). Security threats for students using BYOD do exist as hackers, or cyber attackers seek to gain access to their digital devices. Due to increased mobility and flexibility, smartphones and tablets have become an integral part of BYOD (Singh et al., 2017). Many mobile device owners engage in risky behaviors by removing or altering the original vendor configuration or disabling the native OS security on their mobile device (Singh et al., 2017). This action may place the device owner's data stored on the device in harm's way. Another type of risky behavior occurs when an owner implements a process referred to as "jailbreaking," "root" or

"unlocking" to alter their device which permits the owner of the device to install unauthorized programs on the device (Singh et al., 2017). Not only do such actions have the potential to compromise the digital device but may affect the network to which the device connects (Singh et al., 2017). There are numerous scenarios involving mobile devices, risky behavior on the part of the digital device owner, and security risks that do not end well. Some of these scenarios come about due to personal decisions to avoid security measures that the individual may not fully understand.

Many mobile device owners have reported malware attacks, yet most users are unacquainted with preventive measures (Pinchot & Paullet, 2015). Chin, McRae, Jones, and Harris (2016) cite a Kaspersky (2015) survey that indicated nearly 30% of mobile users did not know much about mobile malware and many failed to initiate the most basic precaution of activating user authentication. Malware can compromise a mobile device. A malicious application can be transferred to a mobile device when the device owner downloads a 'free' app, not realizing it may contain malicious coding (Skovoroda & Gamayunov, 2015). Malware or malicious software was specifically developed to disrupt other software by manipulating it to obtain personal information or to access other software on the device (Skovoroda & Gamayunov, 2015). Malware that infiltrates a device is capable of capturing the device owner's contact list and the personal information associated with the contact, the device owner's email, texts, photos, etc. (Jones & Chin, 2015). Malware may appear as a legitimate piece of software which could explain why many individuals fail to realize that they may be clicking on a virus until it is too late.

Insecure security practices by users include not updating anti-virus software, allowing others to use the device, and not acknowledging the risk of using public or personal networks (Skovoroda, & Gamayunov, 2015). Unsafe security practices also include downloading apps from untrusted sources or downloading apps that request personal information (Jones & Chin, 2015). Pinchot and Paullet (2015) suggest that although a desktop computer may receive security updates regularly, the same is not always true for mobile devices. The anti-virus and anti-malware applications developed for desktop computers are more robust than those for mobile devices (Pinchot & Paullet, 2015). The prevalence of and desire for mobile technology allows for the creation of new threats to the security of organizational and personal data. To counter these insecure security practices more should be done to enhance the security stance of students.

Regularly updating one's anti-virus software reduces the chance of a device becoming infected with a malware or virus. Allowing a third party to access one's device could have repercussions for the owner of the digital device (Skovoroda & Gamayunov, 2015). The use of screen savers with passwords and the use of biometrics to authenticate the user could prevent repercussions from occurring due to the inappropriate access to personal information stored on the mobile device, and the unintended installation of software by unknown individuals (Skovoroda & Gamayunov, 2015). Biometrics are a recent addition or innovation to smart digital devices and has not reached full adoption stage yet. The use of public networks brings about its own set of challenges.

Both Wi-Fi and cellular networks have experienced an increase in strength and reliability; add in the increased availability of unsecured public Wi-Fi hotspots and users

can stay connected in a variety of environments (Singh et al., 2017). The challenges of accessing a public network are twofold; the system is open to anyone, and the data flowing through it is unsecured. However, the use of the virtual private network (VPN) allows for the encryption of data or communication flowing through it (Alshalan, Pisharody, & Huang, 2016). VPNs are typically set up to protect the resources of the internal network (Downer & Bhattacharya, 2015).To lessen such exposures Skovoroda and Gamayunov, (2015) suggest organizations establish security characteristics for mobile devices attempting to connect to the organizational network, and if any devices were not meeting those specifications the device would be rejected, and the connection would fail. It is easier than ever before to stay connected, sometimes securely, and at other times an open network is accessed as our digital devices remain with us throughout our day. There are several types of frameworks suggested for use with BYOD; in the next section, two are discussed.

Security Frameworks

In the context of IT, a security framework is a set of processes, policies, and procedures that guide how to manage IT before, during, and after its implementation. The integral parts of any BYOD security framework are people, policies, and technology. Zahadat et al., (2015) suggested that a BYOD security framework should include the following seven items: a) plan; b) identify; c) protect; d) detect; e) respond; f) recover, and g) assess and monitor. In retrospect, the process does not end with evaluating and monitoring as the method is not finite, but one that evolves to encompass new policies, technology, and people. A different perspective of a BYOD security framework has been

offered by Raj and Catherine (2015), which provides a security framework that uses a hybrid authentication system that includes authenticating the device, the service, and the user. This type of framework would involve running a malware scan on the device before allowing it to connect, using three-tier captcha in addition to verifying user id and password, which authenticates the user. The certificate mechanism in SSL confirms and enables the trust relationship (Raj & Catherine, 2015). There are different types of security frameworks available for use with BYOD; some are hybrids that allow administrators to choose components while others are very straightforward. BYOD strategies should be discussed in the same conversation as security frameworks as they go hand in hand.

An integral part of a comprehensive security framework is a firewall. A firewall can be either software or hardware and is used to monitor network traffic as well as blocking or allowing it (Ali, Hossain, & Parvez, 2015; Chopra, 2016). A firewall has two interfaces; one to protect the network from network-based security threats and one to serve as a mechanism to allow access in from the outside network and internet (Chopra, 2016). A firewall measures every piece of traffic going through it against its protocols; a match and the traffic continues, no match the traffic is stopped. Firewalls were developed to secure an organization's network and access to the protected information that resides on the network (Kruse, Smith, Vanderlinden, and Nealand, 2017).

BYOD Strategies

When an organization chooses to implement BYOD they must consider three things; what are the risks, what are the challenges, and what are the benefits. Brodin

(2017) suggests that organizations typically develop a mobile device strategy using a three-pronged approach incorporating; analysis, design, and action. Brodin (2017) proposes replacing the third item, action, with three subsets; communication, training, and adjustment. Communication is crucial in that users must understand both the purpose and benefits of the strategy if they are to buy into it (Brodin, 2017; Rogers, 2003). Training must be involved in the effective implementation of a strategy, and evaluation comes into play after determining what part of a plan is or is not working and requires adjustments (Brodin, 2017). As CIOs developed strategies for use with BYOD they found some may work from the onset; others may need modification before reaching the desired level of success while still others lacked the desired robustness. Information regarding successful BYOD strategies implemented by North Carolina Community College CIOs was a crucial component of this study.

Ensuring personally owned devices are policy compliant can be a daunting task. However, it becomes an easier task with the use of various frameworks such as mobile device management (MDM), mobile information management (MIM), and mobile application management (MAM) as alternatives to MDM. Typically it is MDM to which IT managers go first (Zahadat et al., 2015). With MDM, an individual's device becomes an employee-owned device that is controlled by organizational policy. An MDM system contains software that hosts some functions such as the distribution of software, policy management, security management, inventory management, and a variety of other tasks that help an IT department manage BYOD (Dang-Pham & Pittayachawan, 2015). Zahadat et al. (2015) concurred that the use of MDM adds a layer of protection to a

BYOD program. Two parts make up MDM – one part resides on organizational equipment, and the MDM agents sit on the user's device and will attempt to complete a handshake with the organizational MDM component to ascertain if the device's certificate meets the requirements established by the organization to access its network (Raj & Catherine, 2015). Within MDM, users are assigned to group profiles, thereby simplifying management and deployment when a change is necessary (Dang-Pham & Pittayachawan, 2015; Zahadat et al., 2015). In many instances, MDM is the framework of choice for IT managers as it relates to BYOD. MDM adds protection yet can simplify the management of BYOD.

Security management scenarios involve or include the use of MDM, MAM, and MIM, which are the primary models for provident BYOD security (Vignesh and Asha, 2015). One type of countermeasure is for educational entities to require anyone using their network via a personal device to download a free software download of MDM software onto their device (Spangler et al., 2016). The use of this software allows the user to keep personal data separate while the IT department can control how the device accesses network data. Chin et al., (2016) noted that MDM typically comes into play when a student connects their mobile device to the college's Wi-Fi or when a user adds their school email account to their mobile device.

Ali, Qureshi, and Abbasi (2015) stated MDM typically uses a client-server architecture in which the server sends policies and permitted applications to an agent installed on the user's device. Other aspects of MDM software include requiring a password, remotely locking or unlocking the device, and encrypting and decrypting data

(Spangler et al., 2016). The entrance of MDM has provided additional avenues for security as have MIM and MAM. Enhancing network security allows networks to play a more pivotal role in determining which user can access the enterprise's applications via BYOD (Spangler et al., 2016). MDM has more capabilities than MIM or MAM, although all three can be used to add a layer of BYOD security. A more recent addition to the line of technology management tools is Enterprise Mobility Management (EMM). Alotaibi and Almagwashi (2018) noted that the Enterprise Mobility Management approach is a more all-inclusive approach as it involves the use of MDM, MAM, and MIM. However, EMM also combines all of the limitations and challenges characteristic of MDM, MAM, and MIM (Alotaibi and Almagwashi, 2018).

Digital Natives and Immigrants

The use of digital devices by digital natives and immigrants continues to encourage manufacturers to improve the devices and IT leaders to enhance network capabilities. A digital native is an individual born and bred within the digital era who have no recollection of time without digital devices (Gkioulos, Wangen, Katsikas, Kavallieratos, & Kotzanikolaou, 2017). Ahn and Jung (2016) further identified a digital native as being born after the 1980s and a digital immigrant as the parent generation of the digital native. If the digital immigrant is a parent of a digital native, the parent may have originally taught the digital native how to use technology. The distinction between digital natives and digital immigrants is necessary as digital natives view technology differently than older generations, and this includes a digital native's attitudes relating to security issues surrounding the devices (Gkioulos et al., 2017). For example, even when

warned about the poor security practice of storing personal passwords on their devices, twenty-nine percent of survey respondents reported they continue to do so (Gkioulos et al., 2017). A study found that digital natives prioritize their access to services and the ability to use their device over security measures (Gkioulos et al., 2017). As digital natives grow up surrounded by technology, they are more apt to embrace and adopt new emerging technology (Ahn & Jung, 2016). Digital immigrants view technology differently than digital natives who see technology and their ability to access information, social or education, as an anywhere, anytime, and any place constant.

Students are engaged users of technology and have demonstrated their inquisitiveness through their early adoption and advocacy of media and IT (Schindler et al., 2017). Students' use of technology can impact student engagement and retention (Schindler et al., 2017). Students are looking at mobile devices as learning tools and are seeking an academic return on investment (ROI) when they purchase a mobile device for educational purposes (Castillo-Manzano, Castro-Nuño, López-Valpuesta, Sanz-Díaz, & Yñiguez, 2017). Over 50 percent of college students are carrying multiple devices, all powered on, all connected to Wi-Fi and all transferring data (Castillo-Manzano et al., 2017; Schindler et al., 2017). The Castillo-Manzano et al., 2017 study also found students want instructors to increase the integration of devices into teaching activities. Higher education entities that fail to introduce and integrate technology into a student's learning experience will also find themselves failing to meet the expectations of students who have embraced and integrated technology into their lives regardless of their distinction as digital native or digital immigrant.

This study seeks to identify successful strategies put into place by community college CIOs to address the challenges of increasing mobile usage demands directly related to devices students are bringing to campus.

Transition and Summary

The body of literature on BYOD continues to be quite varied. The research reviewed offers few strategies to manage BYOD successfully on community college campuses. The topics within this section included a discussion of Rogers's DOI theory as well as BYOD as it pertains to students' use of mobile devices on campus. A study of BYOD would not be complete without including; devices, connectivity, security, and security frameworks all are part of the foundation for the proposed research. The diffusion of innovation theory lends itself well to a qualitative case study among a homophilous group such as a like-minded cultural and social group of CIOs of North Carolina Community Colleges. Diffusion of innovation will provide opportunities to identify the successful strategies that CIOs are using to manage the BYOD demands on campus along with how those strategies were used and why those specific strategies were employed. In Section 2, the topics include a comprehensive description of the research methodology and design, population and sampling, data collection instruments and techniques used in the research study. Section 2 also includes a discussion on the collection and organization of data, its analysis techniques, its reliability, and its validity. Section 3 consists of a detailed account of the research conducted in the exploration of strategies used by North Carolina Community College CIOs to address the challenges of increasing mobile use demands directly related to student use of BYOD on campus.

Section 2: The Project

Purpose Statement

My purpose in this qualitative multiple case study was to explore strategies that are used by North Carolina Community College CIOs/CTOs to address the challenges of increasing mobile use demands directly related to student use of BYOD on campus. The population for this study was made up of CIOs or CTOs. The findings of this study may be used by organizations to alleviate BYOD concerns by identifying strategies that may assist in mitigating issues relating to user demand and networking constructs. My findings in this study may contribute to positive social change by improving the work-life balance of information management services staff members and the school-life balance of students.

Role of the Researcher

As the researcher for this study, I was the main data collection instrument for this study. In qualitative research, the researcher becomes the human instrument of data collection (Baillie, 2015), Palinkas et al., 2015). My role as a researcher began while choosing my research topic and methodology. At this stage of my research, my role continued to evolve to include recruiting participants, collecting data via semistructured interviews, collecting organizational documents that relate to the topic, conducting follow up interviews, and using member checking. At that point the role transitioned to one where the collected data was interpreted to find themes within the information that would provide evidence on the strategies that CIOs are using to mitigate IT infrastructure

demands produced by student BYOD usage. Once completed, the final aspect of the role comes into play: reporting the results.

The qualitative researcher collects the data from participants, analyzing the data, and presenting the information in a cohesive, unbiased, and ethical supporting framework for the research question (Collins & Cooper, 2014). Although researchers bring their own biases, assumptions, and beliefs to a research project, they should be self-aware enough to manage their preconceptions, assumptions or expectations (Elo et al., 2014). Sanjari, Bahramnezhad, Fomani, Shoghi, and Cheraghi (2014) posited that ensuring the confidentiality of participants and information, obtaining informed consent, and recognizing the potential impact of research participants on a researcher and vice versa were essential challenges for a researcher. As the researcher, it was my responsibility to ensure that I met such research challenges ethically. To adequately meet these challenges, researchers should adhere to the Belmont Report's underlying tenets of justice, respect for persons, and beneficence (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). Throughout this study, I followed the ethical principles of justice, respect for persons, and beneficence as laid out in the Belmont Report (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979).

In this qualitative case study, I sought insight into the BYOD on campus phenomenon through the eyes and experiences of the study participants; community college CIOs. I have 30 plus years of experience in the IT field. My work experience as an IT manager, IT resource manager, and IT system administrator have exposed me to

various IT implementation procedures, governance environments, as well as IT security protocols and procedures. My relationship to the population included depth and breadth duties of my prior work experience as senior IT technologist are similar to that of a CIO in that I managed IT staff across multiple locations, implemented and/or upgraded IT infrastructure as necessary, managed budgets, and resources, and others. Fusch and Ness (2015) asserted that it becomes the responsibility of the researcher to take whatever steps are necessary to prevent bias from being introduced. I maintained a reflective journal throughout the data collection and data analysis phases in order to help mitigate any bias. I also used an interview protocol to aid in moderating bias. Jamshed (2014) noted that the use of an interview protocol assists the researcher in staying focused on the interview itself.

My relationship to the geographic area of this study is that I reside in North Carolina, and this is the state from which I sought research participants. I chose participants from the North Carolina Community College System which encompasses 58 community colleges spread out amongst North Carolina's 100 counties. In several instances one centralized community college may serve up to four counties. There are also several community colleges that have one main campus, and several satellite campuses within the same localized area to better serve its students. Although I remain employed at a North Carolina Community College, my current position is not within the IT department nor will the college be participating in the research. I sought to ensure any bias on the part of this researcher did not infiltrate this doctoral study.

Elo et al. (2014) suggested that researchers conduct semistructured interviews to reduce potential bias while also taking care not to steer the participant's answers to obtain inductive data. Before beginning the interview, I asked for the participant's permission to record the interview. During the interview sessions, I followed an interview protocol (Appendix C) because it brought focus to the questions, scope of the study, and time limitations of the interviewee. Before holding any interviews, I identified any potential bias by exploring the suitability of interview questions. A researcher should not manipulate or lead the interviewee (Elo et al., 2014). I examined recordings of the interviews for any attempt by myself to manage or influence the interviewee. Both Elo et al. (2014) and Varpio, Ajjawi, Monrouxe, O'Brien, and Rees (2017) conducted studies and used member checking, a process in which participants are provided a copy of the earlier recording to verify the accuracy, validity, and credibility of the audio files. A recording and its subsequent transcription are vital data sources (Moser & Korstjens, 2018). I used member checking to validate interview data with each participant. Reaching the point of data saturation is obtained during the process of collecting data no new data became available, and themes within the research are similar (Fusch & Ness, 2015). To reach the data saturation point I collected data until no new information was available.

Participants

Researchers should state the criteria used for selecting research participants because it may assist other researchers in determining the transferability of findings (Elo et al., 2014). Researchers can aid transparency by establishing a list of desired attributes before identifying individuals of the target population who meet the criteria (Ketokivi &

Choi, 2014). The potential participants for this study will consist of the CIOs or CTOs of North Carolina's 58 community colleges. Three criteria were used to determine an individual's inclusion as a potential participant: (a) the individual must hold a CIO position at a North Carolina Community College, (b) be in place for at least 1 year, and (c) has knowledge of the strategies used to manage BYOD on campus. Before reaching out to the potential participants, I sought approval from the college president of each community college before contacting the potential participant. Once the associated college president provided their consent, I contacted potential participants via email to request their participation in a study of the research topic and identify how long they have been in their present position as CIO or CTO. When contacting potential participants, I explained the research problem being studied, as well as emphasized the study's inherent value. Prospective participants are more likely to take part in a research study if the topic is seen as relevant to them and could affect business practices (Cacari-Stone, Wallerstein, Garcia, & Minkler, 2014). I worked with each participant to determine which time and place, which method (in-person, Skype, or telephone) would be most suitable for the study participants to meet with me and conduct the semistructured confidential interviews that are necessary for a successful research study.

The relationship between researcher and research participant is one of necessity, and one of the primary responsibilities of a researcher is to identify strategies that will aid in the development of a positive working relationship between researcher and research participant (Kaczynski, Salmona, & Smith, 2014; Yin, 2014). One such strategy requires the researcher to remain impartial and not let preconceived ideas influence the participant

or the study (Kaczynski et al., 2014)). Another approach involves the management of the research participant's expectations regarding how data was to be collected and used (Cacari-Stone et al., 2014). I confirmed that each research participant understood the nature of the research; its anonymity and ensured my own biases did not affect the interview process or subsequent data collection. Jamshed (2014) supported the use of an interview protocol to lessen the risk of bias. I used an interview protocol (Appendix C) to avoid any bias being interjected. I made every effort to establish a rapport with each participant as well as remaining impartial so that a professional working relationship developed.

Each participant's position as CIO or CTO within the North Carolina Community College System is essential in addressing the overreaching research question of the study. As senior IT managers, they are the ones who decide what strategies are used to address the increased demands of mobile device usage on campus. They are the individuals who determine if the strategies have been successful. They are the individuals who will aid in the diffusion of information regarding which strategies are successful. The sharing of their experiences will assist in responding to the central research questions as well as provide additional credence the study.

Research Method and Design

Determining the methodology of a research study is a significant step for a researcher. There are three research method types; quantitative, qualitative, and mixed methods (Yin, 2014). The researcher's choice of the methodology provides a mechanism

to collect data, link it to the overreaching research question, and ultimately to the conclusions posed by the researcher (Yin, 2014).

Method

After considering qualitative, quantitative, and mixed methodologies, I chose to use a qualitative methodology for this study. A qualitative approach allows for the discovery of the strategies that community college CIOs use to successfully address the challenge of increasing mobile usage demands on their respective campuses. According to De Massis and Kotlar (2014), sources of data used in a qualitative research study may include, interviews, observations, and documentation. Parker (2014) elaborates by noting that the themes resulting from the study will assist in the interpretation of the data as well the analysis of the data. By using qualitative research methods, a researcher is able to seek out information from individuals who have experienced the phenomenon thereby leading to a complete understanding of the phenomenon (Vaismoradi, Jones, Turunen, & Snelgrove, 2016). Berger (2015) notes that individuals are able to inform the researcher of their experiences in their words. As a qualitative researcher whose interests lie with the identification of strategies that mitigate IT infrastructure demands produced by student BYOD usage on community college campuses I want the CIOs or CTOs to provide a descriptive narrative of their experiences with the phenomenon in that I might better inform this study. Qualitative research met the needs of this research study as it can be used to explore the perceptions and experiences of CIOs/CTOs as well as dive deeper into the phenomenon under investigation; strategies to manage BYOD.

Quantitative research involves the use of statistical analysis by which the researcher may draw conclusions (Bezzina & Saunders, 2014). Quantitative research is most often associated with 'what' types of questions; such as what number or what percentage (Barnham, 2015). Kahlke's (2014) research indicates quantitative research uses; closed-ended questions, hypotheses, and the correlation of the data to quantify relationships between variables. In quantitative research numerical data is gathered to prove or disprove a hypothesis (Aykol & Leonidou, 2014). While quantitative data may be more efficient with numbers it does not allow for contextual detail (McCusker & Gunaydin, 2015). Although I considered quantitative research methodology as an avenue for this study, its use was ultimately rejected. The use of closed-ended questions, hypotheses or the quantification of relationships between variables will not provide sufficient contextual data with ample detail to answer the specific IT problem of this study. As I was not be using hypotheses to predict outcomes nor would I be evaluating the cause and effect of the research phenomenon, quantitative research methodology was not be used for this doctoral study.

Another method, mixed methods, was reviewed prior to selecting the methodology to be used for this study. A crucial part of mixed method methodology is that it contains attributes of both qualitative and quantitative research into one study and allows both qualitative data and quantitative data to be collected and used to examine or explore an issue (Maxwell, 2016). These two data streams are then combined into one and used for analysis (Sparkes, 2014). As previously discussed a quantitative research methodology was not selected for use in this doctoral study as the research question is

qualitative in nature and seeks to gather information about the CIOs/CTOs lived experiences with the phenomenon. The prior decision not to use quantitative methods negates the use of mixed methods as it uses both qualitative and quantitative approaches. A researcher could choose to use mixed methods if the research question was such that neither qualitative nor quantitative could offer a more comprehensive understanding of the research question by itself (Abro, Khurshid, & Aamir, 2015). Bezzina and Saunders, (2014) noted that the data collected in a mixed method methodology could be used to develop mathematical statistics from which conclusions are drawn. In the case of this study the use of qualitative methods alone drew out sufficient information from participants that there was no need to combine qualitative and quantitative methods to answer the research question. I did not choose mixed methods as a methodology for this doctoral study as to do so offers an opportunity to focus more on numerical data such as mathematical statistics rather than gaining a fuller understanding of lived experiences and contextual information that could be garnered via the selection of qualitative research methods.

Research Design

The three qualitative research designs considered for this study were case study, ethnography, and phenomenology. I chose to use a multiple case study for the research. De Massis and Kotlar, (2014) note that the use of data from multiple cases offers the researcher the opportunity for a more in-depth understanding of the phenomenon under investigation as the phenomenon is occurring at multiple sites. Using the framework of a multiple case study allowed me to investigate the strategies used by nine CIOs from

different organizations as they address the IT infrastructure demands produced by student BYOD usage on their respective campus. A multiple case study may increase a study's credibility (De Massis & Kotlar, 2014) through the examination of multiple data types from a number of sources (Baškarada, 2014). A multiple case study aided in the discovery of the strategies that some community college CIOs use to successfully address the challenge of increasing mobile usage demands on their respective campuses. By implementing a multiple case study I was able to identify if a particular strategy was successfully working to reduce the demands placed on campus IT infrastructure by student BYOD usage on a single campus, or more than one campus, thus adding validity to the use of that strategy. The sample size of nine is representative of the 58 NC community colleges and met data saturation in that CIO is able to provide rich data regarding the successful strategies they have employed to address the BYOD demands related to students. These two aspects; multiple data types and multiple sources, allow for a fuller knowledge base by the researcher. The in-depth knowledge that developed through the richness of data coming from multiple participants and multiple sources; interviews, documentation is why a multiple case study research design was chosen for this study.

Phenomenology was also examined as a possible approach for this study. The phenomenological approach is descriptive in nature as individuals' share their experience with the phenomenon as it is occurring not rationalizing it afterwards (Adams et al., 2014; Yüksel & Yıldırım, 2015). Phenomenology can be described as an external reality that has meaning to those experiencing it (Hannaford, 2017). This study was not seeking

to address what was transpiring on community college campuses as CIOs/CTOs are engaging with BYOD but what strategies have proven to be successful in managing BYOD on campus. Adams et al., (2014) asserted that a phenomenological approach was best suited when a researcher seeks to explore the participant's views and behaviors during their interaction with the phenomenon. This study sought to obtain information about the CIO/CTO's interaction with BYOD but not during the interaction. The data collection methods for phenomenological research include interviews and diaries, (Adams et al., 2014). It is through the use of interviews and diaries that the lived experience comes to life and allows the researcher to accurately portray the interaction between individual and phenomenon (Willis, Sullivan-Bolyai, Knafl, & Cohen, 2016). In this study I did not pursuing the discovery of personal diaries or drawings, nor was I observing the study participant as they interacted with the phenomenon; as a result phenomenology was inappropriate for this study.

I also examined ethnography as a potential research design. The use of ethnography as a research design requires a researcher to become immersed in the culture and a large amount of field observations would be necessary to determine actual behaviors (Brown, 2015). For this study I was not attempting to become immersed in IT departments within a number of community colleges as they addressed BYOD on their campuses. Reich (2015) noted that ethnography occurs when researchers explore the belief and feelings within a culture. Becoming part of the lived realities of a person or group provides an ethnographic researcher with an in-depth insight into how individual and groups interact and provide context for the research study (Hallett & Barber, 2014). I

am not seeking to identify beliefs of the participants nor how they react as a group. The data collection for an ethnographic study would include structured and non-structured interviews, attending meetings, a review of files and documents (Marion, Eddleston, Friar, & Deeds, 2015). As I was not seeking a complete immersion within a culture, to include attending meetings about the phenomenon, nor would I be using structured or non-structured interviews to collect data related to BYOD on campus. As such, an ethnographic research design was not suitable for this study.

Data saturation is a necessary component of research. Hennink, Kaiser, and Marconi, (2017) suggest that reaching saturation involves the characteristics of the study itself, the type of data, and the researcher. One method used by researchers to reach data saturation involves conducting semistructured interviews with the research participants (Fusch & Ness, 2015). Both Cleary, Horsfall, and Hayter, (2014) and Fusch and Ness, (2015) asserted that the point of data saturation is reached when the responses to the semistructured interview questions stop providing new information. I used semistructured interviews as well as analyzing documentation provided by participants to reach data saturation. I stopped conducting semistructured interviews when no new data, themes, or coding was forthcoming. There is no magic tipping point to aid in determining when data saturation has been achieved. In this case, data saturation was not reached with the minimum participants obtained via the original email, thus a second call for volunteer participants was made. I collected data until no new information was being gleaned from the semistructured interview with research participants and documentation they provided as this indicated when data saturation has been achieved.

Population and Sampling

For this study, the population consisted of the CIOs of community colleges within North Carolina who have been in place for a minimum of one year and have knowledge of the strategies used on their respective campus to manage, successfully, the BYOD demands brought about by mobile devices on campus. Using this eligibility criteria could mean that only one individual from each community college would meet the criteria resulting in a 58 member population maximum. Using statistical reporting from North Carolina Community Colleges system office for the 2016-2017 academic year I segmented the 58 community colleges into three units (NCCCS, 2018). Unit One was comprised of community colleges with less than 2000 curriculum students, Unit Two includes community colleges with curriculum students numbering more than 2000 but less than 5000. Unit Three includes community colleges with 5000 or more curriculum students. This study incorporates data from three colleges within each unit for a total of nine cases to be studied. The justification for dividing the 58 community colleges into three units was based on number of students attending each community college. There may be unique BYOD scenarios in place based the location of the campus, the campus size and the population size. Student population numbers are but one of many criteria used to establish budgetary constraints for community colleges and budgets may affect the strategies that are put into place to manage the BYOD demands of students on campus.

Elo et al., (2014) posited that qualitative studies have no universally accepted sample size and that the ultimate sample would depend on items such as the purpose of the study and research questions to name two. For this study I used a sample size of nine

representing the 58 NC community colleges. The data collected from CIOs was specifically related to successful strategies they have used to address demands brought about by student use of BYOD on campus. Malterud, Siersma, and Guassora (2016) suggest that a sample size and study aim are related, in that a narrow focused study can be supported by a smaller sample size, particularly when study participants hold specific characteristics. Participants in this study are CIOs, who have been in the position for more than one year and have successfully addressed the use of BYOD by students on their campus. Elo et al., (2014) further identified that a sample must contain participants who can best represent the topic. This study sought to engage with the CIOs/CTOs who, as senior IT managers, are best qualified to provide responses to the research question as it directly related to IT. Berger (2015) supports Elo et al., (2014) noting that in a qualitative study there is a direct link between the population's characteristics and the participants' experience with the phenomenon. For example, in this study a participant characteristic I sought was that the individual be either a CIO or CTO for a community college and have managed the strategies that are connected to the phenomenon of BYOD. Using the position of a potential participant as a criteria to include or exclude the individual from the population is a practical way to begin the data collection process (Robinson, 2014).

Two aspects of qualitative research, data collection and sampling methodologies, are interwoven. Data collection is crucial in that with data the research question can be answered. How data is collected, compiled and managed falls upon the researcher through the use of sampling techniques (Robinson, 2014). Without correctly collected

data the analysis may prove impossible (Yin, 2014). One method a researcher may use to garner data is through the use of various sampling methods such as probability and non-probability (Etikan, Musa, & Alkassim, 2016). This study used the non-probability sampling method; purposive, which actually encompasses several techniques for sampling.

Purposive sampling methods include maximum variation, total population, quota, expert, homogeneous, among others (Palinkas et al., 2015; Robinson, 2014). Robinson, (2014) asserts that the researcher's use of purposive sampling results in the nonrandom selection of research participants as it involves identifying and then selecting individuals who have knowledge of the phenomenon under investigation. In other words, the focus of purposive sampling is on the characteristics of a population that enable a researcher to answer the research question. Purposive sampling was appropriate for this study in that the research participants met the specific perspectives that this study targeted.

Homogeneous sampling is a type of purposive sampling and occurs when research participants share a commonality such as ages, experiences, or jobs (Etikan et al., 2016). Palinkas et al., (2015) posited that homogeneous sampling can be used to reduce variation and to simplify analysis. Hammarberg, Kirkman and de Lacey (2016) noted that homogeneous sampling involves choosing participants based on their interaction with the phenomenon under study. For the purposes of this study I used homogeneous sampling when surveying individuals who were employed as a CIO or CTO position (job) within the IT department of a community college (commonality) about their experiences with BYOD on their respective campus.

Ethical Research

The transparency of a research study is necessary to ensure the credibility and reliability of a study (Robinson, 2014). Adherence to the requirements for informed consent will lead to transparency. One tenet of ethical research is that of informed consent in which the researcher provides sufficient information to the research participant so that they may make an informed decision regarding their participation in the study (Sanjari et al., 2014). Each research participant received the following: a statement regarding the research nature of the study and an explanation of the purpose of the research. Also, they also received information on how the results will be used, the expected duration of the participant's involvement, a description of the procedures used and an account of participant requirements (Sanjari et al., 2014). The consent form, Appendix A, addresses these requirements in detail.

To all participants, I explained my role as researcher, advised participants of the voluntary nature of their participation and their rights and explained how to withdraw from the study. I obtained informed consent from each participant, ensured they were aware of the confidentiality of their interviews. To ensure compliance with these principles I completed a National Institutes of Health (NIH) online training course which is available to researchers.

Participants were provided with a description of how the confidentiality of their identifying information would be handled during the study and afterward (Sanjari et al., 2014). Substituting an alphanumeric code for each participant securely concealed their personal information. All data was stored in files that are password protected. The files

were placed on a flash drive, and the drive was encrypted, and then the device was stored in a safe where it remain for not less than five years, thus preventing access by a third party.

While an individual's participation in a research study was voluntary the participant was made aware of the manner in which they could terminate their involvement with the research study (Artal & Rubenfeld, 2017). In the case of this study all participants were informed that they could withdraw from the study at any time and were furnished with the researcher's email address and phone number ensuring they had multiple ways to remove themselves from the study should they so choose.

Walden University has its own set of research protocols, and as a Walden Doctoral student, I complied with their requirements. I applied for and received Walden University IRB approval to conduct research, and the IRB approval number is 04-05-19-0530198. The requirements of Walden University IRB and the recommendations of the National Institute of Justice are quite similar. As noted previously, Appendix A is the consent form by which research participants agreed to participate in the doctoral research study.

Data Collection

Data Collection Instruments

In this qualitative study I am serving as the instrument of data collection and will use semistructured interviews as the primary instrument of data collection, followed by an analysis of organizational policies and documents as additional sources of data. In qualitative research, the researcher becomes a human instrument of data collection in that

the method of data collection and its subsequent analysis are under the control of the researcher (Kaczynski et al., 2014). Yin (2014) stated there are six types of sources that can provide evidence; interviews, documents, archival records, physical artifacts, direct observation, and participant observation. I, as the researcher and primary data collector, will use two of these sources; interviews and documentation to gather evidence for this study. Having multiple sources of data will allow me to filter the data to define its themes in order to work towards a more complete analysis of the collected data. The use of multiple sources to collect data also aids in the subsequent triangulation of data. Wilson (2014) asserts that when triangulation is reached it offers richer data and is accomplished by using more than one source to gather data. Fusch and Ness (2015) noted a correlation existing between data triangulation and data saturation. By employing multiple avenues of data collection I was able to show data triangulation which in turn leads to data saturation.

The use of semistructured interviews is a popular data collection method with its versatility and flexibility (Kallio, Pietilä, Johnson, & Kangasniemi, 2016). Semistructured interviews consist of open-ended questions which elicit information from research participants as they respond to the questions posed (Jamshed, 2014). I used open-ended questions in semistructured interviews. This type of interview typically lasts from 30 minutes to 1 hour and it is usually only conducted once (Jamshed, 2014). I allowed one hour for the interview. If the interview session was running long I asked the participant if he or she wished to continue or to schedule a follow-up interview session and I complied with their wishes.

The interview protocol I used was developed using open ended questions to elicit descriptive responses from participants.(Appendix C). Kallio et al., (2016) suggests that the quality of the interview protocol will affect the interview and any subsequent analysis of data coming from the interview. Using an interview protocol form or guide as well as recording the interview serves to keep the researcher focused on the interview itself (Jamshed, 2014). I developed Interview Protocol Form, Appendix C, to ensure each participant I asked the same questions and that they were asked in the same order. I also digitally recorded each interview session so note taking did not become a distraction during the interview. Asking participants the same questions in the same order allows a comparison of responses and can lead to data being quantified even in qualitative research (McIntosh & Morse, 2015). Following an established interview protocol may result in an opportunity create and compare participant responses easier and improve the reliability of the semistructured interview sessions. I also used member checking with the same goal in mind.

For this study, the interview protocol consisted of the primary research question and additional open ended questions that relate to it. I also obtained college/archival documents from participants that may assist in identifying strategies that mitigate infrastructure demands produced by student BYOD usage. I served as the primary data collection instrument and used semistructured interviews, organizational policies and documents as sources of data. Barglowski, Bilecen, and Amelina (2015) note that by combining interviews and document analysis yields a data set that may offer additional insight into the research topic may be identified. I compared information obtained from

the document analysis and interviews to ascertain if similarities existed among the cases. This led to further identifying relevant information regarding strategies used to mitigate IT infrastructure demands produced by student BYOD usage on campus and also aid in the triangulation of data.

Member checking is one way to enhance the reliability and validity of the data collected during semistructured interviews (Elo et al., 2014). Member checking may involve; returning an interview transcript to the participant, holding a second meeting with the participant to review interpreted data (Birt, Scott, Cavers, Campbell, & Walter, 2016). To review data and interpretations of the data I conducted member checking via phone or Skype. Kornbluh (2015) noted that member checking can be used to ensure the accuracy of and the authenticity in the representation of the research participant's views and experiences as captured during the semistructured interview. For this study the process of member checking involved recording the semistructured interviews during the first interview session, creating a verbatim transcription from the digital recording and documenting my interpretation of the data collected during the interview. My interpretation of data collected was then forwarded to the research participant who participated in the semistructured interview process allowing him or her to agree or disagree with the interpretation of the interview. Study participants may or may not agree that the interpretations correctly reflect their views and experiences. Perrotta (2017) asserts that providing interpretations to the participants in order that they may check it for the accuracy of their words, and views enhances the credibility of a study. Incorporating member checking increases the credibility of a study as the accuracy of data collected can

be verified. Wolgemuth et al., (2015) suggests that member checking can be used to allay fears of misrepresentation or that material the participant asked to be excluded has been. If there are questions from the research participants regarding my interpretation or the accuracy of the information they provided the process of member checking will continue until both agree to content and interpretation.

Data Collection Technique

Data collection is an integral part of research as without data one would be unable to test hypotheses, answer research questions or evaluate outcomes. There are several data collection techniques available to researchers. According to Kornbluh (2015), researchers choose a data collection technique based on the design of the research study. For this study, I used two types of data collection techniques; semistructured interviews, and reviewing organizational documentation. From the CIO or chief technical officer I sought to obtain organizational documentation related to BYOD on campus may include documents regarding; changes in the coverage area, availability of network, increases in bandwidth, etc. Elo et al., (2014) suggest semistructured interviews can be used to reduce potential researcher bias while also steering the conversation in such a manner that the participant's answers offer insight to the research question. I used an Interview Protocol Form, Appendix C, to assist in the elimination of any potential bias and to keep the conversation on track. Moser and Korstjens (2018) posited that there is a tipping point at the beginning of the interview session in which the researcher should strike a rapport with the participant to help them feel at ease. To this end, I tried to ensure each participant was aware of the confidential nature of the research, that their participation was voluntary and

that they would not be identified within the study. I endeavored to establish a rapport with each participant as with rapport comes the inclination to share more. I met with participants face-to-face and used a digital audio recorder in the semistructured interview scenario with open-ended questions to identify strategies used by CIOs/CTOs that mitigate IT infrastructure demands produced by student use of BYOD on campus. Eliciting additional details via follow up questions is appropriate and may extract more specifics (Elo et al., 2014). If during an interview further clarification to the participant's response was needed I asked follow up questions as necessary. At the conclusion of the interview I thanked the participant and scheduled a follow-up meeting with them within one week of the initial interview. During this time a verbatim transcript of the interview was transcribed by myself and I began interpreting the data. The second meeting was to discuss my interpretation of data received during the initial interview with the research participant.

Before initiating any data collection on any North Carolina Community College campus approval must be granted by its President. Having received approval, I reached out to the CIOs/CTOs of those specific colleges. This initial contact was via email and contained an invitation to participate in the study as well as one demographic question; identifying how long he or she has been in the position. The eligibility criterial for this study is two-fold; the individual must hold either a CIO or a CTO position and have been in the position for more than one year. The first three positive responses from each unit became the initial participants of this study. If a CIO/CTO declined to participate in the research study all communication with that individual ended at that point. If the

CIO/CTO indicated a willingness to participate, I worked with the individual to arrange a mutually agreed upon time and place for the interview in order to maintain the participant's anonymity. I scheduled the interviews for one hour during which I begin by using an interview protocol to ensure each participant received the appropriate information. If at the close of an hour the interview was not finished I asked the participant if they had the time to continue. If their response was positive the interview would continue from there. If the participant was unable to complete the interview I made another appointment to conclude the interview. By using the prescribed interview protocol (Appendix C), I ensured each participant received the same information regarding the study, its purpose, informed consent, how to withdraw from the study, what happens after the interview, member checking, how the data was be stored, etc. The use of an interview protocol also ensures that the set of questions are asked in order, and none overlooked.

I employed the process of member checking which continued until no new information was elicited from the participant with the understanding that one or more conversations may be necessary in order to reach that point. Member checking is also known as participant validation and can be used to increase credibility within the research project (Birt et al., 2016). In the case of this study, once the initial interview had taken place, and a verbatim transcript was available, each participant received a copy of my interpretation of the information obtained in the initial interview session. Receiving a copy of my interpretation of the interview permits the participant to review the information and determine if any data points need to be changed or modified. Thomas,

(2017) suggests that a second interview, for member checking, be held to go over the interpretation of the data obtained in the first interview with the participant. I contacted the participants to set up a Skype or phone session to discuss interpretations of the data collected during the initial interview. Agreement regarding interpretations is an indication that the point of data saturation has been reached. This activity allows the participants to review the transcript interpretation, identifying that their words match the meanings they intended to convey (Varpio et al., 2017).

During a member checking process the participant has an opportunity to confirm the information within the transcription, modify any information necessary and to verify the information within the transcription. The process of confirming my interpretations with the participant continued until no new data was forthcoming from the participant. The trustworthiness that member checking can bring to research is the reporting of the outcomes (Thomas, 2017). Member checking is one method of enhancing the validity of a research study (Leung, 2015). As this research seeks to identify strategies that mitigate IT infrastructure demands produced by student BYOD usage on campus, member checking offers a viable opportunity for participants to ensure their strategies and voices are heard and appropriately represented.

Data Organization Techniques

To gain an understanding of the data collected during this study, the data must be organized in a manner that facilitates identifying relationships with the research question. How data is organized can be the key to understanding and analyzing the collected data (Elo et al., 2014). Data organization can also be used to ensure the confidentiality and

anonymity of research participants when masking the participant's identities via the use of alphanumeric codes (Arora & Dhiman, 2015). The method of alphanumeric codes to disguise identities is a quid pro quo arrangement between participant and researcher; the resulting anonymity allows the participant to offer their insights and experiences regarding the phenomena under investigation. After each interview, the verbatim transcript of same was uploaded into an MS Word document and given an alphanumeric code. The documentation attributed to each community college i.e. interview transcriptions and interpretations along with organizational documentation was placed in a separate folder protected by a password. Organizational data was scanned, the file was given the appropriate alphanumeric designation and uploaded to flash drive as a PDF. All data collected during this doctoral study will be kept on an encrypted flash drive for a period of five years. Another organizational method suggested by Pucher, Candel, Krumeich, Boot, and De Vries (2015) requires a researcher to use a reflective journal. During each interview, I took notes of essential comments so that I could compare notes to the audio recording of the interview. After each interview, I reflected on the conversation and identified themes or patterns as a result of my observations and transcribed my findings into a digital journal. Vicary, Young, and Hicks (2017) suggest that the use of a reflective journal inside of a software package, such as NVivo, and used for analysis can enhance the quality and validity of the study as the journaling aspect provides an audit trail for decisions.

To further ensure participants' privacy and confidential data, I adhered to the recommendations of Herranz and Nin (2014) regarding securing the data. All materials

(interview recordings and their transcription, documents, any coded files, researcher notes, and researcher's reflective journal) were stored onto two encrypted flash drives, which were password protected. One flash drive, the original, was stored in a locked safe. The second flash drive was stored in a safe at a separate location. All data collected for this study is to be kept for five years before being destroyed.

Data Analysis Technique

Watkins (2017) acknowledges that qualitative research methods allow researchers to gather more in-depth knowledge of the phenomenon under investigation. The time requirements to collect, transcribe, and organize data can be lengthy as can the time to adequately analyze the qualitative data (Watkins, 2017). For this study, data analysis provided a framework to understand the successful strategies used by CIOs/CTOs to manage BYOD on the college campus. Once I collected the data, I moved to the analysis phase. Moser and Korstjens, (2018) suggest immersing oneself in the data, reading transcriptions, field notes, etc. is necessary at the start of the data analysis. This phase involved working with the data to discover what themes, patterns, and description serve to answer the research question (Maree, 2015). The use of semistructured interviews assists the researcher to understand the perspectives of the research participants (Arora & Dhiman, 2015). In this study, the analysis phase included the coding, sorting, querying, and analysis of data obtained from semistructured interviews with research participants and organizational documentation.

Once I completed the corroboration of research data the phase of data triangulation began. Wilson (2014) noted that triangulation can be used to confirm the

results of research or when obtaining data that is richer and fuller is necessary. Varpio et al. (2017) wrote that triangulation is a way to enhance the credibility of study and occurs when multiple points of data are collected from differing perspectives, thus producing a comprehensive picture of the topic. Yin (2009) identified five types of triangulation (a) analysis, (b) data source, (c) investigator, (d) theory, and (e) methodological. Methodological triangulation involves the use of multiple methods to collect data (Yin, 2009). For this qualitative multiple case study, data triangulation was appropriate as I collected data from semistructured interviews, reflective journal entries as well as viewing organizational documentation. The primary data was collected from CIOs during a semistructured interview. Secondary data was collected from organizational documents that the CIOs provided. The primary data, coupled with the secondary data allows for data triangulation. As these two data streams converge, a fuller picture of the successful strategies used by CIOs to address student use of BYOD on campus emerges. The use of triangulation increases the reliability of a study as it also helps remove researcher bias (Joslin, & Müller, 2016).

I used a digital voice recorder recording device to record the interviews. I completed the actual verbatim transcription myself before entering data into the NVivo software. NVivo falls into the category computer-assisted qualitative data analysis software (CAQDAS) and its features include character-based coding, rich text capabilities along with multimedia functions which have proven to be instrumental for qualitative data management (Zamawe, 2015). The NVivo software is a tool that aids in the ability to manage, analyze, and report the information obtained via semistructured

interviews and official documentation (Houghton et al., 2017). It was through the categorization of data that led to identifying and developing themes. Zamawe (2015) posited that NVivo saves researchers time during transcription while heightening the accuracy and speed of the analysis process. By using NVivo, I was able to work with data through inputting, storing, and coding it. Reviewing the interview questions while establishing codes within NVivo enabled me to identify and isolate keywords and themes from the responses of participants. I identified words, descriptions, and experiences that correlate to the central research question and Rogers's diffusion of innovation, which was used as the conceptual, theoretical framework for this study.

Vaismoradi et al. (2016) suggest four phases to theme development; initialization, construction, rectification, and finalization. Vaismoradi et al. (2016) recommends that to understand the collected data, a researcher must immerse themselves in the data by reading transcript, finding recurrent ideas, and finding the essence of the participant's experience with the phenomenon. The finalization phase of theme development is one that Vaismoradi et al., (2016) refers to as a storyline. Vaismoradi et al., (2016) reiterated that as a descriptive, narration tool the storyline is used to connect themes and may prove useful in reassuring other researchers about theoretical data saturation. The emergence of themes from data was developed through the interpretation of collected data by the researcher.

Reliability and Validity

As a researcher, my responsibility to the readers of this study was to demonstrate that my work is, in fact, a credible study. Often this is accomplished by demonstrating a

study's reliability and validity. Reliability for quantitative research means that a researcher should be able to replicate the results of a study if the same methodologies and processes are used (Leung, 2015). Reliability in qualitative research is about the consistent application of methods and processes which may result in outcomes similar to the original research yet may offer a slightly different explanation (Leung, 2015). Noble and Smith (2015) note that consistency or reliability relates to choosing the appropriate methods, implementing them, and documenting the decisions made within the research study.

The reliability of my study depends upon the research participants providing truthful responses to the interview questions. To this end I ensured each participant was aware of the process I undertook to ensure their confidentiality, the use of alphanumeric coding of names, storing interview transcripts in a password encrypted folder stored on a flash drive, and placed into a safe to which only I have access. I assigned an alphanumeric code to each participant, and the data obtained from the participants was kept on an encrypted flash drive and placed in a safe to which only I have access. Pucher et al. (2015) noted that the use of a reflective journal is helpful in tracking the decision making process. Vicary et al. (2017) suggests that the use of a reflective journal inside of a software package, such as NVivo, which is used for analysis can enhance the quality and validity of study as the journaling aspect provides an audit trail for decisions. My use of a reflective journal to document my decision-making processes throughout the research study will confirm that decisions are applied in a manner that was consistent with the chosen methodology.

I used an NVivo software package to code data collected in the semistructured interviews. NVivo has several features; character-based coding, rich text capabilities, and multimedia functions, that have proven to be instrumental for qualitative data management (Zamawe, 2015). The use of a reflective journal coupled with information received through semistructured interviews and organizational documentation may prove useful in determining trends and patterns during the analytic phase.

Dependability. The dependability of a study lies in another researcher being able to take the data collected, walk through the processes used initially, and find similar results (Hammarberg et al., 2016). As a qualitative researcher, my first step to ensure the reliability and dependability of this study was to document my processes and progress. I used a qualitative methodology, a multiple case study design, semistructured interviews, reviewing transcripts, member checking, and a reflective journal. The use of a set of standardized interview questions (Appendix B), and an interview protocol (Appendix C) serve to enhance the reliability and dependability of this study. No pilot test was used in this study.

I used NVivo 12 software to code data received during the interview process. The NVivo software is a tool that aids in the ability to manage, analyze, and report the information obtained via semistructured interviews and official documentation (Houghton et al., 2017). A recent study showed NVivo software could be used to supplement or extend the limits of previously used paper techniques and to enhance the transparency of researcher analytical processes (Woods, Paulus, Atkins, & Macklin, 2016). I used member checking with the research participants to eliminate

misrepresentation and misinterpretations, thus increasing the dependability of this study. Varpio et al. (2017) wrote that sharing data interpretations enhances the involvement of participants while increasing the credibility of data analysis.

According to Leung (2015), validity in qualitative research is synonymous with appropriateness. An example of this would be identifying if the interview questions within a study are appropriate to answer the research question or are the tools chosen for use within a study applicable to the development of the research question. Noble and Smith (2015) noted that the phrase 'truth value' is interchangeable with validity and is an indication of how truthfully the data is acknowledged in the research findings. Controlling the study parameters in addition to guarding against participant expectations, and researcher bias will add to the validity of a study (Brown, 2015). Member checking adds to the validity of data extracted from participants in that participants will have opportunity to verify and attest to the truthfulness of data collected from them (Leung, 2015). I set the parameters of the study, managing participant expectations by ensuring they were aware of how and why the research was being conducted and taking steps to mitigate researcher bias. The data collected from semistructured interviews coupled with member checking and organizational documentation played a crucial role in the data analysis portion of this study. Data saturation within a study can add validity. Fusch and Ness (2015) noted that data saturation plays a role in the quality of research and content validity. Reaching data saturation can be elusive as there is no magic tipping point yet Moser and Korstjens (2018) suggest that achieving data saturation results in no further sampling taking place. Fusch and Ness (2015) noted that data collection methods that

work well in one study design might not in another. For this study when no new data was forthcoming from semistructured interviews and member checking, no new participant interviews were held.

Transferability. For transferability to come into play, a study must have relevance or value to someone not involved in the original research (Cope, 2014; Hammarberg et al., 2016). Brown (2015) suggests providing thick descriptions of participants and the participant selection process for the study as this would enable a reader to determine if the study has implications for their specific situation. I have included rich descriptions of the collected data during the analysis process improving the transferability of my study. Such descriptions should enable other researchers to determine if the findings of this study could be used in another setting. Leung (2015) suggests that the same criteria used to measure the validity of a study should also apply to generalizability. I sought to provide readers with the tools necessary to make an informed decision regarding the transferability of this study to their specific organization by paying strict attention to data collection and the subsequent analysis of same. This process also included using the same interview protocol for each participant, member checking information with participants, and achieving data saturation. Member checking is a second interaction between researcher and participant during which the participant was able to confirm the accuracy of their responses to the interview questions and elaborate, if necessary (Varpio et al., (2017). Achieving data saturation is identified as occurring when no new data becomes available, and themes within the research are similar (Fusch &

Ness, 2015; Moser & Korstjens, 2018). I sought to aid the transferability of this study by including rich, detailed descriptions within the study.

Credibility. El Hussein, Jakubec, and Osuji (2015) describe credibility as the probability that others in similar situations will identify with the research findings. As the human instrument that gathers information in this qualitative research it was up to me to ensure that this study's credibility could be measured. Hammarberg et al. (2016) noted that credibility for a study can be found through a number of measures including; reflexivity, triangulation via semistructured interviews and documents obtained from research participants, and rich descriptions of the interpretation process. After the semistructured interviews had taken place and its transcription and subsequent interpretation were completed I then used member checking to increase the trustworthiness of this study. Noble and Smith (2015) note that full and rich detail in context is one method to enhance the credibility of qualitative research. Another method would be respondent validation (member checking): asking participants to comment on interpretations gathered from interview transcript (Noble & Smith, 2015). In order to enhance the credibility of this study I addressed personal biases, maintained records of decisions, identified processes relating to data analysis and its interpretation. The combining of two data sources within the same study for validation purposes is known as data triangulation (Hussein, 2015). Triangulation involves the use of multiple methods, different types of data and perspectives for the express purpose of enhancing the study's rigor (Varpio et al., 2017). For this study, I used the data collected from semistructured

interviews and official documentation to support data triangulation and enhance the credibility of the study.

Confirmability. Noble and Smith (2015) note that confirmability relates to identifying and documenting how the decisions were reached within the research study. Cope (2014) indicated that the use of rich quotes from participants adds to the fullness of the research and may aid in confirmability. Brown (2015) suggests the use of a recipe format to lend credence to a study's replicability, in that the study should descriptive and include sufficient detail to facilitate someone else replicating the study. I documented my observations during the semistructured interviews and the analytic decisions reached during the data coding phase within my reflective journal. This will provide future reviewers with insight into why/how of the decision-making process for this particular study. I documented coding via NVivo and identified themes that as a result of data interpretation and compilation.

Transition and Summary

In section 2, I discussed the research methodology, purpose statement, role of the researcher, participants, research method and design, data collection and analysis, as well as the reliability and validity of the data collection for this study. Performing a qualitative multiple case study supports an exploration of the strategies that mitigate IT infrastructure demands produced by student BYOD usage on campus. I sought out and gathered data from documents as well as administer semistructured interviews to add to the body of knowledge on BYOD and its effects on college campuses. Section 3 includes an overview of the study as well as a presentation of findings resulting from the data

collection. Also included was a discussion of how the research may be applied, recommendations, and a conclusion.

Section 3: Application to Professional Practice and Implications for Change

Overview of Study

My purpose in this qualitative multicase study was to investigate successful strategies used by community college CIO's to mitigate IT infrastructure demands produced by student BYOD usage. The data for this research study came from semistructured interviews conducted with the senior IT individual associated with the community college. There were various titles associated with this specific individual, for clarity, the title of CIO was used throughout this study. Documents included in this study were organizational documents provided by CIOs as well as my notes and reflective journal. All the research participants of the study had experience with the effects of increased digital devices being brought to campus by students and in developing successful strategies to monitor, contain and manage the subsequent demands being placed on IT infrastructure as a result.

Presentation of the Findings

The central research question was: What strategies do community college CIOs use to strategically address the challenges of increasing mobile usage demands directly related to BYOD on campus? The answer to this question may help other colleges and small businesses as they struggle to adapt to ever-increasing demands for access to Wi-Fi by personally owned digital devices. Semistructured interviews were conducted with community college CIOs to identify the successful strategies to manage BYOD on campus. In addition to the semistructured interviews, I reviewed organizational documents for information concerning successful strategies used by CIOs regarding the

research question. The availability of organizational documents validated information collected during the semistructured interviews with community college CIOs and aided in triangulation.

The participants in this study were all CIOs of community colleges. Each was the senior-most IT individual on campus and had first-hand knowledge about the effects of BYOD or digital devices on campus and had the authority to implement strategies to manage BYOD on campus successfully. Nine CIOs agreed to participate in this study, and nine were interviewed.

Data saturation first began to occur after the interview of Participant 7. No new major or supporting themes resulted from my interview sessions with Participants 8 and 9; this confirmed data saturation via participant interviews was achieved. All nine of the participants provided archival documents related to the central research question of this study. Records were associated with increased demands, the proposed increases in bandwidth, increasing the size of Wi-Fi footprint, adding access points, and others. Other materials included in the study were the notes I took during interviews and that I wrote in my reflective journal. I collected data from two sources, participants, and documents, which is the primary component of methodological triangulation. Varpio et al. (2017) noted that triangulation can enhance the credibility of the study and occurs when multiple points of data are collected from differing perspectives; thus, a more comprehensive picture of the topic appears. Joslin and Müller (2016) noted that triangulation increases the reliability of a study as triangulation also helps to remove researcher bias. To further

improve the analysis and my interpretations, I used member checking as another validation technique.

In my role as the primary research data collection instrument I compiled participant interviews, interview notes, the member-checking session transcripts, my journal notes, and archival documents into a database and maintained an audit trail. Upon completing the transcriptions of the nine semistructured interviews, I uploaded each into NVivo 12 Plus for analysis and coding. By using the NVivo software, I was able to upload the different types of documents that I obtained during the data collection phase of this study; transcripts from the semistructured interview, transcripts from the member checking activity along with organizational documents. With NVivo I analyzed the collected research data. NVivo is a tool that can be used by qualitative researchers to manage, analyze, and report on the information obtained via semistructured interviews and official documentation (Houghton et al., 2017). While analyzing the data within NVivo, several developing themes emerged. As I continued examining the data, I was able to further develop three significant themes. The first theme encompasses several different tools that CIOs use to assist with the management of BYOD on campus. These tools include Mobile Device Management (MDM), Mobile Applications Management (MAM), firewalls, and Unified Endpoint Management (UEM). The remaining two themes are; the importance of security awareness training and the importance of security policies and procedures and the importance of communication. These themes demonstrate successful strategies that CIOs of North Carolina community colleges use to

ensure digital devices brought to campus by students do not adversely affect the IT infrastructure of the community college.

I gained an understanding of the successful strategies used by CIO to mitigate the effects of BYOD on campus through the data collection and its analysis. With NVivo, it was much easier to categorize and identify themes from the archival organizational documents the participants provided and the participant interviews. Methodological triangulation and member checking ensured I reached data saturation.

The findings of this research study aligned well with the diffusion of innovation theory. Diffusion of innovation takes place via communication in that an innovation or idea, over time, gains momentum and spreads through a specific population or social system (Rogers, 2003). Rogers contended that diffusion needed communication but also recognized that diffusion would take place at different rates, and communication needed to be tailored for different groups.

Theme 1: Importance of Technology Management Tools

One of the first significant themes to emerge from the analysis of the collected data was the use of technology management tools by CIOs as their first line of defense to ensure the security of the institution's assets. The use of technology management tools to assist in the management of BYOD supports Bello et al., (2017) research that indicated the use of technical controls was one strategy used to mitigate BYOD privacy risks. As the technological landscape changes frequently, CIOs must take a hands-on stance regarding security by staying aware of not only the latest trends but the associated vulnerabilities and threats.

All nine of the research participants, indicated a reliance, to some degree, on technology management tools. Firewalls were either the solution or part of the solution for BYOD on campus. Firewalls, either as a software program or a device, have become increasingly important as a firewall can be used to monitor threats and safeguard networks. Participant 2 provided a brochure for an analytics-driven security solution that will be installed later this year. The decision to deploy this specific solution was due to its universal approach; it is not platform-specific. Mobile Device Management (MDM) and Network Access Control (NAC) were the first technology management tools to be mentioned by eight out of nine research participants. MDM is a centralized software that applies security agreements onto mobile devices as they connect to organizational systems (Downer & Bhattacharya, 2015). The findings of this study support the research of Muhammad, Zadeh, and Ayesh (2017), who posited that MDM is more focused on management rather than securing devices and that Mobile Application Management (MAM) is better for safeguarding information residing on and accessed on devices. Ali et al. (2015) noted that the typical set up for MDM uses a client-server architecture in which the server sends policies and permitted applications to an agent installed on the user's device. However, a large number of users use their devices to connect to systems not covered by MDM, such as Blackboard.

Eight of nine participants indicated that by itself, MDM is not a complete solution. It is part of a Network Access Control (NAC) list including dynamic role-based access, VLAN Access Control List (ACL), and application aware quality of service (QoS), which were noted by six of the nine participants as being part of a BYOD

solution. All nine participants indicated that the bulk of devices brought to campus are student-owned, not organizationally owned. Eight of the nine participants reported that as a result of device ownership, a critical part of the solution becomes the NAC. Participants 1 and 4 attributed their preference for using NAC to its Role-Based Access Control. Participants 7 and 9 specifically identified the NAC's enforcement of policies as their reason for using NAC. Participant 6 indicated that placing individuals in roles and knowing that they can only access the resources appropriate for that role provides "peace of mind." Five of the nine participants (56%) indicated they kept the standard NAC roles of Student, Faculty, and Guest on their networks. Eight of the nine participants reported that each of the three roles; student, faculty, and guest, has a specific set of privileges designed for the position. The second job of the NAC is to enforce policies, sometimes referred to as integrity checking, which could be as simple as verifying that the device connecting has anti-virus or the latest updates.

Seven of the nine participants or seventy-eight percent (78%) expressed concern regarding device ownership with P3 stating "if you (the institution) don't own the device, you still need to have some control of the device when it connects to your network." Participants, 1, 4, 5, 6, 7, and 9 expressed similar sentiments. P1 added that a decade ago, most machines were windows based — now there must be diversity in operating systems, and meeting the challenge is often difficult. All nine participants (100 %) expressed concern regarding the number of digital devices on campus. Participant 8 stated that a noticeable increase in the number of attempted connections to the network occurs in August and January. This time frame coincides with students purchasing or receiving

gifts of new technology devices or gadgets for the start of the academic year and as Christmas presents. Student innovators influencing students to buy or request digital devices is a classic example of Rogers's diffusion of innovation theory. In this case, both sets of students are among Rogers's five categories of adopters and based upon when they adopt the innovation the student might be an innovator, early adopter, early majority, late majority, or a laggard. Students who have not yet purchased a digital device could be influenced to do so by their peers. Being shown the relative advantage, compatibility, and even the complexity of the devices they witness being used on campus as well possibly trying the gadget before purchasing the item may impact selection. These are all characteristics of DOI theory that can influence the rate of adoption. Participant 8 allowed me to view network logs for the academic 2018-2019 year. There was a noticeable upswing in network connections in August 2018 and January 2019.

Group 1 consists of participants 1, 6, and 7; each of these community colleges had less than 2000 students during the 2018-2019 academic year. All participants (100%) of Group 1indicated they used Network Access Control (NAC) as their primary security solution for BYOD on campus. Participant 6 stated, "it (NAC) reduces my risk as it enforces policy on devices that access the institution's network." Participant 7 noted that with the use of Unified Endpoint Management (UEM), there was "less concern with patch rollouts as UEM can be set up to monitor devices and act on them as they come online." One of the shared documents was a lengthy email conversation in which the CIO outlined the use of MDM and NAC to IT departmental staff. Throughout the discussion it is clear that opinions regarding the use of MDM and NAC were changed from negative to

positive which is a fundamental principle with diffusion of innovation. Diffusion of innovation theory is centered on the premise that an individual may move to embrace a new product or service depending on how and who presents the innovation to them (Rogers, 2003; Xiong et al., 2016). The document is an example of diffusion of innovation in motion with the CIO influencing staff members to accept the change and to support it. Table 3 highlights the number of participants and the number of references in documents from Group 1 supporting the technology management tools theme.

Table 3

Frequency of Theme 1: Technology Management Tools Among Group 1 Participants and Documentation

	Mobile device management (MDM)	Network access control (NAC)	Firewalls (f)	Unified endpoint management (UEM)
Participants	2	3	3	1
documents	3	3	3	0

Group 2 contains community colleges with more than 2000 but less than 5000 students and consists of participants, 2, 3, and 4. All participants of Group 2 (100%) noted that the use of a firewall coupled with MDM was the selection for their colleges. Participant 4 indicated that MDM and the firewall "did not play well together in the DMZ until he was able to work out a few quirks." Zahadat et al. (2015) remarked that of the various frameworks available, it is typically MDM to which IT managers go first. The number of participants of this study who use MDM as a technology management tool supports Zahadat et al., (2015) work. The use of MDM software allows the user to keep personal data separate while the IT department can control how the device accesses

network data. Other aspects of MDM software include requiring a password, remotely locking or unlocking the device, and encrypting and decrypting data (Spangler et al., 2016). Participant 3 stated that "having the MDM server behind the enterprise firewall saved us from several internet attacks on the system." Participant 3 also shared a proof of concept document written a year prior that outlined the advantages of MDM and that such benefits would be a valuable addition to the rollout of a BYOD policy establishment on campus.

Table 4 highlights the number of participants and the number of references in documents from Group 2 supporting the technology management tools theme.

Table 4
Frequency of Theme 1: Technology Management Tools Among Group 2 Participants and Documentation

	Mobile Device Management (MDM)	Network Access Control (NAC)	Firewalls (f)	Unified Endpoint Management (UEM)
Participants	3	2	3	1
Documents	4	4	4	1

Group 3 contains community colleges with more than 5000 students. All three participants in Group 3 (100%) remarked that they wanted it all; MDM, NAC, Firewalls, and Unified Endpoint Management (UEM), working together to protect their networks. Group 3, consisting of Participants 5, 8, and 9, shared five (5) documents, three implementation plans, one network statistics document, and a proposal for future implementation. Table 5 highlights the number of participants and the number of documents received from Group 3 (Participants 5, 8, and 9) supporting the technology management tools theme.

Table 5
Frequency of Theme 1: Technology Management Tools Among Group 3 Participants and Documentation

	Mobile Device Management (MDM)	Network Access Control (NAC)	Firewalls (f)	Unified Endpoint Management (UEM)
Participants	3	3	3	3
Documents	5	4	5	2

Table 6 integrates the data from all nine participants for a broader look at the results related to the technology management tools theme from Group 1, Group 2, and Group 3. The total number of participants in the study was nine (9), and from those nine (9), a total of twelve (12) documents were reviewed. The numbers in Table 5 are not limited to a single document, meaning that two or more of the tools may appear in the same document. Only five of the nine participants (56%) brought up Unified Endpoint Management, and it was mentioned in 25 percent (25%) of the documentation. All nine research participants confirmed that the use of firewalls was a principal tool in their strategies. The findings also reveal that CIOs prefer to use multiple technology management tools to increase the likelihood of reaching their goal – successfully managing BYOD on campus. Participants noted that having a well-developed plan was of utmost importance.

Table 6
Frequency of Theme 1: Technology Management Tools Among Groups 1, 2, and 3 Participants and Documentation

	Mobile Device Management (MDM)	Network Access Control (NAC)	Firewalls (f)	Unified Endpoint Management (UEM)
Participants	8	8	9	5
Documents	12	11	12	3

The primary table for theme 1 (Table 6) includes information from the three sub-tables for Group 1 (Table 3), Group 2 (Table 4), and Group 3 (Table 5). Table 5 indicates that eight out of nine research participants are using MDM (Mobile Device Management) as well as Network Access Control (NAC) as part of their arsenal of technology management tools. This study supports Kearns' (2016) work that indicated MDM could be used to control the wireless distribution of data along with applications on smart devices such as phones, tablets, notebooks, and laptops. All nine of the research participants indicated they used firewalls. The widespread use of firewalls across Groups 1, 2, and 3 support Khelf and Ghoualmi-Zine's (2018) work showing firewalls are convenient to use and are reliable in determining what is or is not legitimate traffic. It is not the size of the institution that determines if technology management tools should be used to protect an institution's IT infrastructure but the CIO's awareness of potential dangers and the best methods for keeping them at bay.

The theme of technology management tools aligns with the diffusion of innovation theory, the conceptual framework for this study, in that it is the function of the CIO to lead the organization's technology platform in the right direction by making the right choices. As CIO, this individual might rely on new or emerging technologies in IT. Challenges may include lack of buy-in, lack of or unfamiliarity with process discipline, inability to determine the innovation's value, and ultimately the buying process. Some will follow the CIO on reputation alone; others will require more. To obtain the appropriate approvals, the CIO must know his audience and address presentations and such appropriately. Some individuals or departments may need additional information or

even a demonstration before they are on board with the emerging technology, application, or tool. Addressing each of these items can be accomplished within Rogers's (2003) diffusion of innovation theory.

Technology management tools are critical parts of the CIO's arsenal used to protect and secure the college's network. As in this study, previous research by Zahadat et al. (2015) concluded that it is MDM to which IT managers go first. Selecting an MDM system is a popular selection due in part to its functionality that includes the management of policy, security, and inventory, all of which support an IT department, according to Dang-Pham and Pittayachawan (2015). The works of Downer and Bhattacharya (2015), and Vignesh and Asha (2015) support the use of Network Access Controls (NAC) as part of a networking solution for BYOD. The security offered by NAC made NAC's use, a practical choice as a strategy by eight of this study's participants. Another component of technology management tools is the use of firewalls. As noted by Kruse et al. (2017), firewalls can be used in securing an organization's network while also preventing unauthorized access to the protected information that resides on the network. All nine study participants acknowledged the use of a firewall as an integral part of protecting and securing the college's network.

Theme 2: Importance of Security Awareness Training

The second resultant theme from participants was the importance of security awareness for students, institutional staff, and the IT staff. The emergence of new digital devices and their associated technologies have ensured that BYOD has become an integral part of students' lives, and with this acceptance comes the challenges of security

(Dang-Pham & Pittayachawan, 2015). Yet, one of the most significant pitfalls to securing personal information and even a mobile device is the user (Innocenzi et al., 2018; Peker et al., 2016). Pinchot and Paullet (2015) noted that although many mobile device owners have experienced malware attacks, most users are unfamiliar with preventive measures. Seven of nine participants noted that security classes were needed for students, as many were unfamiliar with preventive measures available or how to perform the task. There are multiple perspectives regarding security awareness on a college campus. First, there are the institution's students, followed by the institution's staff and then the institution's IT staff. All nine participants indicated that students, staff, and IT personnel should receive some form of security awareness training. Six participants regularly participated in workshops aimed at increasing student's knowledge of how to keep their personal information secure when online. Each group should receive security awareness training. According to participant 9, educating students to recognize insecure mobile security practices such as not updating anti-virus software, allowing others to use the device, or not acknowledging the risk of using public or personal networks is essential. Seven of nine participants indicated all college staff members have a requirement to view a security awareness video annually. Eight of nine participants noted that Human Resources (HR) kept track of the required pieces of training. One participant reported disappointment that the same computer-based instruction video has had no updates for three years. The existing literature supports the theme of security awareness. Ghafir et al. (2018) noted that the University of North Carolina identified computer-based training (CBT) as the delivery method of choice for training and IT managers. A noted drawback

to CBT is the lack of opportunity for the individual viewing to ask questions (Ghafir et al., 2018).

To develop this theme, I collated information gathered from the participants, analyzed data from the organizational documents provided, and the findings of existing research on the topic. The results of this study demonstrate how security awareness is in alignment with existing literature.

Participant 1 indicated a fondness for hosting face-to-face security workshops for students and pointed out that such activities might not be possible on a sprawling, more spread out campus. Participant 8 described delegating the security officer to work with eLearning instructional designer to develop an in-house computer-based training for students regarding online safety. Eight participants expressed their concern regarding how to ensure both staff and students are made aware of and adhere to security policies and procedures. Participant 1 noted that the majority of students seen on campus have a smartphone in their hand, if not a laptop.

Table 7 highlights the number of participants and the number of documents that referenced security awareness from Group 1 (Participants, 1, 6, and 7) supporting Theme 2 importance of security awareness. Group 1 participants are from community colleges with fewer than 2000 students during the 2018 academic year. In Group 1, all three participants regarded security awareness as being an essential aspect of their strategy to mitigate IT infrastructure demands produced by student BYOD usage on campus.

Table 7

Frequency of Theme 2: Importance of Security Awareness Among Group 1 Participants

	Security Awareness

Participants	3
Documents	3

The documentation from Group 1 participants that referenced the importance of security awareness (Theme 2) consisted of; an IT departmental flyer directed at students advocating for strong passwords, a handout from an online safety workshop, and an announcement regarding yearly security training for staff. All three documents communicated the need for good security practices, and one provided guidelines related to passwords and their storage. Each communication offers an opportunity to heighten an individual's security outlook. Presenting security awareness training at a level comparable with the individual's role will help instill better security awareness practices. These documents show a consistent message to staff and students – security is essential. Participant 6 indicated organizational emails are sent to staff and students when phishing attacks are occurring or have occurred. Such emails serve as reinforcement that users would be wary of personal information solicitations.

Table 8 highlights the number of participants and the number of documents from Group 2 participants that support Theme 2 security awareness. Group 2 participants are from community colleges with more than 2000 but less than 5000 students.

Table 8

Frequency of Theme 2: Importance of Security Awareness Among Group 2 Participants

	Security Awareness
Participants	3
Documents	2

The documentation provided by Participants 2, 3, and 4 that related to Theme 2 – Importance of Security Awareness Among Group 2 participants included an email regarding a phishing attack and an announcement to staff about using the college's Virtual Private Network (VPN) when traveling. Participant 2 stated that the IT department periodically holds workshops for students on how to stay safe online. Notifying students during an ongoing phishing attack may help to stop the attack by fewer students opening a suspicious email, and may serve as a memory jogger when they distrust an email. Communication is crucial for users if they are to understand both the purpose and benefit of a BYOD strategy (Brodin, 2017).

Table 9 highlights the number of participants and the number of documents received from Group 3 supporting Theme 2 security policies and security. Group 3 participants were from community colleges with more than 5000 curriculum students during the 2018 academic year. All three of the participants regarded security awareness as being fundamental to their strategies relating to BYOD.

Table 9

Frequency of Theme 2 – Importance of Security Awareness Among Group 3 Participants

	Security Awareness
Participants	3
Documents	1

The document received from a Group 3 participant consisted of a flyer with instructions for installing a VPN on a college device. These directions also included a troubleshooting guide that provided reminders about security awareness, such as; strong passwords, staying safe in public places, etc. Participant 5 stated that the IT department

works with the computer science department to host a workshop for new students during an open house. The workshop included items such as password safety and strength as well as using 2-factor authentication on devices used for school. Participant 9 indicated an email went to everyone announcing college would be going to 2-factor authentication. Participant 8 indicated IT department no longer participated in workshops but did send out regular email reminders about security to students.

Table 10A integrates the data from Groups 1, 2, and 3 for a broader look at the results related to theme 2 – Importance of Security Awareness. There were nine participants in total, and from those nine (9) participants, I received a total of six (6) documents. All nine of the participants (100%) acknowledged the importance of security awareness to their strategies to mitigate IT infrastructure demands produced by student BYOD usage on campus.

Table 10A

Frequency of Theme 2: Importance of Security Awareness Among Group 1, 2, and 3 Participants

	Security Awareness
Participants	9
Documents	6

Table 10B illustrates the different types of approaches used by participants to heighten security awareness. The findings also revealed that the majority of CIOs (seven out of nine) directly involved themselves or their staffs in hosting security workshops for staff and students of their respective colleges. The findings here indicate support for Bello et al., (2017) recommendation that security awareness and training be a part of a multifaceted policy-based management tool used by management. Also supported is

Innocenzi et al. (2018) suggestion that improving the security posture of one individual improves the security posture of the entire organization.

Table 10B

Frequency of Theme 2: Types of Security Awareness Approaches used by Participants

Security Awareness Approaches	P1	P2	P3	P4	P5	P6	P7	P8	P9
Assigned Login	X	X	X	X	X	X	X	X	X
Unique Password	X	X	X	X	X	X	X	X	X
Strong Password	X	X				X		X	X
Workshops for Staff and Students	X	X	X	X	X		X		X
Student email on Security Awareness						X		X	X
Staff Mandatory Training	X	X	X	X	X	X		X	
Computer Based Training for Students	X								X
Computer Based Training for Staff	X	X	X	X	X	X	X	X	X
Require Password Change Yearly for Students	X	X						X	
No Requirement for Students to Change Password			X		X		X		

Throughout this study, it became clear that all of the participants felt strongly about security awareness and wanted to involve staff and students. Existing research such as Bello et al., (2017) noted that regular awareness and training programs might impact how employees and students react when faced with BYOD security issues supports theme 2 of this study. Group 1, Group 2, and Group 3 each sought ways to have security at the forefront. Overall, seven of nine participants specified all staff members, at their respective colleges, have a requirement to view a security awareness video annually. When an incident, such as a phishing attack, occurred, email notifications went out as reminders of appropriate behavior. BYOD and mobile learning come with inherent risks. Students, faculty, and staff should be aware of the associated security risks, and

reminders, along with training, are appropriate avenues towards increased security awareness. The more security awareness that a college student or staff member has personally, the more secure is the college network. I established that CIOs successfully use various communication methods to increase security awareness as a whole and specifically to their respective systems. Increased security awareness may mitigate IT infrastructure demand produced by student BYOD usage on campus.

Existing literature supports the data collected in this study. Based on the results of this study, there is a need for security awareness training. Such training is a worthwhile endeavor, and any such effort should take into account an individual's roles and their association with the network and tailor communication to fit.

The theme of security awareness aligns with the diffusion of innovation theory, which served as this study's conceptual framework. One of the critical components of the diffusion of innovation theory is communication. According to Rogers (2003), everything from one-on-one conversations about the innovation to mass media blitzes would fall under a broad definition of communication. All nine participants indicated that security awareness training was a necessary component for students, staff, and IT staff. This strategy is supported in previous research as, according to Peker et al., (2016), a cybersecurity awareness program seeks to change a user's behavior by providing information that will impact the user's daily actions. Innocenzi et al. (2018) stated that educating students in information security practices improve the information security posture of the entire institution.

Theme 3: The Importance of BYOD Security Policies and Procedures

The third theme developed from this study was BYOD Security Policies and Procedures. The IT infrastructure issues associated with BYOD include adapting local infrastructure to accommodate more devices, different types of devices, and predicting new technology and its demands, and growing current infrastructure to allow institutional systems to work on a wide-range of user-provided technology (Jarrahi et al., 2017). Institutions with BYOD should establish a multifaceted policy-based management model that includes: security standards and procedures, technical controls, security awareness and training, user perception, and user behavior (Bello et al., 2017). BYOD also brings new security challenges such as establishing policies to protect the college IT infrastructure, protecting the personal information of employees and students, as well as the corporate data of the college (Dang-Pham & Pittayachawan, 2015; Kiernan, 2016). While establishing policies, one must look towards the "what if" and determine proactive and reactive procedures that will guide responses should the "what if" occur. One of the procedures that could be implemented with BYOD security is the use of a Virtual Private Network (VPN). A VPN protects the communication channel, but only when data is in transit stated Ali et al. (2015), while Downer and Bhattacharya (2015) added that a VPN is focused on protecting internal resources. A tabletop exercise scenario involving a ransomware scenario led to modifications of the college's BYOD procedures stated participant 4.

To develop this theme, I analyzed data from the participants, from the organizational material provided, and from findings of existing research on the topic. I

established that CIOs successfully use security policies and procedures as a strategy to mitigate IT infrastructure demand produced by student BYOD usage on campus.

All nine participants (100%) indicated that BYOD is here to stay. Seven out of nine participants noted IT departments struggle somewhat to keep up with BYOD's fast-paced changes. BYOD has brought new risks to IT departments. As pointed out by seven participants, the more traditional security measures are not sufficient, and as such, the participants regularly review their specific BYOD policies and revise as necessary. All nine participants (Participant 1-9), spoke about the need for policies and procedures to be in place and understood by their teams. The challenge facing IT departments is to improve the accessibility of services for students while maintaining a security posture that thwarts security attacks (Chou et al., 2017; Kao et al., 2015). I found that participants successfully use carefully constructed security policies and procedures as one strategy to mitigate the IT infrastructure demand produced by student BYOD usage on campus. This supports research indicating that a BYOD policy should make clear the organization's security requirements and the steps for compliance (Alotaibi & Almagwashi, 2018; Pinchot & Paullet, 2015).

As a result of the semistructured interviews with participants, I found that as previous research had observed, the theme of BYOD security policies and procedures is problematic in its implementation. Seven of the nine participants indicated that communicating security policies and procedures is difficult. Eight of nine participants alluded to a yearly training requirement for staff that was computer-based training, and also stated no such condition exists for students.

In Group 1, two participants out of three cited the need for reactive as well as proactive procedures as being essential for the protection of information. The challenge facing IT managers is to improve the accessibility of services for students with maintaining a security posture that thwarts security attacks (Chou et al., 2017; Kao et al., 2015). There is a fine line between improving student accessibility via digital devices and ensuring the network remains secure, and CIOs must find a balance. All three members of Group 1, participants 1, 6, and 7 indicated that to thrive, colleges must accept and adapt to BYOD. According to participant 7, the overarching question is still can we secure the college's data and continue to have BYOD.

Table 11 below highlights the number of participants and the number of references in documents from Group 1 (Participants, 1, 6, and 7) supporting Theme 2 security policies and security.

Table 11
Frequency of Theme 3: BYOD Security Policies and Procedures Among Group 1 Participants

	BYOD Security Policies and Procedures
Participants	3
Documents	3

The following policies and procedures were noted as being successful by the participants of Group 1;

- Establishing IT governance;
  - Who can connect, how and to what information,
  - multi-factor authentication,
  - policy and procedure to investigate breach or attempted breach
- Security and compliance;
  - Multi-factor authentication,
  - use of MDM or MAM to allow policy enforcement

- Understanding the organizational and student culture
- Training

The documentation from Group 1 participants that referenced the importance of BYOD Security Policies and Procedures (Theme 3) consisted of; an IT departmental flyer directed at students advocating for strong passwords, a handout from an online safety workshop, email to IT staff regarding a change to a policy, and an announcement regarding yearly security training for staff. Participant 6 indicated organizational emails are sent to staff and students regarding procedures when justified such as during a phishing attack to remind users to report emails that solicit personal information. The documentation provided by Group 1 shows a consistent effort to inform students and staff of policies and procedures regarding BYOD. DOI theory depends upon communication to foster the adoption of an innovation. Group 1 has established a line of communication with both students and staff concerning BYOD policies and procedures.

In Group 2, two out of three participants cited the need for reactive as well as proactive measures as being essential for the protection of information. All three participants of Group 2 (Participants 2, 3, and 4) indicated a college requirement for yearly training regarding information security. Participant 3 noted that every IT staff member should be on the lookout for problems. A vital component of the diffusion of innovation theory is communication. According to Participant 2, the college's BYOD policies are explained to students during their new student orientation; where they also receive information about password requirements, The actions of the research participants support Bello et al., (2017) suggestion that regular awareness and training

programs may impact how employees and students react when faced with BYOD security issues. Participant 4 noted that as a result of the latest tabletop exercise scenario involving a ransomware scenario, modifications to the college's BYOD policy and several other IT procedures were necessary.

Participants 4 and 5 indicated that security for BYOD must take precedence as unsecured devices are vulnerable to attack and to being used as an attack point. In the existing literature, Bello et al., (2017) suggest the use of a multifaceted policy-based management model that includes: security standards and procedures, technical controls, security awareness and training, user perception, and user behavior is necessary for BYOD security.

Table 12
Frequency of Theme 3: BYOD Security Policies and Procedures Among Group 2 Participants

	BYOD Security Policies and Procedures
Participants	3
Documents	3

The following policies and procedures were identified as being successful by the participants of Group 2;

- Establishing IT governance;
  - Who can connect, how and to what information,
  - multi-factor authentication,
  - policy and procedure to investigate breach or attempted breach
- Security and compliance;
  - Multi-factor authentication,
  - use of MDM or MAM to allow policy enforcement
- Understanding the organizational and student culture
- Training

The documentation provided by Participants 2, 3, and 4 that related to Theme 3 – BYOD Security Policies and Procedures included two emails regarding phishing attacks, a copy of college's BYOD policy, and an announcement to staff about using the college's Virtual Private Network (VPN) when traveling. According to Participant 2, the IT department regularly holds workshops for students on how to stay safe online and includes information about phishing, password management, and other suspicious online activity. Notifying students during an ongoing phishing attack may help to stop the attack by fewer students opening a suspicious email, and may serve as a memory jogger when they distrust an email. Communication is crucial for users if they are to understand both the purpose and benefit of a BYOD strategy (Brodin, 2017). The announcement regarding the Virtual Private Network summarizes the college's BYOD policy and provides its location. According to Participant 3, the college makes available a copy of its BYOD policy to every new employee as a way of ensuring the new employee is aware that there is a policy.

Group 3 consists of Participants, 5, 8, and 9. These participants represent community colleges with more than 5000 students during the 2018 academic year. In Group 3, all three participants (Participants 5, 8, and 9) indicated both reactive and proactive measures as being essential for the protection of information. Recent literature supports the theme BYOD security policies and procedures as a strategy CIO can use to mitigate IT infrastructure demands produced by student BYOD usage. Information security policies and procedures must be up to date and enforced if a college's information is to be actively protected. No one wants to be the victim of a data breach;

however, every organization should be preparing for one. Participant 8 stated, “Our policies and procedures are such that we expect the best outcomes, and we prepare for the worst outcome.” According to Participant 9, recent attendance at a college departmental meeting to explain a change in procedures had led to changes in a presentation, the procedural instructions, and the policy as a result. Hosting a demonstration and revising it for the next group is an example of Rogers’s (2003) DOI theory in action. Rogers (2003) notes that different groups may need a slightly different message delivered to them before adopting the innovation.

Participant 5 indicated that each year, the IT department reviews its current policies and procedure to determine if changes are warranted and if so, dissemination of the changes takes place. Participants 8 and 9 also indicated that regularly scheduled reviews of all IT policies and procedures did take place. Bauer, Bernroider, and Chudzikowski (2017) noted that for an organizations’ information to be secure two things must occur 1) the organizations’ security policies and procedures are up to date, and 2) employees of an organization must comply with and actively follow its security policies and procedures.

DOI theory drove this study by identifying strategies that CIOs have found successful in mitigating the IT infrastructure demands produced by student BYOD usage on campus. Using the doi theory, it is also possible to determine how CIOs go about gaining acceptance for and adherence to these strategies.

Table 13 highlights the number of participants and the number of references in documents from Group 3 supporting Theme 3 BYOD security policies and security.

Table 13
Frequency of Theme 3: BYOD Security Policies and Procedures Among Group 3 Participants

	BYOD Security Policies and Procedures
Participants	3
Documents	2

The following policies and procedures were noted as being successful by the participants of Group 3;

- Establishing IT governance;
  - Who can connect, how and to what information,
  - multi-factor authentication,
  - policy and procedure to investigate breach or attempted breach
- Security and compliance;
  - Multi-factor authentication,
  - use of MDM or MAM to allow policy enforcement
- Understanding the organizational and student culture
- Training

There were two documents provided by Group 3 participants; a copy of the IT committee charter and a proposed revision to BYOD college policy. The committee charter indicates the composition of the group to be a mix of IT staff members, non-IT staff members, and students. Participant 5 indicated that positive outcomes had manifested themselves as a result. The document with the proposed revision to the college's BYOD policy included current and proposed wording, as well as indicating why the change was necessary. The proposed revision to the college's BYOD policy serves as a written communication that will spread throughout the workforce, notifying each of a change in policy. The IT committee serves as several conduits for doi theory.

Although there will be minutes of meetings, such are not usually widespread. However, committee members talk to other staff and students and could be influencers for others.

Table 14 highlights the number of participants and the number of references in documents from Groups 1, 2, and 3 supporting Theme 3 BYOD security policies and security. Eight out of nine participants cited the need for reactive as well as proactive procedures as being essential for the protection of information. This study aligns with the existing literature that I reviewed in that appropriate security policies and procedures are vital to the success of an organization. The findings support the conceptual framework used for this study; the diffusion of innovation (Rogers, 2003). The structure of DOI theory allows CIOs to put forward a new or revised policy or procedure; have it seen as an innovation and to seek acceptance via the diffusion process, which involves an accumulative adoption. For example, the potential adopter (staff) develops an awareness of the innovation (VPN). They become aware of the likely need for innovation (ease of use, and travel); the potential adopter will determine its relative advantage to themselves (ease of use) and decide to adopt the innovation (VPN) or not.

Table 14

Frequency of Theme 3: BYOD Security Policies and Procedures Among Group 1, 2, and 3 Participants

	BYOD Security Policies and Procedures
Participants	9
Documents	8

The following policies and procedures were identified as being successful by the participants of Groups 1, 2, and 3;

- Establishing IT governance;

    - Who can connect, how and to what information,
    - multi-factor authentication,
    - policy and procedure to investigate breach or attempted breach
- Security and compliance;
    - Multi-factor authentication,
    - use of MDM or MAM to allow policy enforcement
- Understanding the organizational and student culture
  Training

The primary table for theme 3 (Table 14) includes information from the three sub-tables for Group 1 (Table 11), Group 2 (Table 12), and Group 3 (Table 13). Included in this table are the nine participants and the eight documents these individuals provided. The existing literature reviewed for this study is in alignment with the findings of the study by highlighting the importance of BYOD security policies and procedures.

The results of this study indicate that by using a diffusion of innovation approach to BYOD and its security policies and procedures, CIOs and their staff can inform college staff and students of the potential threats related to their digital devices. Two of the characteristics of DOI theory are its trialability and observability factors (Rogers, 2003). These concepts indicate that acceptance and adoption of an innovation can be influenced by an individual's ability to observe the innovation in action or to engage with the innovation via a 'try before you buy' mechanism. Both of these interactions could be accomplished within a security awareness workshop.

Data collected from the semistructured interviews and the organizational documents support the theme of BYOD security policies and procedures as one of the fundamental strategies a CIO could utilize to manage the BYOD demands successfully. Chou et al. (2017) noted that it is challenging for IT managers to improve services while

maintaining a positive security posture. Educational entities have FERPA, HIPPA, and PCI regulatory requirements to consider and address when developing security policies and procedures (Kiernan, 2016). Bello et al., (2017) asserted that without the appropriate security protocols or protective policies in place, there is an increased risk of an information breach. The findings of this study demonstrate how BYOD security policies and procedures are in alignment with existing literature

Applications to Professional Practice

The specific IT problem I sought to study was the identification of successful strategies used to mitigate IT infrastructure demands produced by student BYOD usage. Other CIOs or IT managers could utilize the strategies uncovered in this study to alleviate the requirements levied on the IT infrastructure by the ubiquitous phenomenon of BYOD. Participants of this study noted that their participation would contribute to the enhancement of their existing strategies.

The findings of this study, in conjunction with an analysis of its conceptual framework and a review of academic literature, add to the existing body of knowledge of BYOD strategies to increase security posture in general and, more specifically, in the area of cybersecurity. A cybersecurity awareness program seeks to modify a user's behavior by providing the individual with information in such a way that the individual alters their security posture (Peker et al., 2016). Innocenzi et al. (2018) stated that educating students in information security practices improve the information security posture of the entire institution.

The study's findings were significant and reinforced current literature on strategies on the impact of BYOD. The documents that were supplied by the community colleges provided insight into the strategies used. Findings from this study have revealed the successful strategies that are currently in use on educational campuses throughout NC. These strategies impact users' satisfaction as well as strengthen the IT infrastructure. By providing successful strategies, other organizations may adopt comparable strategies to improve their BYOD interactions. The findings of this study may benefit IT managers by providing insight into the essential strategies uncovered in this study, which could be used to form the basis of a new and improved security approach for their organization.

This study's application to professional practice includes sharing the successful strategies CIOs used to protect their institutions while allowing BYOD to flourish. The results of my research indicate that the application of successful BYOD strategies might provide other CIOs a guide to assessing and mitigating BYOD issues. The findings in my study align with the diffusion of innovation theory in which Rogers proposed that new ideas spread and gained acceptance due to the innovation itself, communication about the innovation, time, and a social system.

Implications for Social Change

By identifying successful strategies for use with BYOD, CIOs are provided with additional tools that they may use to enhance the network's interaction with this phenomenon. The social change implications from this research include improving the quality of campus life for students and staff by maintaining a viable yet secure network and improving the security awareness of students and staff. The ubiquitous nature of

BYOD or symbiotic relationship between students and smart mobile devices is not going to go away. Smart mobile devices allow students to connect anywhere, anytime. These devices are typically always on and always searching for a network. IT infrastructure can be adversely affected due to the sheer volume of attempted connections. One of the most significant issues facing CIOs is the ever-changing student population and their lack of knowledge regarding the security measures put in place by the college to protect them. This qualitative multicase study filled a gap in BYOD related literature by providing the perspective of CIOs on the successful strategies they have implemented associated with BYOD. Such strategies, when implemented by CIOs or IT managers offer additional perspective on successful BYOD strategies. Identifying successful BYOD strategies empowers CIO, IT managers, and academic institutions to make changes within their domain. Mobile technologies, smart mobile devices and BYOD has and will continue to have an impact on social change. By providing an individual with the information and tools to improve their personal security posture, Innocenzi et al. (2018) demonstrate that the security posture of the entire organization is also enhanced. The strategies illustrated in this study may assist in positive social change by creating a more positive experience for students interacting with technology on campus, which could, in turn, impact their experiences elsewhere. This type of transformational social change occurs as successful experiences often influence other related areas.

Recommendations for Action

The purpose of this qualitative multicase study was to explore the successful strategies used by CIOs on community college campuses to mitigate BYOD demands on

IT infrastructure. This study focused on the examination of scholarly literature, the analysis of organizational documents, and the collection of data from research participant semistructured interview member checked responses. When combined, these activities provided corroborating support and triangulation in the data collection process to answer the research question of successful strategies that mitigate IT infrastructure demands produced by student BYOD usage on campus. Based on the NVivo 12 examination three major themes emerged: 1, technology management tools 2), security policies and procedures and 3) security awareness

The findings of this research study indicate research participants (a) have implemented BYOD policies and procedures to protect, defend and react to BYOD IT infrastructure demands; (b) are instrumental in campus security awareness campaigns; (c) use technology management tools to restrict or permit access to systems and information as necessary.

Based on the successful strategies identified in this research I recommend CIOs, IT Directors and IT managers consider the following when seeking improvements to their BYOD strategies;

1. Assess the health of the BYOD program by evaluating current BYOD posture, its risks, and vulnerabilities.

2. Develop and implement the policies and procedures which become a part of the strategic plan.

3. Assess in-house IT capabilities and determine if leveraging third-party vendor expertise is an option.

4. Develop security awareness training for employees and students.

Distribution of the findings of this study will take place once I have received CAO approval. Initially, the nine research participants will receive a two-page summary of my findings. The study will also be available via the ProQuest database, which is searchable by topics and keywords. I also plan on pursuing other avenues such as publicizing my research in scholarly journals and at academic conferences, all of which will expand the target audience.

Recommendations for Further Study

This study focused on identifying successful strategies that CIOs used successfully to manage BYOD on their respective community college campuses. However, additional research around this study topic could prove beneficial for all organizations that permit BYOD. This study's main limitation was the focus on strategies used by CIOs of community colleges located in NC. Recommendations for further studies include similar research using different types of organizations in different regions of the United States.

Research on this topic using a different design or methodology could prove to be beneficial. For example, a quantitative study could examine the issue from the student perspective. Finally, this study has contributed to the body of literature on BYOD, but additional research may prove beneficial to the IT industry and academic communities.

Reflections

During this entire research process, my knowledge and understanding of what it takes to complete a doctoral research project have grown. Developing and completing a

doctoral study has been one of the hardest academic endeavors I have accomplished. There were academic and personal challenges on this journey. At times it seemed impossible.

The participants appeared energized by the topic as it is one they continue to grapple with each semester. Participants of this study were willing to share their time and discuss their successful BYOD strategies. The depth of information the participants provided during the semistructured interviews and through documentation was unexpected and added to the study. I have Officer in Charge experience, which includes many of the CIO duties. Identifying and implementing successful strategies is not an easy task. I actively sought to remove any personal biases, lest they influence my interaction with the participants.

Throughout the semistructured interview, I followed an interview protocol and asked open-ended questions so as not to lead the participant in any direction. I found the results interesting and informative. Just as I was the main instrument for data collection, I also reviewed and analyzed the data. During a follow-up member checking session, each participant was provided with a verbatim transcript to verify the accuracy of my interpretations. While each participant had their perspective regarding the research topic, the similarities in what they were trying to accomplish were unmistakable. The organizational documents provided by the participants were triangulated with data received from the participant interviews, and member checking transcripts. The findings from this study identified successful strategies that a CIO can use to manage BYOD or digital devices on the network.

Summary and Study Conclusions

Developing successful strategies to successfully manage BYOD or the burgeoning influx of digital devices arriving on campus is critical. The objective of this qualitative multicase study was to investigate the successful strategies put into place by CIOs to mitigate the effects of BYOD. Methodological triangulation included transcripts of semistructured interviews, and the member checking sessions along with organizational documents all helped to answer this study's research question. After completing data collection and analyzing the data, three themes emerged (a) technology management tools, (b) security strategies, and (c) security awareness.

There were nine CIOs from a cross-section of North Carolina Community Colleges who participated in semistructured interviews, member checking sessions, and provided organization documentation. To compile and analyze the data, I used a purpose-built software application that supports qualitative research – NVivo version 12 Plus. This software has features that support thematic analysis while being robust enough to house a myriad of data types. I was able to use NVivo to organize the collected data into themes.

The study's primary findings confirm that there are successful strategies that can be employed to manage the growing BYOD movement successfully. The study's findings can benefit CIOs in other community colleges or companies who are looking for successful strategies to successfully manage BYOD and the digital device movement.

References

Abro, M. M. Q., Khurshid, M. A., & Aamir, A. (2015). The use of mixed methods in management research. *Journal of Applied Finance & Banking, 5*(2), 103-108. Retrieved from http://www.scienpress.com

Adams, C., Yin, Y., Vargas Madriz, L. F., & Mullen, C. S. (2014). A phenomenology of learning large: The tutorial sphere of xMOOC video lectures. *Distance Education*, *35*(2), 202-216. doi:10.1080/01587919.2014.917701

Adhikari, J., Scogings, C., Mathrani, A., & Sofat, I. (2017). Evolving digital divides in information literacy and learning outcomes: A BYOD journey in a secondary school. *International Journal of Information and Learning Technology, 34*(4) 290-306. doi:10.1108/IJILT-04-2017-0022

Ahn, J., & Jung, Y. (2016). The common sense of dependence on smartphone: A comparison between digital natives and digital immigrants. *New Media & Society*, *18*(7), 1236-1256. doi:10.1177/1461444814554902

Al-Emran, M., Elsherif, H. M., & Shaalan, K. (2016). Investigating attitudes towards the use of mobile learning in higher education. *Computers in Human Behavior*, *56*, 93-102. doi:10.1016/j.chb.2015.11.033

Al-Falahy, N., & Alani, O. Y. (2017). Technologies for 5G networks: Challenges and opportunities. *IT Professional*, *19*(1), 12-20. doi:10.1109/MITP.2017.9

Alhassan, R. (2016). Mobile learning as a method of ubiquitous learning: Students' attitudes, readiness, and possible barriers to implementation in higher education. *Journal of Education and Learning*, *5*(1), 176. doi:10.5539/jel.v5n1p176

Ali, M. N. B., Hossain, M. E., & Parvez, M. M. (2015). Design and implementation of a secure campus network. *International Journal of Emerging Technology and Advanced Engineering*, *5*(7), 370-374. Retrieved from www.ijetae.com

Ali, S., Qureshi, M. N., & Abbasi, A. G. (2015) Analysis of BYOD security frameworks, (2015). *2015 Conference on Information Assurance and Cyber Security (CIACS)*, Rawalpindi, 2015, pp. 56-61. doi:10.1109/CIACS.2015.7395567

Ali, S. M. B. M., Razak, M. R. A., Amran, A. R., Salim, S., & Tahir, M. G. M. (2016). End to end solution for campus environment to improve the WLAN network performance and security. *Journal of Engineering Technology*, *4*, 10-14. Retrieved from https://journals.adrri.org/

Ally, M., & Prieto-Blázquez, J. (2014). What is the future of mobile learning in education? *International Journal of Educational Technology in Higher Education*, *11*(1), 142-151. doi:10.7238/rusc.v11i1.2033

Almarhabi, K., Jambi, K., Eassa, F., & Batarfi, O. (2017). Survey on access control and management issues in cloud and BYOD environment. *International Journal of Computer Science and Mobile Computing, 6*(12), 44-54. Retrieved from http://www.ijcsmc.com/

Alotaibi, B., & Almagwashi, H. (2018). A Review of BYOD security challenges, solutions and policy best practices. *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, 2018, pp. 1-6. doi:10.1109/CAIS.2018.8441967

Alrasheedi, M., & Capretz, L. F. (2015). Determination of critical success factors affecting mobile learning: A meta-analysis approach. TOJET: *The Turkish Online Journal of Educational Technology, 14*(2). 41-51. Retrieved from tojet.net.

Alshalan, A., Pisharody, S., & Huang, D. (2016). A survey of mobile VPN technologies. IEEE Communications Surveys & Tutorials, *18*(2), 1177-1196. doi:10.1109/COMST.2015.2496624

Andersen, J. B. (2017). History of communications/radio wave propagation from Marconi to MIMO. *IEEE Communications Magazine, 55*(2), 6-10. doi:10.1109/MCOM.2017.7841460

Arora, H. D., & Dhiman, A. (2015). Comparative study of generalized quantitative-qualitative inaccuracy fuzzy measures for noiseless coding theorem and 1:1 codes. *International Journal of Mathematics & Mathematical Sciences, 4*, 20151-20156. doi:10.1155/2015/258675

Attal, R., & Rubenfeld, S. (2017). Ethical issues in research. *Best Practice & Research Clinical Obstetrics & Gynaecology, 43*, 107-114. doi:10.1016/j.bpobgyn.2016.12.006

Aykol, B., & Leonidou, L. C. (2014). Researching the green practices of smaller service firms: A theoretical, methodological, and empirical assessment. *Journal of Small Business Management, 53*, 192-209. doi:10.1111/jsbm.12118

Baillie, L. (2015). Promoting and evaluating scientific rigour in qualitative research. *Nursing Standard, 29*(46), 36-42. doi:10.7748/ns.29.46.36.e8830

Barglowski, K., Bilecen, B., & Amelina, A. (2015). Approaching Transnational Social Protection: Methodological Challenges and Empirical Applications. *Population Space & Place*, *21*(3), 215-226. doi:10.1002/psp.1935

Barnham, C. (2015). Quantitative and qualitative research: Perceptual foundations. *International Journal of Market Research*, *57*(6), 837-854. doi:10.2501/IJMR-2015-070

Baškarada, S. (2014). Qualitative case studies guidelines. *The Qualitative Report, 19*(40), 1-18. Retrieved from http://nsuworks.edu

Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' noncompliance with information security policies in banks. Computers & Security, 68145-159. doi:10.1016/j.cose.2017.04.009

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report, 13*(4), 544-559. Retrieved from http://nsuworks.nova.edu

Bello, A. G. , Murray, D., & Armarego, J. (2017) A systematic approach to investigating how information security and privacy can be achieved in BYOD environments, *Information & Computer Security, 25*(4), 475-492. doi:10.1108/ICS-03-2016-0025

Berbary, L. A. (2014). Too good at fitting in: Methodological consequences and ethical adjustments. *International Journal of Qualitative Studies in Education, 27*, 1205-1225. doi:10.1080/09518398.2013.820856

Berger, R. (2015). Now I see it, now I don't: Researcher's position and reflexivity in qualitative research. *Qualitative Research*, *15*(2), 219-234. doi: 10.1177/1468794112468475

Bezzina, F., & Saunders, M. (2014). The pervasiveness and implications of statistical misconceptions among academics with a special interest in business research methods. *The Electronic Journal of Business Research Methods, 12*(2). 29-42. Retrieved from www.ejbrm.com

Bhat, S., Gijo, E., & Jnanesh, N. (2014). Application of lean six sigma methodolgy in the registration process of a hospital. *International Journal of Productivity & Performance Management, 63*, 613-643. doi:10.1108/IJPPM-11-2013-0191

Bichsel, J. (2015). IT service delivery in higher education: Current methods and future directions. *Research Report*. Louisville, CO: ECAR, 2015. Retrieved from http://www.educause.edu/ecar.

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation?. *Qualitative Health Research*, *26*(13), 1802-1811. doi:10.1177/1049732316654870

Briz-Ponce, L., & Juanes-Méndez, J. A. (2015). Mobile devices and apps, characteristics and current potential on learning. *Journal of Information Technology Research. 8*(4), 26-37. doi:10.4018/JITR.2015100102

Briz-Ponce, L., Pereira, A., Carvalho, L., Juanes-Méndez, J. A., & García-Peñalvo, F. J. (2017). Learning with mobile technologies–students' behavior. *Computers in Human Behavior*, *72*, 612-620. doi.10.1016/j.chb.2016.05.027

Brodin, M. (2017). Mobile device strategy: From a management point of view. *Journal of Mobile Technologies, Knowledge and Society*, *2017*, 1-9. doi:10.5171.2017.593035

Brown, J. D. (2015). Characteristics of sound quantitative research. *SHIKEN, 19*(2) 24-28. Retrieved from http://teval.jalt.org

Cacari-Stone, L., Wallerstein, N., Garcia, A. P., & Minkler, M. (2014). The promise of community-based participatory research for health equity: A conceptual model for bridging evidence with policy. *American Journal of Public Health*, *104*(9), 1615-1623. doi:10.2105/AJPH.2014.301961

Castillo-Manzano, J. I., Castro-Nuño, M., López-Valpuesta, L., Sanz-Díaz, M. T., & Yñiguez, R. (2017). To take or not to take the laptop or tablet to classes, that is the question. *Computers in Human Behavior*, *68*, 326-333. doi:10.1016/j.chb.2016.11.017

Cheboi, S., & Mberia, H. (2014). Efficacy of interpersonal communication channels in the diffusion and adoption of zero grazing technology. *International Journal of Academic Research in Business and Social Sciences*, *4*(9), 352. doi:10.6007/IJARBSS/v4-i9/1164

Cheng, G., Guan, Y., & Chau, J. (2016). An empirical study towards understanding user acceptance of bring your own device (BYOD) in higher education. *Australasian Journal of Educational Technology*, *32*(4). Retrieved from ajet.org.au

Chin, A. G., McRae, D., Jones, B. H., & Harris, M. A. (2016). An Exploration of Mobile Device Security Artifacts At Institutions Of Higher Education. *Journal of*

International Technology and Information Management, *25*(3), 27-52. Retrieved from https://scholarworks.lib.csusb.edu/jitim/vol25/iss3/4

Chitanana, L., & Govender, D. W. (2015). Bandwidth management in the era of bring your own device. *The Electronic Journal of Information Systems in Developing Countries*, *68*(1), 1-14. doi:10.1002/j.1681-4835.2015.tb00489.x

Chopra, A. (2016). Security Issues of Firewall. *International Journal of P2P Network Trends and Technology (IJPTT)*, 4-9. Retrieved from https://pdfs.semanticscholar.org/ce41/f4a5fa5c7c816038309c500f7cb5b230abf6.pdf

Chou, P. N., Chang, C. C., & Lin, C. H. (2017). BYOD or not: A comparison of two assessment strategies for student learning. *Computers in Human Behavior*, *74*, 63-71. doi:10.1016/j.chb.2017.04.024

Cleary, M., Horsfall, J., & Hayter, M. (2014). Data collection and sampling in qualitative research: does size matter?. *Journal of Advanced Nursing*, *70*(3), 473-475. doi:10.1111/jan.12163

Collins, C. S., & Cooper, J. E. (2014). Emotional intelligence and the qualitative researcher. *International Journal of Qualitative Methods, 13*(1), 88-103. doi:10.1177/160940691401300134

Cope, D. G. (2014). Methods and meanings: Credibility and trustworthiness of qualitative research. *Oncology Nursing Forum*, *41*(1), 89-91. doi:10.1188/14.ONF.89-91

Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *Nurse Researcher, 21*(5), 19-27. doi:10.7748/nr.21.5.19.e1240

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security*, *48*, 281-297. doi:10.1016/j.cose.2014.11.002

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Exploring behavioral information security networks in an organizational context: An empirical case study. *Journal of Information Security and Applications*, 34(1), 46-62. doi:10.1016/j.jisa.2016.06.002

Debele, F. G., Meo, M., Renga, D., Ricca, M., & Zhang, Y. (2015). Designing resource-on-demand strategies for dense WLANs. *IEEE Journal on Selected Areas in Communications*, *33*(12), 2494-2509. doi:10.1109/JSAC.2015.2482007

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, *19*(4), 9-30. doi:1080/07421222.2003.11045748

De Massis, A., & Kotlar, J. (2014). The case study method in family business research: Guidelines for qualitative scholarship. *Journal of Family Business Strategy*, *5*(1), 15-29. doi:10.1016/j.jfbs.2014.01.007

Dennen, V. P., & Hao, S. (2014). Intentionally mobile pedagogy: The M-COPE framework for mobile learning in higher education. *Technology, Pedagogy and Education, 23*(3), 397–419. doi.10.1080/1475939X.2014.943278

Diaz, A., Sherman, A. T., & Joshi, A. (2019). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, 1-15. doi:10.1080/01611194.2019.1623343

Downer, K., & Bhattacharya, M. (2015). BYOD security: A new business challenge. In *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)* (pp. 1128-1133). IEEE. doi:10.1109/SmartCity.2015.221

Doyle, G. J., Garrett, B., & Currie, L. M. (2014). Integrating mobile devices into nursing curricula: Opportunities for implementation using Rogers's diffusion of innovation model. *Nurse Education Today*, *34*(5), 775-782. doi:10.1016/j.nedt.2013.10.021

Dündar, H., & Akçayır, M. (2014).Implementing tablet PCs in schools: Students' attitudes and opinions. *Computers in Human Behaviour, 32*, 40-46. doi:10.1016/j.chb.2013.11.020

El Hussein, M., Jakubec, S. L., & Osuji, J. (2015). Assessing the FACTS: A mnemonic for teaching and learning the rapid assessment of rigor in qualitative research studies. *The Qualitative Report*, *20*(8), 1182-1184, Retrieved from http://nsuworks.nova. edu

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

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1-4. doi:10.11648/j.ajtas.20160501.11

Farley, H., Murphy, A., Johnson, C., Carter, B., Lane, M., Midgley, W., & ... Koronios, A. (2015). How do students use their mobile devices to support learning? A case study from an Australian regional university. *Journal of Interactive Media in Education*, *2015*(1), 1-13. doi:10.5334/jime.ar

Ferreira, K. D., & Lee, C. G. (2014). An integrated two-stage diffusion of innovation model with market segmented learning. *Technological Forecasting and Social Change*, *88*, 189-201. doi:10.1016/j.techfore.2014.06.007

Fettweis, G., & Alamouti, S. (2014). 5G: Personal mobile internet beyond what cellular did to telephony. *IEEE Communications Magazine*, *52*(2), 140-145. doi:10.1109/MCOM.2014.6736754

Fielding, H. (2016). Any Time, Any Place: The myth of universal access and the semiprivate space of online education. *Computers and Composition*, *40*, 103-114. doi:10.1016/j.compcom.2016.03.002

Flauzac, O., Gonzalez, C., & Nolot, F. (2016). Developing a distributed software defined networking testbed for IoT. *Procedia Computer Science*, *83*, 680-684. doi:10.1016/j.procs.2016.04.151

Fletcher, A. J., MacPhee, M., & Dickson, G. (2015). Doing participatory action research in a multicase mtudy: A methodological example. *International Journal of Qualitative Methods*, *14*(5), doi:10.1177/1609406915621405

Franceschinis, C., Thiene, M., Scarpa, R., Rose, J., Moretto, M., & Cavalli, R. (2017). Adoption of renewable heating systems: An empirical test of the diffusion of innovation theory. *Energy*, *125*, 313-326. doi: 10.1016/j.energy.2017.02.060

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*(9), 1408-1416. Retrieved from http://nsuworks.nova.edu

Gaikwad, P. (2017). Including Rigor and Artistry in Case Study as a Strategic Qualitative Methodology. *The Qualitative Report*, *22*(13), 3431-3446. Retrieved from http://nsuworks.nova.edu/tqr

Gan, C. L., & Balakrishnan, V. (2017). Mobile technology in the classroom: What drives student-lecturer interactions?. *International Journal of Human–Computer Interaction*, 1-14. doi:10.1080/10447318.2017.1380970

Garba, S., Abdulmalik, M., & Tekanyi, A. M. S. (2015). Efficient Bandwidth Management and Implementation of Cross-Layer Queuing Model in a Wireless Campus Area Network. *International Journal of Computer Applications*, *112*(2). doi:10.5120/19636-1210

Gartner. (2018). CIO (*Chief Information Officer).* Retrieved from https://www.gartner.com/en/information-technology/glossary/cio-chief-information-officer

Gartner. (2018). *CTO (Chief Technology Officer).* Retrieved from https://www.gartner.com/en/information-technology/glossary/cto-chief-technology-officer

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., … & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing*, *74*(10), 4986-5002.

Gkioulos, V., Wangen, G., Katsikas, S. K., Kavallieratos, G., & Kotzanikolaou, P. (2017). Security awareness of the digital natives. *Information*, *8*(2), 42. doi:10.3390/info8020042

Hallett, R. E., & Barber, K. (2014). Ethnographic research in a cyber era. *Journal of Contemporary Ethnography*, *43*(3), 306-330. doi:10.1177/0891241613497749

Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: when to use them and how to judge them. *Human Reproduction*, *31*(3), 498-501. doi.10.1093/humrep/dev334

Hannaford, L. (2017). Motivation in group assessment: a phenomenological approach to post-graduate group assessment. *Assessment & Evaluation in Higher Education*, *42*(5), 823-836. doi:10.1080/02602938.2016.1195787

Hao, S., Cui, M., Dennen, V. P., Türel, Y. K., & Mei, L. (2017). Analysis of mobile learning as an innovation in higher education: a comparative study of three countries. *International Journal of Mobile Learning and Organisation*, *11*(4), 314-339. doi:10.1504/IJMLO.2017.087080

Harland, T. (2014). Learning about case study methodology to research higher education. *Higher Education Research & Development, 33*(6), 1113-1122. doi:10.1080/07294360.2014.911253

Hennink, M. M., Kaiser, B. N., & Marconi, V. C. (2017). Code saturation versus meaning saturation: how many interviews are enough?. *Qualitative health research*, *27*(4), 591-608. doi:10.1177/1049732316665344

Herranz, J., & Nin, J. (2014). Secure and efficient anonymization of distributed confidential databases. *International Journal of Information Security, 13*, 497-512. doi:10.1007/s10207-014-0237-x

Hoehle, H., Zhang, X., & Venkatesh, V. (2015). An espoused cultural perspective to understand continued intention to use mobile applications: A four-country study of mobile social media application usability. *European Journal of Information Systems, suppl. Special Issue: Cross-Cultural IS Research: Perspectives, 24*(3), 337-359. doi:10.1057/ejis.2014.43

Hollinger, G. A., Yerramalli, S., Singh, S., Mitra, U., & Sukhatme, G. S. (2015). Distributed data fusion for multirobot search. *IEEE Transactions on Robotics*, *31*(1), 55-66. doi:10.1109/TRO.2014.2378411

Houghton, C., Murphy, K., Meehan, B., Thomas, J., Brooker, D., & Casey, D. (2017). From screening to synthesis: Using NVivo to enhance transparency in qualitative evidence synthesis. *Journal of Clinical Nursing*, *26*(5-6), 873-881. doi:10.1111/jocn.13443

Hsiao, K. L., & Chen, C. C. (2016). What drives in-app purchase intention for mobile games? An examination of perceived values and loyalty. *Electronic Commerce Research and Applications, 16*(C), 18-29. doi:10.1016/j.elerap.2016.01.001

Hsu, M. H., Chang, C. M., Chu, K. K., & Lee, Y. J. (2014). Determinants of repurchase intention in online group-buying: The perspectives of DeLone & McLean IS success model and trust. *Computers in Human Behavior*, *36*, 234-245. doi:10.1016/j.chb.2014.03.065

Hussein, A. (2015). The use of triangulation in social sciences research: Can qualitative and quantitative methods be combined?. *Journal of Comparative Social Work*, *4*(1). Retrieved from http://journal.uia.no

Hyysalo, S., Johnson, M., & Juntunen, J. K. (2017). The diffusion of consumer innovation in sustainable energy technologies. *Journal of Cleaner Production*, *162*, S70-S82. doi:10.1016/jclepro.2016.09.045

Ilic, P. (2015). The effects of mobile collaborative activities in a second language course. *International Journal of Mobile and Blended Learning, 7*(4), 16–37. doi:10.4018/IJMBL.2015100102

Innocenzi, R. L., Brown, K., Liggit, P., Tout, S., Tanner, A., Coutilish, T., & Jenkins, R. J. (2018). Think Before You Click. Post. Type. Lessons learned from our University Cyber Security Awareness Campaign," Journal of Cybersecurity Education, Research and Practice: Vol. 2018: No. 1, Article 3. Retrieved from https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/3

Jahanmir, S. F., & Lages, L. F. (2016). The late-adopter scale: A measure of late adopters of technological innovations. *Journal of Business Research*, *69*(5), 1701-1706. doi:10.1016/j.jbusres.2015.10.041

Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of basic and clinical pharmacy*, *5*(4), 87. doi:10.4103/0976-0105.141942

Jarrahi, M. H., Crowston, K., Bondar, K., & Katzy, B. (2017). A pragmatic approach to managing enterprise IT infrastructures in the era of consumerization and individualization of IT. *International Journal of Information Management*, *37*(6), 566-575. doi:10.1016/ijinfomgt.2017.05.016

Jones, B. H., & Chin, A. G. (2015). On the efficacy of smartphone security: A critical analysis of modifications in business students' practices over time. *International Journal of Information Management*, *35*(5), 561-571. doi:10.1016/j.ijinfomgt.2015.06.003

Joslin, R., & Müller, R. (2016). Identifying interesting project phenomena using philosophical and methodological triangulation. *International Journal of Project Management*, *34*(6), 1043-1056. doi:10.1016/j.ijproman.2016.05.005

Jothi, N., Rashid, N. A., & Husain, W. (2015). Data mining in healthcare–a review. Procedia Computer Science, 72, 306-313. doi:10.1016/j.procs.2015.12.145

Kachouie, R., & Sedighadeli, S. (2015). New product development success factors in prospector organisations: Mixed method approach. *International Journal of Innovation Management*, *19*(04). doi:10.1142/S1363919615500401

Kaczynski, D., Salmona, M., & Smith, T. (2014). Qualitative research in finance. *Australian Journal of Management*, *39*(1), 127-135. doi:10.1177/0312896212469611

Kahlke, R. M. (2014). Generic qualitative approaches: Pitfalls and benefits of methodological mixology. *International Journal of Qualitative Methods*, *13*(1), 37-52. doi:10.1177/160940691401300119

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of advanced nursing*, *72*(12), 2954-2965. doi:10.1111/jan.13031

Kao, Y. C., Chang, Y. C., & Chang, R. S. (2015). Managing bring your own device services in campus wireless networks. In *Computer Science and Engineering Conference (ICSEC), 2015 International.* Chiang Mai, Thailand. doi:10.1109/ICSEC.2015.7401456

Kearns, G. S. (2016). Countering mobile device threats: A mobile device security model. *Journal of Forensic & Investigative Accounting*, *8*(1), 36-48. Retrieved from https://www.nacva.com/jfia

Ketokivi, M., & Choi, T. (2014). Renaissance of case research as a scientific method. *Journal of Operations Management, 32*, 232-240. doi:10.1016/j.jom.2014.03.004

Khelf, R., & Ghoualmi-Zine, N. (2018, November). IPsec/Firewall Security Policy Analysis: A Survey. In *2018 International Conference on Signal, Image, Vision and their Applications (SIVA)* (pp. 1-7). IEEE. doi:10.1109/SIVA.2018.8660973

Kiernan, M. D. (2016). Legal ethics and concerns with security in a bring your own device program. *Issues in Information Systems*, *17*(4) 254-259. Retrieved from http://www.iacis.org/index.php

Kim, J., & Lee, I. (2015). 802.11 WLAN: History and new enabling MIMO techniques for next generation standards. *IEEE Communications Magazine*, *53*(3), 134-140. doi:10.1109/MCOM.2015.7060495

King, J., & Evans, D. (2016). Key criteria for selecting a secure cloud wireless network. *Network Security*, *2016*(1), 17-20. doi:10.1016/S1353-4858(16)30010-1

Kiwanuka, A. (2015). Acceptance Process: The missing link between UTAUT and diffusion of innovation theory. *American Journal of Information Systems*, *3*(2), 40-44. doi:10.12691/ajis-3-2-3

Kornbluh, M. (2015). Combatting challenges to establishing trustworthiness in qualitative research. *Qualitative Research in Psychology*, *12*(4), 397-414. doi:10.1080/14780887.2015.1021941

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of Medical Systems*. 41: 127. doi:10.1007/s10916-017-0778-4

Langergaard, L. L. (2017). Care work and diffusion of innovation in danish elder care. *Nordic Journal of Social Research*, *8*. doi:10.7577/njsr.2213

Lee, D. C., Lin, S. H., Ma, H. L., & Wu, D. B. (2017). Use of a Modified UTAUT Model to Investigate the Perspectives of Internet Access Device Users. *International Journal of Human–Computer Interaction*, *33*(7), 549-564. doi:10.1080/10447318.2016.1261249

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

Liao, Q., Luo, X. R., Gurung, A., & Shi, W. (2015). A holistic understanding of non-users' adoption of university campus wireless network: An empirical investigation. *Computers in Human Behavior*, *49*, 220-229. doi:10.1016/j.chb.2015.02.044

Lichterman, P. (2017). Interpretive reflexivity in ethnography. *Ethnography*, *18*(1), 35-45. doi:10.1177/1466138115592418

Lynch, M. J., Barrett, K. L., Stretesky, P. B., & Long, M. A. (2017). The neglect of quantitative research in green criminology and its consequences. *Critical Criminology*, *25*(2), 183-198. doi:10.1007/s10612-017-9359-6

Magsamen-Conrad, K., Upadhyaya, S., Joa, C. Y., & Dowd, J. (2015). Bridging the divide: Using UTAUT to predict multigenerational tablet adoption practices. *Computers in human behavior*, *50*, 186-196. doi:10.1016/j.chb.2015.03.032

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies: guided by information power. *Qualitative health research*, *26*(13), 1753-1760. doi:10.1177/1049732315617444

Mannan, S., Nordin, S. M., Rafik-Galea, S., & Rizal, A. R. A. (2017). The ironies of new innovation and the sunset industry: Diffusion and adoption. *Journal of Rural Studies*, *55*, 316-322. doi:10.1016/j.jrurstud.2017.07.015

Maree, J. G. (2015). Research on life design in (South) Africa: A qualitative analysis. *South African Journal of Psychology*, 45, 332-348. doi:10.1177/0081246314566785

Marion, T. J., Eddleston, K. A., Friar, J. H., & Deeds, D. (2015). The evolution of interorganizational relationships in emerging ventures: An ethnographic study within the new product development process. *Journal of Business Venturing*, *30*(1), 167-184. doi:10.1016/j.jbusvent.2014.07.003

Matthews, J. R. (2017). Understanding indigenous innovation in rural west africa: Challenges to diffusion of innovations theory and current social innovation practice. *Journal of Human Development and Capabilities*, *18*(2), 223-238. doi:10.1080/19452829.2016.1270917

Maxwell, J. A. (2016). Expanding the history and range of mixed methods research. *Journal of Mixed Methods Research, 10*, 12-27. doi:10.1177/1558689815571132

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion*, *30*(7), 537-542. doi:10.1177/0267659114559116

McIntosh, M. J., & Morse, J. M. (2015). Situating and constructing diversity in semistructured interviews. *Global Qualitative Nursing Research*, *2*, doi:10.1177/2333393615597674

Medhi, D., & Ramasamy, K. (2017). *Network routing: algorithms, protocols, and architectures*. USA: Morgan Kaufmann.

Mehmood, Y., Barbieri, N., & Bonchi, F. (2015). Modeling adoptions and the stages of the diffusion of innovations. *Knowledge and Information Systems, 48*(1), 1-27. doi:10.1007/s10115-015-0889-5

Moser, A., & Korstjens, I. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *European Journal of General Practice*, *24*(1), 9-18. doi:10.1080/13814788.2017.137509

Muhammad, M. A., Zadeh, P. B., & Ayesh, A. (2017, July). Improving Security in Bring Your Own Device (BYOD) Environment by Controlling Access. ACM. doi:10.1145/3102304.3105573

Nan, N., Zmud, R., & Yetgin, E. (2014). A complex adaptive systems perspective of innovation diffusion: An integrated theory and validated virtual laboratory. *Computational and Mathematical Organization Theory, 20*(1), 52-88. doi:10.1007/s10588-013-9159-9

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research. Retrieved from http://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/

National Institute of Standards and Technology (NIST), (2016). Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. *NIST Special Publication 800-46* (Rev-2). doi:10.6028/NIST.SP.800-46r2

NCCCS. (2018). *Statistical Reports.* Retrieved from http://www.nccommunitycolleges.edu/analytics/statistical-reports

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

Noughabi, E. A. Z., Far, B. H., & Raahemi, B. (2016, July). Predicting Students' Behavioral Patterns in University Networks for Efficient Bandwidth Allocation: A Hybrid Data Mining Method (Application Paper). In *2016 IEEE 17th International Conference on Information Reuse and Integration (IRI)* (pp. 102-109). IEEE. doi:10.1109/IRI.2016.21

Oye, N. D., Aiahad, N., & Abrahim, N. (2014). The history of UTAUT model and its impact on ICT acceptance and usage by academicians. *Education and Information Technologies, 19*(1), 251-270. doi:10.1007/s10639-012-9189-9

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health*, *42*(5), 533–544. doi:10.1007/s10488-013-0528-y

Paredes, R. K., & Hernandez, A. A. (2018). Designing an Adaptive Bandwidth Management for Higher Education Institutions. *International Journal of Computing Sciences Research*, *2*(1), 17-35. doi:10.25147/ijcsr.2017.001.1.22

Parker, L. (2014). Qualitative perspectives: Through a methodological lens. *Qualitative Research in Accounting and Management, 11*(1), 13-28. doi:10.1108/QRAM-02-2014-0013

Pashaeypoor, S., Ashktorab, T., Rassouli, M., & Alavi-Majd, H. (2016). Predicting the adoption of evidence-based practice using Rogers diffusion of innovation model. *Contemporary nurse*, *52*(1), 85-94. doi:10.1080/10376178.2016.1188019

Peine, A., van Cooten, V., & Neven, L. (2017). Rejuvenating design: Bikes, batteries, and older adopters in the diffusion of e-bikes. *Science, Technology, & Human Values*, *42*(3), 429-459. doi:10.1177/0162243916664589

Peker, Y. K., Ray, L., Da Silva, S., Gibson, N., & Lamberson, C. (2016). Raising Cybersecurity Awareness among College Students. In *Journal of The Colloquium for Information System Security Education* (Vol. 4, No. 1, pp. 17-17). Retrieved from https://cisse.info/journal/index.php/cisse/article/view/55

Perrotta, C. (2017). Beyond rational choice: How teacher engagement with technology is mediated by culture and emotions. *Education and Information Technologies*, *22*(3), 789-804. doi:10.1007/s10639-015-9457-6

Pinchot, J., & Paullet, K. (2015). Bring your own device to work: Benefits, security risks, and governance issues. *Issues in Information Systems*, *16*(3). 238-244. Retrieved from iacis.org

Poushter, J. (2016). Smartphone ownership and internet usage continues to climb in emerging economies. *Pew Research Center*, *22*, 1-45. Retrieved from www.perresearch.org

Pucher, K., Candel, M., Krumeich, A., Boot, N., & De Vries, N. (2015). Effectiveness of a systematic approach to promote intersectoral collaboration in comprehensive

school health promotion: A multiple-case study using quantitative and qualitative data. *BMC Public Health, 15*(1), 1-14. doi:10.1186/s12889-015-1911-2

Raj, U., & Catherine, M. S. (2015). Certificate based hybrid authentication for Bring Your Own Device (BYOD) in Wi-Fi enabled Environment. *International Journal of Computer Science and Information Security*, *13*(12), 41. Retrieved from https://sites.google.com/site/ijcsis

Redza, A., Nordin, S. M., & Saad, M. S. M. (2017). The innovative society: A comparison study of innovation diffusion among farmers in malaysia two major mranary area. *Global Business and Management Research*, *9*(1s), 703-713

Reich, J. A. (2015). Old methods and new technologies: Social media and shifts in power in qualitative research. *Ethnography*, *16*(4), 394-415. doi:10/1177/1466138114552949

Rimal, B. P., Van, D. P., & Maier, M. (2017). Mobile edge computing empowered fiber-wireless access networks in the 5G era. *IEEE Communications Magazine*, *55*(2), 192-200. doi**:**10.1109/MCOM.2017.1600156CM

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology*, *11*(1), 25-41. doi:10.1080/14780887.2013.801543

Rogers, E. M. (2003). *Diffusion of Innovations, Fifth Edition*. New York, NY: The Free Press

Rost, P., Banchs, A., Berberana, I., Breitbach, M., Doll, M., Droste, H., … & Sayadi, B. (2016). Mobile network architecture evolution toward 5G. *IEEE Communications Magazine*, *54*(5), 84-91. doi**:**10.1109/MCOM.2016.7470940

Rouibah, K., Lowry, P. B., & Almutairi, L. (2015). Dimensions of business-to-consumer (B2C) systems success in Kuwait: Testing a modified DeLone and McLean IS success model in an e-commerce context. *Journal of Global Information Management (JGIM)*, *23*(3), 41-71. doi:10.4018/JGIM.2015070103

Russell, C. (2016). Assessing the risk of transformative technologies. *Computer Fraud & Security*, *2016*(7), 15-19. doi.10.1016/S1361-3723(16)30054-9

Sama, M. R., Conteras, L. M., Kaippallimalil, J., Akiyoshi, I., Qian, H., & Ni, H. (2015) Software-defined control of the virtualized mobile packet core. *IEEE Communication Magazine 53*(2); 107-115. doi:10.1109/MCOM.2015.7045398

Sanjari, M., Bahramnezhad, F., Fomani, F. K., Shoghi, M., & Cheraghi, M. A. (2014). Ethical challenges of researchers in qualitative studies: The necessity to develop a specific guideline. *Journal of medical ethics and history of medicine*, *7*, 14. Retrieved from www.ncbi.nlm.nih.gov

Schindler, L., Burkholder, G., Morad, O., & Marsh, C. (2017). Computer-based technology and student engagement: A critical review of the literature. *International Journal Of Educational Technology In Higher Education*, *14*(1), 1-28. doi:10.1186/s41239-017-0063-0

Scott, S., & McGuire, J. (2017). Using diffusion of innovation theory to promote universally designed college instruction. *International Journal of Teaching &*

Learning in Higher Education, *29*(1). 119-128. ISSN 1812-9129. Retrieved from https://files.eric.ed.gov/fulltext/EJ1135837.pdf

Shi, J., Liu, Y., Liu, W., & Zhang, X. (2015). High-resolution synthetic aperture radar based on the IEEE 802.11 protocol. *Electronics Letters, 51*(22), *1815-1817*. doi:10.1049/el.2015.1136

Shraim, K., & Crompton, H. (2015). Perceptions of using smart mobile devices in higher education teaching: A case study from Palestine. *Contemporary Educational Technology*, *6*(4), 301-318. Retrieved from www.cedtech.net

Shumate, T., & Ketel, M. (2014, March). Bring your own device: Benefits, risks and control techniques. IEEE *SOUTHEASTCON 2014,* Lexington, KY*,* 2014. 1-6. doi:10.1109/SECON.2014.6950718

Siddiqui, F., Zeadally, S., & Salah, K. (2015). Gigabit Wireless Networking with IEEE 802.11 ac: Technical Overview and Challenges. *Journal of Networks*, *10*(3), 164-171. doi:10.4304/jnw.10.3.164-171

Singh, M. M., Chan, C. W., & Zulkefli, Z. (2017). Security and privacy risks awareness for bring your own device (BYOD) paradigm. *International Journal of Advanced Computer Science and Applications*, *8*(2), 53-62. Retrieved from http://thesai.org/Publications/Archives?code=IJACSA

Skovoroda, A., & Gamayunov, D. (2015). Securing mobile devices: malware mitigation methods. *JoWUA*, *6*(2), 78-97. doi:10.22667/JOWUA.2015.06.31.078

Smith, R. A., Kim, Y., Zhu, X., Doudou, D. T., Sternberg, E. D., & Thomas, M. B. (2018). Integrating Models of Diffusion and Behavior to Predict Innovation

Adoption, Maintenance, and Social Diffusion. *Journal of health communication*, *23*(3), 264-271. doi:10.1080/10810730.2018.1434259

Smith-Rose, R. L. (1967), Early days in radio research. *Electronics and Power*, (13)7, 253-258, doi:10.1049/ep.1967.0172

Song, Y. (2016). We found the 'black spots' on campus on our own: Development of inquiry skills in primary science learning with BYOD (Bring Your Own Device). *Interactive Learning Environments, (24)*2, 291-305, doi:10.1080/10494820.2015.111370

Song, Y., & Kong, S. C. (2017). Affordances and constraints of BYOD (Bring Your Own Device) for learning and teaching in higher education: Teachers' perspectives. *The Internet and Higher Education*, *32*, 39-46. doi:10.1016/j.iheduc.2016.08.004

Spangler, S. C., Rodi, A., & Kiernan, M. (2016). Case study: BYOD in the higher education classroom: Distraction or disruption? The adoption of Spangler's 2016 digital human IT integration charting system. *Issues In Information Systems*, *17*(3), 100-108. Retrieved from www.iacis.org

Sparkes, A. C. (2014). Developing mixed methods research in sport and exercise psychology: Critical reflections on five points of controversy. *Psychology of Sport and Exercise. 16*. doi:10.1016/j.psychsport.2014.08.014

Sundgren, M. (2017). Blurring time and place in higher education with bring your own device applications: A literature review. *Education and Information Technologies*, *22*(6), 3081-3119. doi:10.1007/s10639-017-9576-3

Sung, Y. T., Chang, K. E., & Liu, T. C. (2016). The effects of integrating mobile devices with teaching and learning on students' learning performance: A meta-analysis and research synthesis. *Computers & Education*, *94*, 252-275. doi:10.1016/j.compedu.2015.11.008

Tarhini, A., El-Masri, M., Ali, M., & Serrano, A. (2016). Extending the UTAUT model to understand the customers' acceptance and use of internet banking in Lebanon: A structural equation modeling approach. *Information Technology & People*, *29*(4), 830-849. doi:10.1108/ITP-02-2014-0034

Thomas, D. R. (2017). Feedback from research participants: Are member checks useful in qualitative research?. *Qualitative Research in Psychology*, *14*(1), 23-41. doi:10.1080/14780887.2016.1219435

Tossell, C. C., Kortum, P., Shepard, C., Rahmati, A., & Zhong, L. (2015). You can lead a horse to water but you cannot make him learn: Smartphone use in higher education. *British Journal of Educational Technology*, *46*(4), 713-724. doi:10.1111/bjet.12176

Traxler, J. (2016). Inclusion in an age of mobility. *Research In Learning Technology, 24*. doi:10.3402/rlt.v24.31372

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, *52*(4), 506-517. doi:10.1016/j.im.2015.03.002

Uchida, Y. (2015). The relationship between technology and diffusion process. *Journal of International Business and Economics, 15*(2), 87-94. doi:10.18374/jibe-15-2.7

Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. *Journal of Nursing Education and Practice*, *6*(5), 100-110. doi:10.5430/jnep.v6n5p100

Varpio, L., Ajjawi, R., Monrouxe, L. V., O'Brien, B. C., & Rees, C. E. (2017). Shedding the cobra effect: Problematising thematic emergence, triangulation, saturation and member checking. *Medical Education*, *51*(1), 40-50. doi:10.1111/medu.13124

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, *27*(3).425-478. Retreived from www.misq.org

Vicary, S., Young, A., & Hicks, S. (2017). A reflective journal as learning process and contribution to quality and validity in interpretative phenomenological analysis. *Qualitative Social Work*, *16*(4), 550-565. Retrieved from http://journals.sagepub.com

Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD. *Procedia Computer Science*, 50, pp. 511-516. doi:10.1016/j.procs.2015.04.023

Vorderer, P., Krömer, N., & Schneider, F. M. (2016). Permanently online–Permanently connected: Explorations into university students' use of social media and mobile smart devices. *Computers in Human Behavior*, *63*, 694-703. doi:10.1016/j.chb.2016.05.085

Wang, Y. S., Li, H. T., Li, C. R., & Zhang, D. Z. (2016). Factors affecting hotels' adoption of mobile reservation systems: A technology-organization-environment

framework. *Tourism Management*, *53*, 163-172. Retrieved from https://www.journals.elsevier.com/tourism-management

Watkins, D. C. (2017). Rapid and rigorous qualitative data analysis: The "RADaR" technique for applied research. *International Journal of Qualitative Methods*, *16*(1), 1-9. doi:10.1177/1609406917712131

Willis, D. G., Sullivan-Bolyai, S., Knafl, K., & Cohen, M. Z. (2016). Distinguishing features and similarities between descriptive phenomenological and qualitative description research. *Western Journal of Nursing Research*, *38*(9), 1185-1204. doi:10.1177/0193945916645499

Wilson, V. (2014). Research methods: triangulation. *Evidence Based Library and Information Practice*, *9*(1), 74-75. doi:10.18438/B8WW3X

Wolgemuth, J. R., Erdil-Moody, Z., Opsal, T., Cross, J. E., Kaanta, T., Dickmann, E. M., & Colomer, S. (2015). Participants' experiences of the qualitative interview: Considering the importance of research paradigms. *Qualitative Research*, *15*(3), 351-372. doi:10.1177/1468794114524222

Woods, M., Paulus, T., Atkins, D. P., & Macklin, R. (2016). Advancing qualitative research using qualitative data analysis software (QDAS)? Reviewing potential versus practice in published studies using ATLAS. ti and NVivo, 1994–2013. *Social Science Computer Review*, *34*(5), 597-617. doi:10.1177/0894439315596311

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. doi:10.1016/j.socec.2016.04.017

Yang, S. C., & Winter, P. (2015). LTE-Advanced and IEEE 802.11 ac: A new network architecture and opportunity for higher-education institutions. *The International Journal of Information and Learning Technology*, *32*(4), 221-234. doi:10.1108/IJILT-04-2013-0016

Yin, R. K. (2009). *Case study research: Design and methods.* (4th ed.). Thousand Oaks, CA: Sage

Yin, R. K. (2014). *Case Study Research: Design and Methods,* (5th ed.). Thousand Oaks, CA: Sage

Yüksel, P., & Yıldırım, S. (2015). Theoretical frameworks, methods, and procedures for conducting phenomenological studies in educational settings. *Turkish Online Journal of Qualitative Inquiry, 6*(1), 1-20. Retrieved from http://dergipark.ulakbim.gov.tr/tojqi/index

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security*, *55*, 81-99. doi:10.1016/j.cose.2015.06.011

Zamawe, F. C. (2015). The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal*, *27*(1), 13-15. doi:10.4314/mmj.v27i1.4

Zhang, X., Yu, P., Yan, J., & Spil, I. T. A. (2015). Using diffusion of innovation theory to understand the factors impacting patient acceptance and use of consumer e-health innovations: A case study in a primary care clinic. *BMC Health Services Research, 15*, 71. doi:10.1186/s12913-015-0726-2

Appendix A: Consent Form

CONSENT FORM

You are invited to take part in a research study about bring your own device (BYOD) and the challenges it brings to community college campuses regarding security, support and IT infrastructure. The researcher is inviting Chief Information Officers and/or Chief Technical Officers of selected North Carolina Community Colleges with at least one year in the position to be in the study. I obtained your name/contact info via your campus directory. This form is part of a process called "informed consent" to allow you to understand this study before deciding whether to take part.

This study is being conducted by a researcher who is a doctoral student at Walden University. You might already know the researcher as the individual does hold a full time staff position at a community college, but this study is separate from that role.

Background Information:

The purpose of this study is to identify and explore strategies that have been put into play on North Carolina Community Colleges to strategically address the challenges of increasing mobile usage demands associated with bring your own device (BYOD).

Procedures:

If you agree to be in this study, you will be asked to:

- Participate in a face-to-face interview during which data is collected.
- Review data collected in original interview for any omissions or to clarify information.
- Participate in a follow up interview if necessary. This will include reviewing data previously collected and any additional follow up questions.

Here are some sample questions:

- What are the challenges that emerge with the increasing mobile usage demand?
- What are the strategies employed to address those increasing mobile usage demands?
- How do you plan to address these increasing demands in the future?

Voluntary Nature of the Study:

This study is voluntary. You are free to accept or turn down the invitation. No one at Walden University or your own institution will treat you differently if you decide not to be in the study. If you decide to be in the study now, you can still change your mind later. You may stop at any time.

Risks and Benefits of Being in the Study:

Being in this type of study involves some risk of the minor discomforts that can be encountered in daily life, such as fatigue or stress. Being in this study would not pose risk to your safety or wellbeing.

Today's educational institutions exist in a world that is very different from the more traditional one in which they were designed. Both students and colleges are undergoing an identity transformation in that the norms are being challenged by an increasingly mobile and connected society. This research may benefit colleges as they strive to identify what devices are connecting to their networks and for what purpose. It may also assist in identifying which devices and operating systems could be supported on campus. This research may also be beneficial to students in that the successful strategies put into play by CIOs may lead to increased personalized student-centered learning,

which could lead to increased motivation by students to succeed at their coursework which, in turn, could improve the student's economic future.

Payment:

No payment or gift is tied to participation in the study.

Privacy:

Reports coming out of this study will not share the identities of individual participants. Details that might identify participants, such as the location of the study, also will not be shared. The researcher will not use your personal information for any purpose outside of this research project. Data will be kept secure by password protection of files associated with the research study. Data encryption was used on the flash drive, itself. The flash drive will be securely kept for a period of at least 5 years, as required by the university.

Contacts and Questions:

You may ask any questions you have now. Or if you have questions later, you may contact the researcher. Walden University's approval number for this study is 04-05-19-0530198 and it expires on April 4th, 2020. The researcher will give you a copy of this form to keep.

Obtaining Your Consent:

If you feel you understand the study well enough to make a decision about it, please indicate your consent by signing below.

Printed Name of Participant _____

Date of consent _____

Participant's Signature _____

Researcher's Signature _____

Appendix B: Interview Questions

Interview Questions

1. Overall, what do you see as challenges resulting from individuals bringing multiple digital devices with them, to campus?
2. Which of these challenges are affecting your campus network? What steps have been taken to mitigate the challenges?
3. What successful strategies are you using to reduce the effects of mobile usage demands on campus?
4. How did you identify and select the successful strategies for reducing the effects of mobile usage demands on campus?
5. How did you implement the successful strategies for minimizing the effects of mobile usage demands within your campus network?
6. What challenges did you encounter in implementing the strategies to reduce the consequences of mobile usage demands?
7. How did you manage the challenges faced in implementing the strategies to minimize the effects of mobile usage demands?
8. What strategies are most effective in reducing the effects of mobile usage demands on campus?
9. What factors influence the implementation of strategies to minimize the effects of mobile usage demands on campus?
10. What additional information, documentation, or processes would you like to share that may help in this research study?

Appendix C: Interview Protocol Form

INTERVIEW PROTOCOL FORM

Institution: _____
Interviewee: (Title and Name): _____
Interviewer: _____

Introductory Protocol

To facilitate our note-taking, we would like to record our conversations today. Please sign the release form. For your information, only researchers on the project will be privy to the digital recording which will be eventually destroyed after a five-year period. Prior to continuing I'd like to retrieve the consent form that was sent to you. This document stated that: (1) all information will be held confidential, (2) your participation is voluntary and you may stop at any time if you feel uncomfortable, and (3) we do not intend to inflict any harm. Thank you for your agreeing to participate.

This interview should last no longer than one hour. During this time, there are several questions that I would like to put to you. If time begins to run short, it may be necessary to interrupt you in order to push ahead and complete this line of questioning.

Introduction

You have been selected to participate in this study because you have been identified as someone who has a great deal to share on strategies for managing the number of mobile devices being brought to campus and students expecting to access campus apps as though they were using a desktop computer. This research project as a whole focuses on the strategies currently in use and any proposed strategies that would assist in managing bring your own device (BYOD) on campus. To this end we are talking about the impact of the number of digital devices that students bring to campus. This study does not aim to evaluate your techniques or experiences. Rather, I am trying to learn more about the strategies you are using and how they are helping you balance between accessibility for students and security for your institution.

Let's begin with question

1. Overall, what do you see as challenges resulting from individuals bringing multiple digital devices with them, to campus?
2. Which of these challenges are affecting your campus network? What steps have been taken to mitigate the challenges?

3. What successful strategies are you using to reduce the effects of mobile usage demands on campus?
4. How did you identify and select the successful strategies for reducing the effects of mobile usage demands on campus?
5. How did you implement the successful strategies for minimizing the effects of mobile usage demands within your campus network?
6. What challenges did you encounter in implementing the strategies to reduce the consequences of mobile usage demands?
7. How did you manage the challenges faced in implementing the strategies to minimize the effects of mobile usage demands?
8. What strategies are most effective in reducing the effects of mobile usage demands on campus?
9. What factors influence the implementation of strategies to minimize the effects of mobile usage demands on campus?
10. What additional information, documentation, or processes would you like to share that may help in this research study?