SHARED WIRELESS INFRASTRUCTURES IN LARGE PUBLIC VENUES: CASE STUDIES ON PREVENTING DATA BREACHES

by

George G. Aguilera

ALEX LAZO, PhD, Faculty Mentor and Chair

NESTOR COLLS, PhD, Committee Member

PAMELYN WITTEMAN, PhD, Committee Member

Todd C. Wilson, PhD, Dean

School of Business, Technology, and Health Care Administration

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Information Technology

Capella University

June 2021

Abstract

The purpose of this qualitative multiple case study was to uncover effective strategies to reduce the risk of cybersecurity data breaches of wireless IT network infrastructures at large public-event venues. The case study research design addressed the nature of the solution needed in a contemporary context and allowed thematic development from lived experiences. The research question was what are effective strategies large public venue operators use to reduce the risk of data breaches in their wireless networks during and between venue events? Factors investigated include large public venue (a) wireless infrastructure, (b) vendor and tenant relationships, (c) events and impact, and (d) cybersecurity strategies and development. A sample of seven IT managers and persons responsible for cybersecurity in different large public venues in the United States were interviewed. Characteristics of large public venues investigated include having (a) a high-density wireless network, (b) a large attack surface, (c) multiple tenants and multiple purpose-use, (d) complexity, and (e) undersized IT staff. Cross-synthesis of themes from multiple cases yielded consensus and increased external validity. The literature review was conducted for technical, regulatory, and business topics using conference proceedings, government and consulting company reports, as well as peer-reviewed and scholarly journals. Findings revealed that using segmentation techniques, compliance and policies, continuous improvement, and a support system helped to prevent and protect against data breaches. A framework emerged to help large public venues develop cybersecurity strategies. Three trends emerged: (a) using multi-factor authentication with all venue operations except for guests, (b) enabling controls to lock down device security, and (c) having executive buy-in to fund improvements. A recommended future research is to conduct a quantitative study of CIOs, CTOs, CISOs, league, and large public venue owners and cybersecurity decision-makers, to

understand the relationship between reported and unreported data breaches. IT managers and practitioners in this study did not address vulnerabilities common to wireless networks, which raised whether IT managers can address the problem of preventing data breaches effectively without the assistance of a combination of wireless engineers and cybersecurity IT practitioners.

Dedication

I dedicate this work to my loving wife, Noemi, for her enduring support and consult while I was a working student. You sacrificed your time with me so we can move ahead as a family. I dedicate this work to my mother, Judy, who always encouraged me to learn more to become a greater person. To my dear sister, Susana, you made learning a joy from the time I was eight years old. I dedicate this loving memory to my brother, Henry, who was always so proud and taught me many practical skills and valuable life lessons. I started my doctoral journey shortly after your unexpected passing. I dedicate this work to my dear father, Jorge, who passed away while developing my proposal for this research study. You taught me honesty and integrity, care for others, and joy of the arts. May you both rest in peace.

Acknowledgments

First, I give thanks to God Almighty for having bestowed upon me so many gifts and blessings. I am grateful to my mentor, Dr. Alex Lazo, for always being responsive and providing me with much-needed guidance to get me through my academic journey. I thank my committee members, Dr. Pamelyn Witteman and Dr. Nestor Colls, for making my dissertation stronger. Thanks to my former committee members, Dr. Vanessa Wood and Dr. Randall Valentine, for their insight and support. I thank Dr. Dani Babb for being accessible and an example of a prolific IT consultant early in my doctoral journey. I also thank Dr. Kimberly Lowrey for making the residency a joy and introducing me to systems thinking theory. Many thanks to the Capella faculty and staff, fellow students, and colleagues, who sometimes unknowingly inspired and supported me. Finally, I want to thank the participants for their insightful and valuable contribution to this study and the field of IT. Thank you all.

Table of Contents

List of Tables

List of Figures

CHAPTER 1. INTRODUCTION

Large public venues in the United States host close to 250 million visitors annually (Fulks, 2016; Oxford Economics, 2018). The annual contribution to the economy from professional sports venues' is greater than $45 billion (Amadeo, 2018; Trading Economics, n.d.). The yearly contribution from convention centers is approximately $38 billion, with amusement parks and outdoor events contributing roughly $12 billion (Oxford Economics, 2018; U.S. Department of Homeland Security, 2015). Every year, event attendees make purchases, scan credit cards at point-of-sale terminals, and sign up for mobile apps requiring the input of personal information on personal mobile wireless and Wi-Fi devices (McGuire, 2015). The transactions occur mostly within reach of the venue's wireless network infrastructure during an event, where a customer's mobile wireless or Wi-Fi device accesses Internet-based social media and streaming applications.

The large public venue may also offer services using locally generated content such as video instant replay for sports (Mickulicz, Drolia, Narasimhan, & Gandhi, 2016), wayfinding (Intel IoT, 2016), and ordering merchandise and concessions. The situation provides opportunities for attackers to analyze the mobile wireless or Wi-Fi network and find vulnerabilities to break into the information technology (IT) venue network during and after events (Bartoli, Medvet, & Onesti, 2018; Wang, Miao, & Jiao, 2016). Attackers can broaden the target beyond individual credit card data, including identity theft and the venue's intellectual property and other sensitive data (McGuire, 2015).

Background of the Study

Breaking into a network and gaining unauthorized access to sensitive or private individual or organizational data is a data breach (Ullah et al., 2018). Data breaches often result from viruses, malware, distributed denial of service attacks, and others. Data breaches are widely known but often poorly understood (Borum, Felker, Kern, Dennesen, & Feyes, 2015). According to the Federal Bureau of Investigation Internet Crime Complaint Center (2017), reported losses in the United States because of data breaches among individuals and corporations exceeded $138 million. Also, the frequency and size of data breaches have been increasing since 2009 (Edwards, Hofmeyr, & Forrest, 2016). Data breaches can have high associated costs because of the compounding effects of long detection times, averaging 30 days, and often recurring attacks within two years of the first event (Schatz & Bashroush, 2016). Data breaches are also complicated by going mostly unreported, amounting to approximately 66% of the attacks (LiCalzi, 2017). The impact compounds when cybercriminals use breach-related data for other cybercrimes, such as individual identity theft, often occurring within a short time of the initial data breach (Hughes, Bohl, Irfan, Margolese-Malin, & Solórzano, 2017).

Reputation and non-monetary losses of individuals and corporations because of data breaches are difficult to ascertain (Urrico, 2017). According to a report by Price Waterhouse Cooper, approximately 38% of businesses that experienced financial losses also suffered intellectual property theft and brand reputation damage due to the consequences of the attack (Gerard, 2016). Also, when a data breach occurs in one venue, others in the same market or industry are likely to suffer stock devaluation (Kashmiri, Nicol, & Hsu, 2017). Despite ongoing investments in information security, the risk of a data breach continues to climb as demand for applications and capacity increases (Brillat, 2018; Gordon, Loeb, Lucyshyn, & Zhou, 2015; Jenkins & Evans, 2018).

The wireless infrastructure at large public venues provides access to services for attendees, event staff, the sports league of a sports venue, and the venue. Attendees make purchases on personal mobile devices as e-commerce transactions or through merchandisers carrying mobile point of sale devices (Jenkins & Evans, 2018). Attendees also connect with personal devices to view the event, watch the instant replay, look up statistics, and use geo-location services to guide them to their destination (Bovee & Read, 2018; Melander, 2016; Sritapan & Eldefrawy, 2018). Event staff uses the wireless network to scan event tickets, provide point-of-sale services for concessions and merchandise, and surveillance. Venue personnel connects information displays, control systems (Wang, 2016), and support sensors such as IoT and team wearable technology. During events, the wireless infrastructure services thousands of users and devices (Melander, 2016).

The large public venue wireless infrastructure is typically a Wi-Fi network purposely built to accommodate high-density traffic, interactive services such as voice and video, and connection points for third-party applications and services as a shared infrastructure (Cisco Systems, 2015). Wi-Fi access points and antennas are mounted throughout the venue to meet the coverage and bandwidth requirements necessary to provide reliable services. Equipment in an on-premise datacenter delivers core network and application services to support back-office and attendee access applications. Clubs and leagues install additional equipment in exclusive areas to deliver in-venue luxury services (Sunnucks, 2019). The venue may own and operate the wireless infrastructure as part of the enterprise network or have a managed service provider to operate the non-enterprise wireless network (Kubler et al., 2017).

As network architectures evolve, wireless network vendors may offer venues revenue sharing to operate cellular-like networks. For example, the MulteFire standard network enables an enterprise to operate a carrier-like long-term evolution (LTE) network in a portion of the same unlicensed frequencies as Wi-Fi (Nicholls, 2016). The United States Navy and federal government share the Citizens Broadband Radio Service (CBRS) spectrum with private commercial businesses. One use case for CBRS is to offer shared cellular-like LTE network services to enterprises (Matinmikko, Latva-aho, Ahokangas, & Seppänen, 2018). This research study targeted enterprise and shared mobile wireless networks. The focus of this study was on large public venues, which outsource wireless networks and would suffer monetary and reputation losses in the event of a data breach.

IT wireless network infrastructures in large public venues have unique characteristics that may result in increased risk for data breach events. One set of related characteristics includes operating a highly dense, high capacity, and large footprint shared wireless network, providing services to thousands of attendees and vendors during events (Butler, 2018). Wireless networks are vulnerable to eavesdropping and impersonation attacks (Shivaramu, Prasobh, & Poti, 2016). The risk increases with many nodes over a large area. In some instances, an environment with high node density resembles signal jamming, which an attacker can exploit to reset and hijack user sessions (Bottarelli, Epiphaniou, Ismail, Karadimas, & Al-Khateeb, 2018). Large public venues may be located near dining facilities, entertainment venues, and shopping areas (Jenkins & Evans, 2018). Signals propagating from a large public venue into nearby facilities can increase the risk. With a large footprint, an attacker can hide in the environment, perform network data captures, and launch attacks during and after the event (Braun, Fung, Iqbal, & Shah, 2018).

Other characteristics that can result in increased risk are multiple-tenancy and multiple-purpose use of large public venues. Providers of different types of services use a shared physical infrastructure. Among the services are merchant and concession transactions, convenience services such as online ordering, displaying queue line wait times, location-based map directions, and video and secure communications for public safety and venue environmental controls and signage (Arfaoui et al., 2018; Butler, 2018). Each of the different types of services may require different cybersecurity mechanisms. During the 2018 Pyeongchang Winter Olympics, the Wi-Fi network was breached in the Olympic press center, resulting in a large malware attack in other functional areas (Jenkins & Evans, 2018).

Multiple-purpose venues can host different types of events, sometimes within a short time. For example, a venue can host a professional basketball game one day, a music concert the following day, and a multiple-day trade show or a convention later in the week (DHS, 2015). The venue, event, and sports league staff may need to connect and disconnect equipment, possibly reconfiguring the wireless network to cater to the different events (DHS, 2015). Changes in system configuration and the introduction of new applications may reduce protection or create new vulnerabilities (National Science and Technology Council Office of the President, 2016).

Characteristics related to increasing complexity may also increase risk in large public venues (DHS, 2018). With the ongoing adoption of new customer applications, the Internet of Things (IoT), venue environmental controls and event signage, venue public safety, government partner communications, and integration of other technologies such as cellular-like services, the large public venue can be dynamic and complex. In sports venues, players and coaches capture and save player performance analytics to the Cloud for analysis (Jenkins & Evans, 2018).

Among customer applications frequented by venue attendees are Facebook, Ticketfly, and Ticketmaster, all of whom experienced a data breach in 2018 (McCandless, n.d.). Wi-Fi calling, which provides cellular-like voice calling over a Wi-Fi network, is vulnerable to man-in-the-middle (MITM) attacks (Xie et al., 2018). According to The Cybersecurity Insight Report, respondents identified the complexity of the organization to be a problem 16% of the time (CDW, 2018). Network and equipment monitoring and management of a complex network may be difficult without direct or common control and visibility of all infrastructure devices, leading to increased risk.

Another characteristic of large public venues that may result in an increased risk of data breaches is the often-reported small staff assigned to IT enterprises. According to The Cybersecurity Insight Report, respondents identified a shortage of knowledgeable security staffing as a problem 9% of the time and request budget increases for security staff and managed security services 18% of the time (CDW, 2018). Approximately 46% of 133 digital preservation respondents from several industries reported being understaffed and would ideally double the number of employees dedicated to digital preservation (Atkins et al., 2020). If staff is undersized, employees may become overwhelmed and will not perform the necessary functions required of the role (Carmichael, 2015). Moreover, an undersized IT staff may miss essential functions for network resiliency, such as applying patches and infrastructure vulnerability testing.

Large public venues may have variable IT staffing needs to manage different events and during different times of the year, such as during a sports season (Mason, Sant, & Misener, 2018). Unlike most business environments, where the IT staff has complete control of network devices with slight traffic variation, stadiums support the logistics and internal equipment that services thousands of concurrent network connections for tens of thousands of untrusted wireless devices (Hennick, 2016). A series of sporting events in 2020 in Japan was to generate large amounts of data from IoT and other advanced technologies; however, the computer security emergency response teams continue to suffer from staffing shortages and task overload (Ohta et al., 2018). Staff limitations can lead to increased risk.

Large public venue operators, such as sports events, often focus on security for crowd control and the prevention of violent crimes and terrorism, such as surveillance and monitoring (Hassan, 2016). The Department of Homeland Security has designated commercial sector public venues as critical infrastructures (DHS, 2015). Although the Department of Homeland Security specifically addresses cyber-terrorism, cybersecurity strategies encompass data breach protection. Several of the operating conditions of venues in the commercial facilities sector can lead to an elevated risk of a data breach (U.S. Department of Homeland Security Commercial Facilities Sector, 2020). Some of the increased risks to large public venues are facilities and events operating with open public access, including high profile tenants, neighbors, and special events; facilities considered soft targets to terrorist attacks; and stadiums and other facilities recognized internationally to be iconic (DHS, 2015). With a critical infrastructure designation, large public venue network infrastructures can also be critically important.

Chief information officers (CIOs) and cybersecurity managers in large public venues with limited budgets face increasing cybersecurity risks (CDW, 2018). Among these are technical challenges of large and growing attack surfaces, a growing number of users, a growing number and diversity of applications, IoT, and systems' integration such as venue controls (CDW, 2018). While cyber-criminal attacks increase in number and frequency, large public venue wireless network infrastructures also face challenges related to high-density wireless, large attack surface, multiple-tenancy and multiple-purpose, complexity, and undersized staff (Booz Allen, 2019; CDW, 2018; DHS, 2018; Mason et al., 2018).

Cybersecurity approaches and data breach prevention strategies apply to businesses of different sizes and across markets and industries. Saber (2016) focused on small businesses when much of the research focused on large companies. Business leaders should have a cybersecurity policy, provide cybersecurity training for the leadership and employees, comply with industry standards, and offload security services to the Cloud (Saber, 2016). Organizations with available resources could mitigate data breaches by focusing on cybercriminals, cybercriminal identification, understanding cybercriminal motivations, and intentions with the stolen data to anticipate attacks (Décary-hétu & Leppänen, 2016; Leslie, Harang, Knachel, & Kott, 2018). Organizations of any size and industry that contain publicly accessible networks should apply technical measures such as routine security audits, taking data offline whenever possible, using appropriate software tools, traffic monitoring, intrusion prevention, and detection systems, and encryption help to prevent data breaches (Alneyadi, Sithirasenan, & Muthukkumarasamy, 2016; Botha, Eloff, & Swart, 2016; Ullah et al., 2018). No studies on data breach prevention strategies specific to large public venues were found.

This study focuses on wireless networks such as Wi-Fi and IoT and control devices owned, operated, or managed by large public venues. Though property lines can be a practical delineation for the span of control, participants in the study identified the boundaries for organizational responsibility. Typical users, or customers, included employees, attendees, and vendors who either used the host wireless network or installed a temporary network to offer services during events. In this study, the researcher addressed the impact personal devices have on a stadium’s IT infrastructure. Excluded from this study were mobile wireless cellular operators, or similar, who traditionally do not permit the host organization control of cellular operator assets.

The IT field is dynamic, and attackers adopt new tactics and circumvent preventative measures (Edwards et al., 2016). Data breaches continue to occur at a growing rate (Dhameja, 2015; Giorgio, 2018; Ullah et al., 2018). There are no signs of stopping the more frequent and destructive data breaches (Gunzel, 2017). Enterprise and shared wireless networks operating in large public venues have unique qualities that may make them vulnerable to data breach cyber-attacks (Bartoli et al., 2018; Jenkins & Evans, 2018; Kraemer-Mbula, Tang, & Rush, 2013; National Science and Technology Council Office of the President, 2016; Saeed Ahmadinia, Javed, & Larijani, 2016; Shivaramu, Prasobh, & Poti, 2016; Wang et al., 2016; Xie et al., 2018). The increasing trend of data breach events and their increasing frequency in the context of large public venues can lead to increased risk and susceptibility to data breach cyber-attacks (Edwards et al., 2016). Therefore, CIOs and cybersecurity managers who operate wireless networks at large public venues should be concerned about being targeted for data breach attacks.

Researchers have applied systems and systems thinking theories to understand cyber risk and phenomena like data breaches in complex environments. Ceric (2015) applied systems theory to evaluate the influence of cybersecurity risk resiliency to information communication technology business value creation. Yan (2020) argued that applying systems thinking treats cybersecurity as a whole entity, identifying and understanding the cybersecurity system, describing the interaction among the various components, and thus helps to address cybersecurity problems effectively. Armenia, Ferreira Franco, Nonino, Spagnoli, and Medaglia (2019) used systems thinking causal loop diagrams in a case study design on data breaches and other cyberattacks to evaluate related functional areas and the entire organization. Maahs (2018) and Saber (2016) applied systems thinking in multiple case study designs to small businesses to determine strategies for preventing data breaches. Systems thinking theory was used in this study primarily to understand the phenomenon of a data breach and preventive strategies.

This study has two theoretical implications for understanding the phenomenon of data breaches. One implication was to develop a deeper understanding of how operators of wireless networks in complex large public venues prevent and mitigate data breaches using a systems approach. Saber (2016) used systems thinking in a similar study and recommended expanding the research beyond small businesses. The other implication was to either develop or apply a testable framework specific to large public venues, which could be used by CIOs, IT managers, and non-IT staff to simplify and focus on strategies that prevent and mitigate data breaches and other forms of attacks. A framework such as the prioritize-resource-implement-standardize-monitor (PRISM) helps organizations, at a strategic level, to operationalize a tailored approach to address cybersecurity risks and problems (Goel, Kumar, & Haddow, 2020). The NIST Cybersecurity Framework helps organizations establish or improve cybersecurity risk management related to critical infrastructure (Barrett, 2018). Both PRISM and NIST frameworks have broad applications. By developing a framework specific to large public venues, decision-makers may more readily adopt cybersecurity strategies.

The researcher chose the phenomenon of data breaches for pervasiveness and commonality of knowledge of the problem. Data breaches have been increasing in size and frequency and are likely to continue (Edwards et al., 2016). Data breaches are widely known (Borum et al., 2015). Large public venues were chosen due to familiarity with the setting and after finding a gap in research between small businesses and similar settings such as industrial.

No previous research was found that addresses data breaches in large public venues such as stadiums, arenas, or large theme parks.

Rationale

Data breach events continue to occur and increase in frequency as attackers adopt new tactics and circumvent preventative measures (Edwards et al., 2016). Large public venues with deployed wireless networks, such as shared mobile, Wi-Fi, venue control systems, and IoT are likely targets. Large public venues may be targeted because of high usage, often with thousands of attendees, event staff, and venue operators during events. An attacker does not even need to be on the venue’s property to access the wireless network (Hoeper & Chen, 2009). Some victims of data breaches undergo recurring attacks, leading to monetary losses, including the devaluation of the organization’s stock market value (Schatz & Bashroush, 2016; Urrico, 2017). CIOs and cybersecurity managers need to prevent data breaches and provide for timely detection. The problem is that large public venue events are subject to an increased risk of cybersecurity data breaches of the venue’s wireless IT network infrastructure, increasing at an annual rate of 50% since 2013 (Morgan, 2016; NIST, n.d.).

By identifying the problem of increased risk for data breaches in large public venue wireless infrastructures, IT practitioners will be exposed to the growing negative impact of maintaining the status quo on critical infrastructure. The cybersecurity strategies gained from the study will equip undersized IT staffs with actionable evidence to use to obtain funding to strengthen the venue’s cybersecurity posture. CIOs responsible for telecommunications in large public venues and similar businesses will know about the mounting complexities and will be able to apply an appropriate security framework practically and economically.

Purpose of the Study

The purpose of this qualitative, exploratory, multiple case study was to uncover effective strategies to reduce the risk of cybersecurity data breaches of wireless IT network infrastructures at large public-event venues. To uncover the strategies, the researcher conducted seven cases of personal interviews with cybersecurity managers who typically work under a CIO's direction and decide on information security and wireless infrastructure protection in their large public venues. Themes obtained from each case triangulated with the literature review, publicly available information on the Internet, and researcher notes. The principal line of questioning in this study was related to how to develop processes, how the processes are effective, and how to implement processes. In a case study, the researcher's mode of inquiry is to answer how and why questions about a contemporary set of events, where the researcher has no control in a real-world context (Taguchi, 2018; Yin, 2017). This study's mode of inquiry and conditions aligned with case study research. Yin (2017) advocated that multiple cases have stronger validity than a single case.

Using multiple cases enabled the researcher to capture from a cross-section of venue participants to reinforce similarities, explore, and contextualize the differences. Using this research methodology should help achieve an in-depth understanding of themes for effective strategies from the collected data (Cooper & Schindler, 2014). Data collection and subsequent triangulation analysis included interviewing cybersecurity managers with open-ended and semi-structured questions, analyzing themes according to the extant literature, reviewing publicly available information on the Internet, and using researcher notes. The participants were IT managers and persons responsible for the cybersecurity of wireless network infrastructures operated by large public venues in the United States. In-depth knowledge obtained offered insight to identify effective strategies, development and implementation methods, and prioritization for applying strategies. A researcher should be careful in selecting questionnaire items to keep the reliability and validity in the original context of the study (Cooper & Schindler, 2014). Though findings in this multiple case study may not be generalizable across industries, the results helped establish a framework for different types of large public venues, such as sports stadiums, amusement parks, convention centers, or even smart cities with similar characteristics. According to Melander (2016), insights gained from smart stadiums can apply to smart cities as well. Small smart cities such as Schenectady, N.Y., and Ketchum, I.D., are self-contained and managed locally to reduce expenses, conserve natural resources, increase safety, and foster business (Wagenen, 2017). In cybersecurity, individual studies of cybersecurity behavior may not be generalizable but contribute to the systemic body of knowledge (Edgar & Manz, 2017).

Significance of the Study

Communities of interest with a similar scope of services and size can benefit from the study. These include other CIOs and cybersecurity professionals in large public venues. Among communities with similar characteristics are municipalities, convention centers, and locations with recurring temporary events like festivals and concerts, and even evolving smart communities and cities. When considering characteristics of building operations, crowd management and safety, and impaired mobility management, stadiums are like smart cities and serve to model the development of future smart cities (Panchanathan, McDaniel, Tadayon, Rukkila, & Venkateswara, 2019). A study of the phenomenon surrounding data breaches seeking discovery of effective strategies would help prevent and detect data breaches. However, it would also strengthen the cybersecurity posture of organizations in the same market. For example, a strategy that strengthens against a data breach on the internal or outsourced network may also increase resilience to denial of service attacks.

CIOs and cybersecurity professionals operating large venues and telecommunications commissioners and planners operating in small cities seeking to hire employees for cybersecurity initiatives will have the opportunity to be informed. Large convention center operators made aware of cyber-threats hidden in the crowds are more likely to prevent data breaches. Many communities host concerts in the fall or festivals throughout the year, potentially benefiting event operators with knowledge about the risks of installing high-capacity temporary networks for public Internet access. When planning for smart communities, developers need to be aware of current cybersecurity problems to prevent existing ones from permeating into future deployments or bypassing them as much as possible.

Owners of small businesses increasing in size and breadth will benefit from the research for business continuity planning. A wider community of interest may be any organization that considers implementing a high capacity network with guest and merchant data, integrates control systems such as electrical and IoT devices, and benefits from the knowledge and application of effective data breach prevention strategies.

The study was necessary to help CIOs and IT managers responsible for cybersecurity who operate large public venues to have the opportunity to be informed about the likelihood their venues will suffer a data breach and to help them to strengthen the cybersecurity posture of their IT organizations. The investigation should have been conducted to build on the existing body of knowledge. The study related to the extant literature a culmination of the available strategies, discoveries, and applications as a set of strategies to assist CIOs and cybersecurity managers in preventing data breaches. Applying effective strategies determined from this study can reduce the effects of the long-standing data breach problem and contribute to the body of knowledge. This study builds on prior research by Saber (2016), focusing on IT managers or persons responsible for cybersecurity as participants and expanding the research from small businesses to other recommended areas. Newly uncovered strategies during the investigation also added to the body of knowledge.

An increase of cybersecurity data breach incidents on the venue's IT infrastructure is also a business problem because of the potential loss of privacy information, loss of valuables, loss of organizational credibility, and market credibility loss. Furthermore, a data breach in the network could lead to attacks on the corporate network or individuals compromising their personal information, leading to an eroding brand reputation (Wang et al., 2016). CIOs and cybersecurity practitioners entrusted with financial, human resources, and policy-making decisions add value to their customers and align with the IT organization's information assurance and business objectives (Muller, 2015). The study helped the researcher uncover effective strategies that help large public venue CIOs and cybersecurity practitioners to enable a strong security posture. By using an effective security strategy, CIOs and cybersecurity practitioners will be able to generate more revenues, achieve significant savings, and maintain credibility with their customers within the markets served by large public venues.

If this research were not conducted, the status quo is the proliferation of recurring high-visibility data breaches. Potential attackers are prolific and use various tools and skills to scan potential targets for openings in their networks (Borhade & Kahate, 2016). If CIOs and cybersecurity managers remain uninformed on effective strategies, the increasing data breach trend will continue unchecked as network complexity and use increase.

Research Question

The research question for this study was: What are effective strategies large public venue operators use to reduce the risk of data breaches in their wireless networks during and between venue events?

Definitions of Terms

The following definitions cover conceptual descriptions and their application in the study.

Data breach. A data breach is an act of breaking into a network and gaining unauthorized access to sensitive or private individual or organizational data (Ullah et al., 2018). Exposed sensitive data is often used for payment fraud and identity theft (Sullivan & Maniff, 2016).

The data breach was the phenomenon under study. The interview was the primary data collection technique for qualitative studies (Cooper & Schindler, 2014). Therefore, participants were interviewed to elicit detailed descriptions surrounding data breaches. Participants who experienced a data breach would have been asked to recall and express their thoughts about the experience. Participants who did not experience a data breach were asked about their understanding of the phenomenon and the preventative and mitigative processes undertaken in the IT role. Purposive sampling was used to reach the intended population, which included persons responsible for the cybersecurity of wireless networks at large public venues. Researchers use purposive sampling based on the researcher's knowledge of the population, choosing participants for their unique characteristics, experiences, or perceptions (Cooper & Schindler, 2014; Edgar & Manz, 2017). Cybersecurity responsibilities included the application of cybersecurity controls or being involved in the decision-making process to apply controls.

Information technology. Information technology is a collection of sets of interrelated components for collecting, processing, storing, and disseminating data and information (Stair &

Reynolds, 2017). It helps meet personal, group, and enterprise-level objectives. All participants in this study had a cybersecurity role in information technology.

Information technology manager. An information technology manager is an individual who uses information technology assets to align with strategic organizational goals (Lainhart, Conboy, & Saull, 2018; Ullah & Lai, 2013). This study's target population comprises information technology managers primarily, who were likely to have historical and decision-making knowledge on cybersecurity strategies.

Large public venue. A large public venue is an indoor or outdoor multiple-purpose public facility such as a convention center, airport, shopping center, sports stadium, or arena, which is owned and operated by the private sector, cooperatives, or local government partnerships (DHS, 2015; Jia et al., 2017). All participants who qualified for this study worked in a large public venue.

Systems thinking theory. Systems thinking theory is a multi-faceted theoretical paradigm, which conceptualizes the world with real and imagined elements as systems (Checkland, 1999; von Bertalanffy, 1972). Systems thinking application to a problem establishes corrective controls and includes the communication process, whether automated or human, to decide whether to use particular controls (Checkland, 2012). Systems thinking can be a powerful tool of cybersecurity modeling for finding, characterizing, understanding, evaluating, and predicting cybersecurity (Edgar & Manz, 2017). Systems thinking was used in this study to understand data breaches within organizations holistically and as interrelated processes and relationships.

Theory of deferred action. The theory of deferred action is a theoretical paradigm that incorporates emergence into a formal design (Patel, 2009). Planned action is incorporated into every design, regardless of actual conditions. Emergence describes unknowable social actions along with their manifestations. A deferred design is a purposeful formal design to deal with emergence. Businesses and systems built with deferred design principles often have a robust infrastructure with employees and users designed to be flexible mechanisms for adapting to emergent events.

The theory of deferred action was used as a secondary lens to uncover preventative measures that could complement the corrective measures afforded by systems thinking for emergent events like data breaches. The theory helps researchers to describe the influences on the design of information systems through emergent events (Patel 2009). Information systems described in this study were a part of large public venues with wireless networks.

Theoretical Framework

This study's research focus stems from strategies for data protection in a complex and large venue wireless network environment. Specifically, data breach prevention was researched for enterprise and shared wireless networks operated in large public venues. Data breaches increase in risk as attackers adopt new tactics and circumvent current preventative measures (Edwards et al., 2016). Large public venues have unique characteristics that make them likely targets for data breaches.

In some cases, the inability to detect a data breach and recurring attacks promptly compound the losses (Schatz & Bashroush, 2016). It is vital for CIOs and cybersecurity managers to apply effective strategies to prevent and promptly detect data breach events. A theoretical framework informs existing knowledge about complex phenomena, reflects the researcher's epistemological dispositions, and provides a lens and a methodological approach for analysis (Collins & Stockton, 2018). The systems thinking theoretical lens helps in understanding the different factors in multiple systems with a common set of characteristics (Matook & Brown, 2017). A deferred action theoretical lens helps in understanding how processes and tools can be developed using plans and contingencies to meet current and emergent events (Khan, Patel, & Eldabi, 2010). Systems thinking theory was utilized to inform the research about existing knowledge and provided the primary lens to understand data breaches and the methodological approach to analyze the data. The theory of deferred action was mainly utilized to provide an emergent design-oriented planning perspective for addressing emergent events.

With a thorough understanding of data breach prevention strategies and development, the researcher can reproducibly uncover effective strategies. The knowledge obtained from this study will help to inform CIOs and cybersecurity managers who operate wireless networks in large public venues to make effective choices in preventing data breaches.

Systems Thinking Theory

Systems thinking praxis helps in understanding the collected data and in developing themes. By applying systems thinking techniques to the collected data, the researcher can understand the different factors in multiple systems with a common set of characteristics (Jonker, 2017; Matook & Brown, 2017). General system theory, an earlier version of systems thinking theory, was the basis for viewing organizations as systems with complex component interactions, supporting methodologies that can be used to explore experiences (Drack & Schwarz, 2010). Systems thinking theory can be used to reveal qualitative explanations of strategies and experiences. For example, an existing IT artifact such as an application suite intended to detect data breaches may be rendered ineffective by changing organizational policy on data sensitivity.

Theory of Deferred Action

A praxis on the theory of deferred action on collected data may help the researcher understand IT artifact development using planned and contingency approaches and enable the artifact to withstand emergent events (Khan et al., 2010). For example, an intrusion detection system implemented to alert regarding potential data breaches should be not only able to automatically update and upgrade software but be subjected to periodic reviews for effectiveness in response to emerging cyber-criminal threats. A deferred action design typically depends on end users or employees to develop contingent approaches to address emergent events (e.g., Tavanapour, Bittner, & Brügger, 2019).

Research Design

A qualitative, multiple-case study design was utilized to conduct the research. The design was appropriate as the study was based on a constructivist epistemological perspective as meaning was created from participants' unique experiences and multiple views (McCusker & Gunaydin, 2015). The goal of the research was to identify effective strategies to prevent data breaches in large public venues. Qualitative research methods tell the researcher how and why a phenomenon occurs, as the research focus is to understand and interpret participant experiences (Cooper & Schindler, 2014). The phenomenon for the focus of this study was a data breach and to understand related preventative strategies.

Case study research "investigates a contemporary phenomenon (the 'case') in depth and within its real-world context, especially when the boundaries between phenomenon and context may not be clearly evident" (Yin, 2017, p. 15). An exploratory case study uses the theoretical lens to focus on the research (Yin, 2017). This study is exploratory because the systems thinking theoretical lens provided an understanding of the phenomenon. A holistic case study design was chosen because, according to Yin (2017), the design examines an organization in its entirety as a single unit of analysis. Each case study consisted of a large public venue. A multiple case study is appropriate when a researcher seeks convergent evidence regarding the findings and conclusions (Yin, 2017). Using a multiple case study approach enabled informing the study with a cross-section of venue participants, reinforcing contextual similarities, and exploring any differences. The selected qualitative multiple case study design provided the means to investigate data breach prevention strategies in large public venues, using multiple analysis levels in a real-world context.

Data collection depended on open-ended and semi-structured interviews with IT managers and other cybersecurity professionals, who typically work under a CIO's direction in large public venues with wireless networks. Following Yin's (2017) recommendations, an interview script helped the interviewer maintain a consistent inquiry line, allowed for clarifying questions and helped to verbalize the questions in an unbiased manner. The interview questions are addressed in Chapter 3. Researcher notes were also taken on direct observation of the interviews. Research or field notes is a qualitative data collection that captures the researcher's thoughts about a participant's behavior (Edgar & Manz, 2017). The interview data was subsequently triangulated with the extant literature, publicly available online information, and researcher notes.

Assumptions and Limitations

Assumptions

Assumptions are issues researchers accept without verification (Kamin, 2017; Kirkwood & Price, 2013). In qualitative case-study research, the variables are difficult to anticipate because of the unknown nature of the interviewees' real-life experiences.

General methodological assumptions. An ontological and methodological assumption is that individual study participants may experience a different reality (Edgar & Manz, 2017; Kirkwood & Price, 2013). One participant's perspective depends on personal experiences and may have developed under different social constructs than others. The epistemology relates to the researcher's and participant's ability to influence each other. Research methods reflect on the epistemological position to drive the scope of inquiry and findings (Kirkwood & Price, 2013). The researcher must be careful to be objective and not influence participant responses (Cooper & Schindler, 2014). The axiological paradigm relates to researcher values that should not influence the study. A non-controversial subject was chosen to encourage learning, inclusion, and tolerance of differing perspectives.

Theoretical assumptions. The theoretical perspective of this study depends primarily on systems thinking theory. A good theory can be applied generally and reliably, is plausible, and is simple (Weick, 1989). Systems thinking theory has been applied to similar studies (Armenia et al., 2019; Ceric, 2015; Maahs, 2018; Saber, 2016). The researcher assumed systems thinking theory could be applied to this study and required no further validation as an adequate and appropriate theory. The theory of deferred action was utilized as a secondary theory to uncover design elements in the data that are preventative strategies that could have been missed by applying systems thinking alone. The theory of deferred action required no further validation for the context in which it was utilized.

Topic-specific assumptions. It was assumed that data breaches manifest similarly across different types of large public venues. The research focused on the characteristics of wireless networks in large public venues, not on demographics. The research also focused on the knowledge and experiences of participants who were not necessarily cybersecurity experts but had the knowledge and experience to conduct cybersecurity roles. It was essential for this study to achieve a deep understanding of participants' roles, knowledge, and experiences.

As noted by Brinkmann (2016), interviewees were assumed to be knowledgeable, apply the practices required of their role, and able to describe their lived experiences. Interviewees were responsible for the operation and security of an enterprise or shared wireless network in a large public venue. CIOs in these types of venues actively participate and define strategies for their shared wireless network. Similarly, cybersecurity managers apply and monitor security controls for wireless networks that fall under their purview. The researcher assumed the ability to communicate questions effectively and consistently to allow the interviewees to elucidate responses relating to the research question. It was also assumed that the interviewees provided honest responses.

Limitations

Limitations are unavoidable flaws in the study that lead researchers to restrict their conclusions (Kamin, 2017; Kirkwood & Price, 2013). As an instrument of study, the researcher was a novice in the techniques and approaches to fully capture the data necessary to answer the research question.

Design flaw limitations. A design flaw limitation was that the study participants might not represent all large public venue operators of wireless networks. The study may not be exhaustive and not transferable to other industries, affecting external validity (Cooper & Schindler, 2014). Compared to quantitative research methods, the sample size for case study research is small, limiting the ability to project the research findings to a broader target population (Cooper & Schindler, 2014).

Delimitations. Delimitations are boundaries set by researchers to keep the study within the defined scope and context (Kamin, 2017; Svensson & Doumas, 2013). The delimitations in this case study focused on the ability to obtain potentially sensitive information, the interview setting, sample size, and geographic location. The researcher chose to conduct this study after learning of the frequency of occurrences of preventable breaches.

The target sample population for this study was limited to an accessible number of large public venues that also met the wireless infrastructure requirement. Even though the expected staff size in each location was small, the target population had to be reachable. Due to the sensitive nature of the security-related information, which included internal practices and defenses, participants may not have readily disclosed information. After weighing the potential for obtaining sensitive information with a limited target population, a reasonable approach was to limit the interview format to online Zoom recordings and limit the population to the entire United States. While an onsite interview setting could provide more meaningful insights, the researcher notes and the audio recordings of Zoom meeting sessions were enough to obtain the information. The sample size consisted of seven cases from seven large public venue operators. The target population included IT managers and persons responsible for cybersecurity who typically work under a CIO's direction to operate a wireless network in a large public venue. The sample population was also intended to include property owners that outsource shared wireless networks. Excluded were locations such as parks and non-permanent structures that host temporary events.

Organization for Remainder of the Study

This research study is organized into five chapters, with additional sections for references and appendices. Chapter 2 is a literature review of research that supports this study. It encompasses research on cybersecurity data breach prevention, characteristics of large public venues that could make them desirable targets, and the development of effective strategies to address risks in similar environments. Chapter 3 contains the research design, the target population, the sample, the setting, instrument and measurements, data collection and analysis, validity, and the study's ethical considerations. Chapter 4 contains the findings associated with the interviews, observations, document reviews, and data collection related to the research questions. It also summarizes the data analysis methodology and concludes with analyzing the interview data based on the research questions. Chapter 5 contains an overview of the study and explains the findings.

CHAPTER 2. LITERATURE REVIEW

Large public venue events are subject to an increased risk of cybersecurity data breaches of the venue's wireless IT network infrastructure, increasing at an annual rate of 50% since 2013 (Morgan, 2016; NIST, n.d.). The purpose of this qualitative, exploratory, multiple case study was to uncover effective strategies to reduce the risk of cybersecurity data breaches of wireless IT network infrastructures at large public-event venues.

Large public venues provide many services to different types of customers over wireless infrastructures and may be vulnerable to data breaches during and after events (Bartoli et al., 2018; Wang et al., 2016). Also, data breaches can relate to and lead to other types of cybersecurity events such as identity theft and data loss that would damage the host organization (McGuire, 2015). Loukaka and Rahman (2017) supported an economic impact after an attack but underline organizations' reluctance to change, adapt, and collaborate with others in the market (p. 21).

Data breaches are expensive and affect organizations at an increasing rate. According to the FBI IC3 (2017), reported losses in the United States because of data breaches among individuals and corporations exceeded $138 million. The frequency and size of data breaches have been increasing since 2009 (Edwards et al., 2016). Data breaches can have high associated costs because of the compounding effects of long detection times, averaging 30 days, and often recurring attacks within two years of the first event (Schatz & Bashroush, 2016). Data breaches are also complicated by going mostly unreported, amounting to approximately 66% of the attacks (LiCalzi, 2017).

After reviewing the extant research, the researcher understood that uncovering data breach prevention strategies in large public venues may be used to reduce the risk of a data breach for wireless network operators. A data breach may not be preventable, but the detection time may be reduced to minimize the venue’s impact. Once a data breach occurs, it is up to the organization to be prepared to minimize damages and restore normal operation.

Data breaches can result in damage to a large public venue’s wireless infrastructure. The literature review contains information on four main themes: (a) data breaches, (b) wireless network infrastructure, (c) large public venues, and (d) strategy development. The subthemes for data breaches are: (a) intrusion prevention, (b) intrusion detection, and (c) incident response and mitigation. Subthemes for wireless network infrastructure are: (a) critical information infrastructure, (b) wireless vulnerabilities, (c) large attack surface and high density, and (d) staffing.

Methods of Searching

The scholarly literature source used in preparation for this case study was the Capella University electronic library. Capella’s library provided access to an extensive collection of scholarly journals, books, and dissertations to support the research. The researcher searched IT, management, cybersecurity-related journals for literature related to the research topic and included the *Journal of Systems and Information Technology*, *Strategic Management Journal, Journal of Information Technology,* and *Information & Management*. Once fewer journals appeared in the search, Google Scholar linked to the Capella University Library was used to conduct further searches, resulting in works appearing from the Institute of Electrical and Electronics Engineers (IEEE) for detailed vulnerability information on wireless technologies. The journals selected were current within five years, with high validity, and pertinent to the research topic. While the primary focus was to search for peer-reviewed journals to uncover strategies to reduce the risk of data breaches, books, conference proceedings, dissertations, consulting company reports, government reports, and websites provided a depth of information for the study.

Keyword searches included *large public venues*, *wireless network*, *sports stadiums*, *sports arenas*, *wireless vulnerabilities*, and *critical infrastructures.*

Theoretical Orientation for the Study

Systems Thinking Theory

This study's systems thinking theoretical orientation has been used to uncover data protection strategies in similar studies. Systems thinking theory was used to analyze the interdependencies between people to manage project risks in complex public-private partnership projects (PPP), as risks from multiple interacting organizations cannot be addressed either individually or managed by a single organization (Loosemore & Cheung, 2015). Stanton, Salmon, and Walker (2018) recommended taking the cybersecurity system as the unit of analysis and all the component interactions that shape behavior to understand systems and emergent properties. Identifying participant experiences and behaviors was essential for understanding and improving systems' protection from new data breaches.

Systems thinking theory originates from the general system theory (Loosemore & Cheung, 2015). Von Bertalanffy (2015) explained that the general system theory played a dominant role in a wide range of fields, from industrial enterprise to esoteric topics of pure science (p. 3). One objective of von Bertalanffy was to consider alternative solutions and choose the most efficient and cost-effective among tremendously complex network interactions in general systems. At the time, experimentation and mathematical modeling did not include qualitative considerations in research. Von Bertalanffy reasoned that "humanistic aspects can[not] be evaded unless general systems theory is limited to a restricted and fractional vision" (von Bertalanffy, 1972, p. 424). In later research, von Bertalanffy argued that decisions undertaken in a complex system are not always rational, and observed or experiential data would be beneficial in analyzing systems (von Bertalanffy, 2015).

Systems thinking theory emerged from biological principles of thinking of whole systems from von Bertalanffy and electrical, communication, and control engineering (Checkland, 1999). Psychology, anthropology, and linguistics groups also contributed to the development of systems thinking, but to a lesser degree. The resulting foundation for systems thinking was established on emergence and hierarchy and communication and control. Hierarchy relates to their formation at different levels, which generates the levels, what separates the levels, and what connects them (Checkland, 1999). Open systems are open to the environment and can be manipulated more effectively than closed systems with a limited number of components. According to von Bertalanffy, biological closed systems try to reach equilibrium, while other closed system models reach higher entropy (Checkland, 1999). Communication can then be used to control hierarchical open systems. A parallel can be drawn to a framework established wherein devices communicate the status of certain variables with automated controllers for active regulation and achieve sustained optimal operation. The principles can apply to more complex systems such as communication networks or IT organizations.

Theory of Deferred Action

The theory of deferred action complements system thinking theory by accounting for emergent events that cannot be predicted. Checkland and Winter (2006) recognized emergent events implicitly and real-world experiences of problem situations when developing the soft systems methodology (SSM). Patel and Hackney (2008) proposed techniques based on the theory of deferred action to establish which structural and functional designs can be deferred.

Deferred systems analysis requires continuous systems analysis techniques for continuous and emergent systems (Patel & Hackney, 2008). To apply continuous analysis, strategically located organizational deferment points serve as mechanisms within a formal system to enable continuous and deferred systems responses. A formal system can be automated, but the organizational deferment points may likely be human gatekeepers capable of identifying and responding based on the perceived impact of emergent events.

The researcher used systems thinking theory as part of a systematic approach to generate questions and analyze responses for themes that may emerge from the study (e.g., Stanton et al., 2018). Instead of looking for artifacts, such as vendor implementations of a particular intrusion detection system, the researcher sought to understand strategies used by participant organizations to prevent data breaches on their large public venue wireless infrastructures. Using a system thinking approach, the researcher understood the components in the infrastructures and the relationships between the components in the system (e.g., Checkland, 1999). Systems thinking helped to holistically identify the automated and human components and understand the system's interrelationships.

Systems thinking theory complements the theory of deferred action when used to uncover latent strategies in participant responses. Security, in general, requires vigilance and planned responses to events (e.g., IAEMSC, 2017). Deferred action theory introduces the design concepts for organization deferment points and continuous systems analysis to act on new threats, requiring a response from an organization or individuals (Patel & Hackney, 2008). One practical application can place physical sensors in strategic locations to efficiently and accurately detect and trigger alarms. Another illustration can be to structure the organization's first responders to be alerted continuously, covering chokepoints and areas typically not covered. Additional techniques may emerge from thinking in terms of deferred action, but continuous analysis at deferment points provides a view of preparing for emergent events.

Review of the Literature

Data Breaches

Since 2009, large amounts of data have been collected on data breach events. Much of the data has been categorized by industry, such as financial, healthcare, retail, education, and public sector. According to a report by Price Waterhouse Cooper, approximately 38% of businesses that experienced financial losses also suffered intellectual property theft and brand reputation damage because of the attack (Gerard, 2016).

A data breach can be defined as breaking into a network and gaining unauthorized access to sensitive or private individual or organizational data (Ullah et al., 2018). It can also be the unauthorized release of secure information from within an organization into an untrusted external environment (Morovati, Kadam, & Ghorbani, 2016). Data breaches often result from viruses, malware, distributed denial of service attacks, and others. Data breaches are widely known but often poorly understood (Borum et al., 2015). Decision-makers mainly focus on the technical dimension of cyber-threats, such as malware, viruses, and distributed denial of service attacks (DDoS). Decision-makers may miss the human dimension, which includes activities, intentions, and capabilities. Evans, Maglaras, He, and Janicke's (2016) research on cybersecurity assurance supports organizations' focus on technical elements that do not provide real assurance. A complete understanding of a data breach involves taking cyber-intelligence and risk management posture with continuous risk assessment (Borum et al., 2015).

Public awareness and nondisclosure. Data breaches occur in government agencies, businesses, and individuals. A 2016 Pew Research Center national survey of more than 1,000 adults found most Americans have personally experienced a data breach and lack trust, especially in the government and social media organizations, to protect their data (Olmstead & Smith, 2017). Most data breaches appeared as fraudulent credit card transactions, followed by sensitive information like account numbers, email accounts, and personally identifiable information. About half of Americans felt their personal information was less secure than five years prior. Most Americans expected significant cyber-attacks in the next five years, especially in public locations (Olmstead & Smith, 2017). Most Americans did not apply security best practices, such as using two-factor authentication, password management software, or automatic screen locks on their mobile devices (Olmstead & Smith, 2017).

When respondents were asked about their awareness of five high-profile cyber-attacks that had occurred around the time, three quarters had heard about the 2013 Target breach, and half were well informed (Olmstead & Smith, 2017). However, respondents were less aware and informed about the 2015 AshleyMadison.com website attack, the 2014 Sony corporate attack, the 2015 United States Office of Personnel Management attack on records, and the 2015 Ukrainian power grid computer systems attack (Olmstead & Smith, 2017). The attacks were larger and arguably more dangerous than the Target attack. An implication is that many Americans may not have had the opportunity to learn from the data breaches and are not motivated to apply security best practices.

The frequency and size of data breaches have been increasing since 2009 (Edwards et al., 2016). Applying Bayesian Generalized Linear Models (GBLM) on data breach events occurring between 2006 and 2015 predicted the likelihood of some larger events. Their findings uncovered some contradictory evidence, such as observing the frequency of reported data breaches may have stabilized. Moreover, the largest data breach disclosed was in 2009, and the second largest in 2007. Even though data breach disclosure laws have been enacted since that time, researchers believe many breaches remain undisclosed. Organizations tend not to disclose data breaches to avoid exposure as they do not want to expose information about their security posture information unless necessary (Sarabi, Naghizadeh, Liu, & Liu, 2016).

Data breaches can have high associated costs because of the compounding effects of long detection times, averaging 30 days, and often recurring attacks within two years of the first event (Schatz & Bashroush, 2016). Data breaches are also complicated by going mostly unreported, amounting to about 66% of the attacks (LiCalzi, 2017). The impact compounds when cyber-criminals use breach-related data for other cyber-crimes, such as individual identity theft, often propagating within a short time of the initial data breach (Hughes et al., 2017). Exposed sensitive data is often used for payment fraud and identity theft (Sullivan & Maniff, 2016).

Types of attacks. An attack exploits a vulnerability in a closed system (Borhade & Kahate, 2016). Among the many types of attacks, some of the most likely in a public network may be related to authentication, connect-back, connect availability use, and backdoor attacks. An active attack compromises availability or integrity, such as attempts to change or affect operation (Borhade & Kahate, 2016). A passive attack affects data confidentiality without affecting system resources. For example, brute force and dictionary password capture, keylogging, phishing, spidering, and port binding can be considered passive attacks. Zero-day attacks involving malware or other forms are difficult to detect and require constant monitoring. Intrusion detection is the accurate realization that actions are taken to compromise the confidentiality, integrity, and availability of resources (Borhade & Kahate, 2016). It expands on access controls previously used by incorporating processing layers to monitor, detect, and respond to unauthorized activities.

Data breaches also occur because of attacks on backdoor vulnerabilities in IT systems. Backdoors include software installed on servers and systems used to troubleshoot and other purposes (Borhade & Kahate, 2016). Backdoors bypass security mechanisms for convenient access by the organization's support staff, vendors, and are exploited by potential attackers.

Behavioral aspects. Internal risky behaviors can have a strong impact on cybersecurity. Evans et al. (2016) iterate people are the principal vulnerabilities to a secure enterprise, human error, lack of staff awareness, and weaknesses in vetting individuals, contributing to some of the worst breaches in recent history. In some cases, individuals have been rewarded for falsely being perceived as helpful during events without applying security controls or practices in actuality. More broadly, people continue to believe events such as data breaches only happen to other people, which may lead to risky behaviors that affect cybersecurity (Evans et al., 2016). Insider threat continues to be a major cause of data breaches. Also, user data breach incidents continue to rise in organizations regardless of increased employee awareness, use of security tools, and strategies for securing information systems (Mitra, 2016).

Perri and Perri (2018) designed a pedagogical platform to train business students on data breach management. In their review, the researchers reiterate that data breaches have become large in number and impact. Perri and Perri's (2018) training topics include data breach prevention and assume that data breaches are the new norm. Data breach prevention includes employee training, data encryption, portable data management, intrusion detection and prevention, content filtering, vulnerability assessments, software patch management, security information, incident response, handling threat intelligence, and cyber-insurance. Applying data breach prevention techniques is required, but organizations should be prepared for a breach, which is likely to occur (Mitra, 2016; Nazareth & Choi, 2015). Densham (2015) proposed to assume systems will be compromised and to have a comprehensive mitigation plan.

Intrusion Prevention

Data breaches cannot always be prevented because of access, sharing, information use requirements, and other issues (e.g., Alneyadi et al., 2016; Ullah et al., 2018). Although firewalls, intrusion detection systems, intrusion prevention systems, and virtual private networks have long been used as security measures against well-defined, structured, and constant threats, those measures fail to protect against evolving and emergent attacks (Borhade & Kahate, 2016). A firewall's primary function is to apply policies between network segments to block access to unauthorized users, computers, or networks automatically (Borhade & Kahate, 2016). Some firewalls fail to detect application-layer attacks, internal attacks, or new attacks (Borhade & Kahate, 2016).

An attacker who uses malicious email attachments, application vulnerabilities, or other vectors (Alneyadi et al., 2016) can often defeat a firewall. Intrusion prevention and detection systems and virtual private networks also lack the sophistication to adapt, persist, and understand the nature of the data under protection. Machine learning and methods combined with analyst intelligence can detect new attacks and reduce the time between intrusion prevention and detection (Veeramachaneni, Arnaldo, Korrapati, Bassias, & Li, 2016). Efforts to improve against evolving attacks have also led to considering text clustering and social network analysis (Alneyadi et al., 2016). Most data breach prevention methods have limitations, mainly relying on inflexible techniques to combat evolving attacks.

According to Lanjouw and Schankerman (as cited in Love & Roper, 2015), small to medium enterprises often employ different data protection strategies than larger enterprises. For example, a small enterprise may prefer to use secrecy and speed to market to protect intellectual property rather than filing for a patent. However, Saber's (2016) study "revealed organization size is not a factor when it comes to protecting data…[which is] crucial to business survival" (p. 104). Lanjouw and Schankerman studied data protection strategies across small to medium enterprises, while Saber appeared to refer to motivations for protecting data while focusing on small businesses. Other recommended methods to protect against data breaches are avoiding storing critical data on an enterprise network and using Cloud service providers to store critical data (Saber, 2016).

Preventing data breaches involves applying countermeasures specific to an organization's environment. However, finding effective solutions requires strategies such as risk management, strategic cybersecurity intelligence, education and awareness, and eliminating risky behaviors. The leading general standard for security management is ISO/IEC 27001, although it focuses on compliance rather than the primary desire to protect data (Evans et al., 2016). Strategic cybersecurity intelligence focuses on prevention by using data collection and analysis to understand threat actors' capabilities, plans, and intentions to develop countermeasures (Borum et al., 2015). Positive results among IT professionals have been achieved in organizations that implemented an awareness program, focused training on countermeasures, and performed an ongoing evaluation of the program (Torten, Reaiche, & Boyle, 2018). Risky behaviors within an organization can be reduced through behavior modification, such as enforcing policies and practices using a feedback loop and rewarding the application of cybersecurity controls and practices (Evans et al., 2016).

Once countermeasures or controls are in place, organizations should monitor the controls through common channels (Evans et al., 2016). These include penetration testing, vulnerability assessments, risk assessments, auditing, patch management, incident statistics, and anti-virus software updates. Auditing and cyber-risk assessments are the most common. Monitoring through common channels applies to past events and fails to proactively monitor human behavior (Evans et al., 2016).

Data breach countermeasures are unable to protect in real-time (Ullah et al., 2018). Relative to the state of data, much of the research focuses on protecting data in use, not at rest or in transit. Ullah et al. (2018) also found that most data breach countermeasures focus on preventative and detective techniques and not investigative. Some countermeasures do not account for privacy and ethical concerns, leading to acceptance issues during implementation (Ullah et al., 2018). Lastly, Ullah et al. (2018) detail no standardized approach to evaluate data breach countermeasures.

Nondisclosure versus disclosure. Applying nondisclosure policies may help to prevent cybersecurity events. However, its implementation and purpose have resulted in mixed outcomes. Nondisclosure versus disclosure policies has been the subject of much research. Amazon Web Services (AWS) does not disclose its internal Cloud computing architecture for security purposes (Ramachandran, 2016). In this case, nondisclosure helps protect the security and intellectual property of a company's hardware and software. Also, vendors often protect their reputation and assets using bounties (Eichensehr, 2016). In 2015, Google paid $2 million in bounties to security researchers that would report vulnerabilities and allow Google to patch the software before its knowledge became public (Eichensehr, 2016).

The price paid for vulnerability bounties is substantially lower than the black-market value and not in line with the values applied by the National Vulnerability Database (NVD) (Munaiah & Meneely, 2016). Once vendors learn of their product's vulnerabilities, they may not be motivated to disclose the information to the public, potentially those most adversely affected. Counter to vendor protection, since the 1990s, the National Security Agency has paid hardware and software companies not to disclose vulnerabilities or backdoors for exploitation and espionage purposes (Eichensehr, 2016). For most vulnerabilities, disclosure to the public is not a matter of occurrence but when and to what level (Dingman & Russo, 2015).

Related research. Data breach prevention on Supervisory Control and Data Acquisition (SCADA) systems rely on automated dynamic tools, such as early warning systems that can predict the presence of faults (Alcaraz & Zeadally, 2015). Sensors embedded in strategic locations continuously feed data into automated tools for detection. Studying SCADA systems may be relevant to data breach prevention in large public venues in that a portion of the infrastructure is likely to support automated heating, ventilation, and air-conditioning (HVAC) equipment controls and interfacing with other systems. The Target store data breach of 2013 occurred through Fazio Mechanical, a third-party HVAC vendor (Shu, Tian, Ciambrone, & Yao, 2017).

Intrusion prevention systems use automated methods to block malicious traffic or connections without completely blocking all network activity whenever possible (Wahl, 2016). An intrusion prevention system actively monitors network activity, often located at the boundary between the internal and external company networks. Intrusion prevention systems may perform intrusion tolerance, which attempts to work around an intrusion, isolating it from normally operating traffic in the network while maintaining data integrity and availability (Wahl, 2016).

An intrusion prevention system may contain an intrusion detection function or rely on alerts triggered by an intrusion detection system. Intrusion prevention is difficult to employ, as it is dependent on detection accuracy in a complex dynamic environment and can shut down an entire network (Wahl, 2016).

Even if a data breach attack is imminent, security professionals should invest in the resources and funds necessary for prevention and deterrence. Any prevented attack has a definite advantage in reducing damage potential, recovery effort, and subsequent risk assessment and vulnerability reduction effort (Nazareth & Choi, 2015). Deterrence has different forms and levels of effectiveness, such as policies for internal threats with repeat violations or less effect on external threats because of lack of visibility (Nazareth & Choi, 2015). The effectiveness of deterrence varies with the security tool investment level by deploying security resources more effectively (Nazareth & Choi, 2015). From a systems perspective, investments should never go to zero in any area under any circumstances because that will always increase security costs. The researchers also found that investment in security tools for deterrence activities had a lower payoff than tools designed to detect attacks covered in the next section.

Intrusion Detection

Intrusion detection is the accurate identification of actions taken to compromise the confidentiality, integrity, and availability of resources (Borhade & Kahate, 2016). It had its beginnings in access control, where only authorized employees could log into systems to perform work. Intrusion detection expands on access controls by incorporating processing layers for monitoring, detection, and responses to unauthorized activities (Borhade & Kahate, 2016). An intrusion detection system uses software to automate the entire process (Bamakan, Amiri, Mirzabagheri, & Shi, 2015). Among the actions intrusion detections systems perform are (a) monitor and analyze the system and user activities, (b) audit vulnerabilities and system configuration, (c) assess the integrity of data files and critical systems, (d) analyze abnormal activities, and (e) audit the operating system (Jabbar & Aluvalu, 2017). Intrusion detection is difficult to accomplish, as attacks on a network may come from vectors at every entry point and in multiple directions.

Intrusion detection research. Intrusion detection must scale to meet the demands of a large scale of traffic data, deal with heterogeneous data sets, decipher ambiguous behaviors between legitimate and authentic attacks in a dynamic environment (Bamakan et al., 2015). The researchers realized that computational intelligence methods resulted in better performance than prior methods using high-speed computing, fault tolerance, and managing noisy data sets. Computational intelligent systems include artificial immune and neural networks, swarm intelligence, and soft computing methods to apply to networks and Cloud-computing. Bamakan et al. (2015) built upon prior research using multiple criteria linear programming, an optimization-based classification algorithm. Also, Bamakan et al. (2015) applied particle swarm optimization, which borrows from biological behaviors, on multiple criteria. Particle swarm optimization is simple to implement, scalable, robust, and fast in finding an optimal solution. The application of particle swarm optimization helped improve the accuracy and running time over the sole use of multiple criteria linear programming.

Other researchers addressed the problem of large heterogeneous or unbalanced data sets with a hybrid computer network topology design and anomaly-based selection (e.g., Mazini, Shirazi, & Mahdavi, 2018). In Mazini et al.'s (2018) example, the artificial bee colony algorithm selects features, and the AdaBoost machine-learning meta-algorithm evaluates and classifies the features. The results increased the detection rate across different data sets. Though some were marginal improvements, others were as much as 20% to 30%.

A highly efficient approach for the classification and training stages uses a centroid-based classification hybrid learning approach (Setiawan, Djanali, & Ahmad, 2017). Classification performance is improved by applying an unsupervised k-means type clustering technique first, then feeding the results into a supervised classifier. The researchers analyzed 11 papers using a centroid-based classification. A benefit of using a centroid-based classification is a lessened dependency on data pre-processing since the beginning stage clusters the data.

With the increasing sophistication of cyber-attacks, intrusion detection's main challenge is recognizing unknown attacks (Carrasco & Sicilia, 2018). Algorithms ported from general-purpose use have resulted in misuse detection and anomaly detection techniques. Misuse detection compares current activities with actions expected of an attacker. Anomaly detection builds a normal activity profile for legitimate system use. Anomaly detection has more manageable disadvantages and was the basis for research using an outlier detection method, neighborhood node trust, then a skip-gram model (Carrasco & Sicilia, 2018).

Detecting outliers and strengthening algorithms. An outlier detection method uses neighborhood outlier factors (NOF) on k-cluster distances to increase detection precision and stability over prior methods (Jabez & Muthukumar, 2015). Similarly, a neighbor node trust approach determines risky behaviors in wireless sensor networks (Sajjad, Bouk, & Yousaf, 2015). The skip-gram model, in turn, learns about the relationships among components of the network behavior. When tested against a known intrusion detection data set such as USNW-NB15, the skip-gram model required 82.7% less storage, achieved 99.20% precision or advantage over false positives, and a recall or detection rate 82.07%. The metrics were achieved with the skip-gram technique requiring less storage, less input, and no prior knowledge (unsupervised), exhibiting several advantages over most other systems (Sajjad et al., 2015).

To exploit the strength of weak learning algorithms, Jabbar and Aluvalu (2017) aggregated random forest techniques, multiclass classifier average one dependency estimator (AODE) for accuracy, and overcoming naïve Bayes shortcomings well as ensemble learning. Experimental results revealed that the aggregated classifiers were more effective for detecting intrusions on network nodes than single parameter evaluation.

Random neural networks (RNN) can be applied to embedded low power systems with limited resources and often zero security (Saeed, Ahmadinia, Javed, & Larijani, 2016). The RNN dataset takes valid and invalid behavioral cases as input parameters to baseline behavior. The RNN software is then embedded into a base station to detect the presence of malicious sensor nodes. It also measures performance overhead when data is transmitted to the base station. However, the embedded software on the base station is accessible by anyone, rendering it vulnerable to attacks (Saeed et al., 2016).

Automated intrusion detection systems analyze log files continuously for anomalies. Landauer, Wurzenberger, Skopik, Settanni, and Filzmoser's (2018) research improved upon statically clustered similar items with anomaly detection based on outliers. The researchers added clustering groups incrementally within time windows, making it a more dynamic approach for anomaly and intrusion detection. Also, the time windows formed a common channel by which clusters can be compared, which was not previously possible with static clusters (Landauer et al., 2018). The resulting experiments and data validation demonstrated up to 99.3% precision and 61.8% recall rate when coupled with a self-learning algorithm.

Log files can be analyzed for attack variants, such as the Malware Zero Access attack in 2013 (Hidayanto, Muhammad, Kusumawardani, & Syafaat, 2017). The FP-Max algorithm is used to find the maximum number of rules that have a similar pattern. The Apriori Categorization Algorithm is then used to find the frequency for each rule. The data mining techniques on log files resulted in that 90% of the attacks were triggered by eight intrusion detection rules, and 17 rules triggered 100% of the attacks.

Unsupervised versus supervised machine learning. Intrusion detection and automated mitigation can be improved using unsupervised machine learning techniques. Unsupervised machine learning is preferable to supervised analyst-driven detection and mitigation because no human resources are necessary for detection (Veeramachaneni et al., 2016). Three of the major challenges for intrusion detection are: (a) lack of labeled data normally applied by analysts, (b) constantly evolving attacks as threat actors learn, and (c) limited analyst time and budget resources (Veeramachaneni et al., 2016). The intrusion detection platform developed by the researchers combined big data behavioral analytics, several outlier detection methods, incorporating feedback from analysts, and a supervised learning module. When validated across 3.6 billion log lines, unsupervised machine learning techniques showed an increasing detection rate of 3.41 times that of a simpler anomaly detector and more than a five-fold reduction in false positives (Veeramachaneni et al., 2016).

Another approach designed to alleviate analyst-driven detection is to apply cognitive assistants, which learn from expert analysts on investigating advanced persistent threat intrusions (Tecuci, Marcu, Meckl, & Boicu, 2018). Teaching a cognitive assistant requires an expert cyber-analyst to follow a systematic evidence-based scientific method to detect an advanced persistent threat, such as a data breach. When using this approach, alerts lead to alternative explanatory hypotheses that represent either intrusion or legitimate activities. Each hypothesis guides the search for evidence to support or not support each claim, thus determining the probability of each hypothesis (Tecuci et al., 2018).

Genetic algorithm-based parameter selection and multiple support vector machine classifiers on wireless mesh networks can achieve high accuracy (Vijayanand, Devaraj, & Kannapiran, 2018). Wireless mesh networks are susceptible to flooding denial-of-service attacks, blackhole man-in-the-middle attacks drop packets from all nodes, and grey-hole man-in-the-middle attacks dropping a packet for select nodes. The genetic algorithm uses a population-based search technique that incorporates biological constructs of selection, crossover, and mutation. Genetic algorithms apply to address uncertainties (Hamamoto, Carvalho, Sampaio, Abrão, & Proença, 2018). Specific parameters of network traffic data increase detection accuracy, while others have a decreasing effect. The genetic algorithm is applied to each category of attack to select the parameters with the highest accuracy. Experiments using known intrusion detection data sets resulted in higher accuracy, less computational complexity, and less traffic overhead than techniques not optimized by the genetic algorithm (Vijayanand et al., 2018).

Artificial neural networks can be applied to network intrusion detection and deep packet inspection (Shenfield, Day, & Ayesh, 2018). Intrusion detection systems are often plagued by false positives, especially shell programs that can be used for malicious or benign purposes. Artificial neural networks are a form of a machine-learning algorithm, where inputs are weighed and fed based on decisions to artificial neurons in one or more layers (Shenfield et al., 2018). Artificial neural networks use a learning rule to adaptively tune based on the weights and biases, enabling the capturing of complex non-linear relationships without having prior knowledge (i.e., unsupervised learning). Also, because of the adaptive nature, no domain knowledge is required for classification. Shenfield et al.'s (2018) experiments returned a 98% average accuracy rate and 2% false positives with 400,000 samples of data.

Network and device-level. Intrusion detection techniques apply to identify networks of illegally controlled computers, called botnets (Álvarez Cid-Fuentes, Szabo, & Falkner, 2018). Mirai botnet malware created the potentially most massive denial of service attack in history with large botnets of about 100,000 small IoT devices, at an estimated throughput of 1.2 terabits per second, on Dyn Corporation's domain name system servers in 2016. The researchers built upon signature-based and anomaly-based botnet detection with a framework that builds and stores hosts' legitimate behavior in a decentralized network and analyzes packets (Álvarez Cid-Fuentes et al., 2018). Moreover, it is a plug-and-play mechanism that can be added to any network. Experiments on publicly available datasets revealed the framework achieved similar or better accuracy in detecting novel botnets than contemporary approaches, with a reduction in false positives of one to two orders of magnitude.

On the device level, smartphones are ubiquitous and have been subjected to techniques like intrusion detection. Zulkefli, Singh, Mohd Shariff, and Samsudin (2017) addressed spear phishing, the most popular type of advanced persistent threat, with an application to detect URL hijacking on smartphones. An attacker sends fake URLs resembling popular and legitimate sites to a user's smartphone as a web or email attachment or during sensing and service connection (Zulkefli et al., 2017). A sensing and service connection example is Bluetooth sense to connect with a file transfer service profile.

The researchers proposed a label-based spear phish detection (LESSIE) machine learning technique to examine URLs with blacklisting and heuristics (Zulkefli et al., 2017). The technique incorporates domain name service redirect locations, results from search engines, blacklist lookups, statistical references, domain age, country-specific domain ranking, and similarity scores. Experimental results revealed a slightly lower accuracy than a domain-based technique using a small dataset. LESSIE can potentially outperform other methods, as it more thoroughly covers more parameters and runs on a smartphone (Zulkefli et al., 2017).

As part of the findings of a non-experimental correlational study between network-based intrusion detection and host-based intrusion detection systems, there are differences in the number of reported cyber-attacks depending on the type or model of the intrusion detection system (Wahl, 2016). The network-based system detected a higher number of attacks than a host-based system. A knowledge or signature-based intrusion detection system detected a larger number of potential cyber-attacks, with higher false negatives and lowered false positive rates, than a behavior-based system reporting higher false positives. The findings reinforce that intrusion prevention can be improved when using multiple intrusion detection approaches and layers of hardware and software to leverage each's strengths. Wahl's (2016) findings seem to contradict the extant intrusion detection research, which focuses mostly on anomaly-based or behavioral intrusion detection. It is noteworthy that in the extant literature, knowledge-based detection functions more often feed anomaly-based functions to increase accuracy and speed and reduce resource usage.

Incident Response and Mitigation

Incident response tools enable a system to automatically and rapidly react and recover from threatening cybersecurity situations (e.g., Alcaraz & Zeadally, 2015). An example of a reactive tool is the DARPA-funded Event Monitoring Enabling Responses to Anomalous Live Disturbances (EMERALD) project, which can trace malicious activities across large networks and automatically initiate attack isolation and other responses (Alcaraz & Zeadally, 2015).

Commercial versions that perform automated reactions and responses to protect network traffic, developed over a decade, including Cisco's intrusion protection system (IPS) and Sourcefire IPS (Garcia-Teodoro, Diaz-Verdejo, Maciá-Fernández, & Vázquez, 2009).

Recovery tools address faults and enable systems to return to a normal state of operation (e.g., Alcaraz & Zeadally, 2015). An example is a tool developed by seven European Universities called the SELFMAN Research Project. It stems from cybernetics and system theory systems for self-regulation to reinstate normal operation in large-scale distributed systems automatically and dynamically (Alcaraz & Zeadally, 2015). Protection services provided by SELFMAN depend on complex and decentralized subsystems, such as access over the Internet, GPS geolocation and visualization, mobile networks for out-of-band remote access, and IoT-like wireless sensors for localized and detailed monitoring (Van Roy et al., 2008). A self-managing Internet application called Scalaris stems from the SELFMAN project. Wikipedia uses it as an overlay system for its scalability in maintaining high data processing availability during node failures and network problems (Van Roy, 2009).

Critical information infrastructure protection has been applied to industrial control systems (Alcaraz & Zeadally, 2015). Principles that pertain to industrial control systems are also applicable to large public venues as critical infrastructures. For example, protecting a networked system should focus on security mechanisms for detection and intelligently responding to vulnerabilities and faults that threat actors can exploit. Both types of actions can apply equally to an industrial or public venue wireless network. It is developing the baseline behavior, for example, of a node in an industrial setting, which is identical to establishing one in a public venue's network.

Many situational awareness approaches do not ensure complete protection based on prevention, detection, and response, nor do the approaches satisfy the unique conditions and prerequisites of industrial control environments (e.g., Puuska et al., 2018). Similarly, protections against a public wireless venue's network vulnerabilities and data breaches cannot be assured. Once a data breach event occurs, some of the mitigation can be accomplished using automated systems. However, the organization should have a plan in place for contingencies for the attack itself and perform recovery actions such as damage control and remunerations to those affected.

Cost and liability reduction. Four factors that can reduce the cost of a data breach are (a) consultative engagement, (b) CISO appointment, (c) using incidence response plan, and (d) having a strong security posture (Miklai, 2018). A consultative engagement involves security experts providing guidance specific to the organization. The CISO, though still an evolving role, needs to have technical and business expertise. More intuitively, merely having someone in a CISO role that focuses on security reduces the average cost of a data breach. An incident response plan should be practiced and should have representatives for all the stakeholders, a plan for restoring the organization from the data breach, a communication plan for all the stakeholders, and service offerings to the stakeholders to re-establish trust in the organization and the market (Miklai, 2018). A strong security posture may include data encryption, the use of firewalls, risk management, governance, and appropriate countermeasures in place to prevent, deter, and detect security incidents.

The large public venue cybersecurity environment is not well defined nor regulated when compared to the healthcare industry. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires healthcare organizations to leverage their resources to establish governance and comply with IT directives (HHS Office of the Secretary Office for Civil Rights).

The motivation for governance and compliance in healthcare is to prevent the release of highly sensitive patient records and prevent physical harm. It safeguards physical and technical safeguards to protect individuals' health information (HHS Office of the Secretary Office for Civil Rights, 2013).

Large public venue operators are more likely motivated to have cybersecurity controls to enable physical security protection, in addition to asset and financial protection. By nature, large public venues have much more extensive public access, with smaller yet critical information systems for venue operations. Venue operations include retail transactions regulated by the Payment Card Industry (PCI) guidelines and financial penalties for non-compliance (Talesh, 2018). However, CIOs and IT managers who treat large public venues as critical infrastructures must access a body of knowledge aimed at counterterrorism, which may bring many advantages to facilities' protection.

The DHS SAFETY Act of 2002 provides legal liability protections for providers of qualified anti-terrorism products and services (SAFETY Act of 2002, n.d.). Companies qualified under the SAFETY Act, such as CNIguard and Northrop Grumman, integrate sensor, SCADA, and communications systems for antiterrorism protection. For stadiums and arenas, the National Football League (NFL) and National Basketball Association (NBA) have qualified under the SAFETY Act with best practices programs (U.S. Department of Homeland Security Science and Technology, n.d.). The NFL uses stadium security, evaluation, compliance, and training to promote high-security compliance during games. The program, however, does not apply directly to NFL clubs, venue owners, or operators. The NBA uses standards, audits, and training to achieve similar goals but adds the hiring, vetting, qualifications, and training of NBA personnel for protection during events (DHS S&T, n.d.).

Cyber-insurance. Experts recommend cyber-insurance for organizations that serve mobile users and work with third-party vendors for services such as accounting and data storage on the Cloud (Selznick & LaMacchia, 2017). Large public venues can serve many mobile users and often host several outsourced services on their infrastructure. Some third-party services include retail, concessions, physical security, and content providers, many of whom depend on Cloud services (Selznick & LaMacchia, 2017). One recommendation is for the large public venue owner or operator to review contracts with third parties to determine how to protect client data and to what extent the parties can play a part in preventing data breaches. The large public venue owner or operator may require vendors to carry cyber insurance if vendor policies and mechanisms are not enough to cover the risk the operator is willing to take.

When an organization invests in cyber insurance, a required step is implementing technical security data controls and developing data security policies (Golden, Tyler, Eucker, & Meyers, 2016). Cyber-insurance may also have to cover the cost of retribution to users for credit monitoring because of data breach incidents. Cyber risk management should align with an enterprise risk management program if it exists, confirm enough budget to cover the assessed risk and response, provide employee awareness training, and develop an incident response plan that is often tested for effectiveness (Golden et al., 2016).

Standards and guidelines. Response planning, analysis, mitigation, and improvements for commercial facilities guidelines can be found in CRR, CSET, PCI, ISO/IEC 27001/2, and COBIT (U.S. Department of Homeland Security Commercial Facilities Sector, 2020). The Cyber Resilience Review (CRR) approach is used to evaluate an organization's operational resilience and cybersecurity practices across ten domains (p. 7). The Cyber Security Evaluation Tool (CSET) guides an organization through the steps to assess their control system and IT network security practices against industry standards (p. 7). In the lodging and retail subsectors, the Payment Card Industry Data Security Standard (PCI-DSS) establishes global standards to prevent fraud prevention using controls that limit data exposure to compromise (Liu & Kuhn, 2010).

The International Standards Organization and International Electrotechnical Commission (ISO/IEC) 27001/2 specifications specify requirements for establishing, implementing, maintaining, and continuous improvement of an organization's management system (p. 8). The retail subsector's Control Objectives for Information and Related Technology (COBIT) is a worldwide framework in which enterprise IT governance enables delivering value (p. 9). The guidance provided by the Commercial Facilities Sector Cybersecurity Framework Implementation Guidance is for voluntary use by Commercial Facilities Sector owners. It stems from the National Institute of Standards and Technology (NIST) publications (U.S. Department of Homeland Security Commercial Facilities Sector, 2020).

Wireless Network Infrastructure

Every year, event attendees make purchases, scan credit cards at point-of-sale terminals, and sign up for mobile apps requiring the input of personal information on personal mobile wireless and Wi-Fi devices (McGuire, 2015). The transactions occur mostly within reach of the venue's wireless network infrastructure during an event, where a customer's mobile wireless or Wi-Fi device accesses Internet-based social media and streaming applications. Attackers can broaden the target beyond individual credit card data, including identity theft and the venue's intellectual property and other sensitive data (McGuire, 2015).

Users' response efficacy has a substantial impact on users' behavioral intentions to use mobile technologies. The implication is that designers of security features on mobile technologies should make devices simple for performing security functions like having a single app for anti-virus, one for anti-malware, one virtual private network (VPN) installed, and one secure Cloud backup installed so that the user can run the software easily (Mitra, 2016). While a large public venue operator may not have the ability to enforce software installation and use on end-user mobile devices, being aware of cybersecurity challenges can help in understanding the role the devices play and guide infrastructure decisions to maintain a strong security posture.

Critical Information Infrastructure

During sporting events, large public venue operators often focus on security for crowd control and the prevention of violent crimes and terrorism, such as surveillance and monitoring (Hassan, 2016). Physical security is a primary motivation for the expedient management of large crowds and emergency response. The Department of Homeland Security has designated commercial sector public venues as critical infrastructures (DHS, 2015). Although the Department of Homeland Security specifically addresses cyber-terrorism, cybersecurity strategies encompass data breach protection. Several of the operating characteristics of venues in the commercial facilities sector can lead to an elevated risk of a data breach (DHS, 2015).

Among the commercial facilities sector of critical infrastructures is a high reliance on information and communications technologies for situational information exchange and direct contact with first responders. At a national level, The United States Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA) combined several emergency broadcast systems into the Integrated Public Alert and Warning System (IPAWS) using a common alerting protocol (U.S. Federal Emergency Management Agency, n.d.). On a county or large public venue level, first responders with smartphones or ruggedized terminals (Qualcomm Technologies, 2018) can use mission-critical push-to-talk (MCPTT) mobile services. Security personnel can use mobile multicast operation on demand (MOOD) to broadcast to all mobile-connected users without requiring authentication. Moreover, local mobile routing enables limited communication if the local cellular core network is compromised (Qualcomm Technologies, 2018).

Critical information infrastructure information and communications technologies are categorized as (a) information system and network protection, (b) fixed telecommunications, (c) mobile telecommunications, (d) radio communications and navigation, and (e) satellite communications and broadcasting (Alcaraz & Zeadally, 2015). Large public venue wireless operators would likely focus on network protection and mobile telecommunications.

Commercial facilities' critical infrastructures consist of commercial centers, office buildings, sports stadiums, and other places that accommodate many people (Alcaraz & Zeadally, 2015). Communication technologies used on critical infrastructures are interdependent because of a dependency on common information and communications systems. The protection of critical commercial infrastructures can then be viewed as a cross-sector activity. An element of the Homeland Security Act of 2002, which created the Department of Homeland Security, states that critical information infrastructures contain information not commonly available in the public domain and are related to the security of critical infrastructures (Homeland Security Act of 2002). Therefore, critical infrastructures such as sports stadiums and commercial centers should provide common means of communication, and the information obtained in the process is protected by law.

The situational awareness of critical infrastructure and networks (SACIN) framework often employs SCADA and sensor networks for intrusion detection (Puuska et al., 2018). Puuska et al. (2018) tested that plug-in intrusion detection offers an advantage in its ability to operate without prior knowledge of the network (i.e., unsupervised). A domain expert who understands when the system is operating normally (Puuska et al., 2018) ideally creates the plug-in. Tecuci et al. (2018) proposed a similar process called a cognitive assistant. Intrusion detection sensors are deployed at strategic and vulnerable locations to enable network packet captures and subsequent analysis.

Wireless Vulnerabilities

Wi-Fi vulnerabilities and mitigation. The Institute for Electrical and Electronics Engineers (IEEE) developed the first standard for the Wireless Local Area Network (WLAN) in 1999, designated as the IEEE 802.11. It is more popularly known as Wi-Fi, as named by the Wireless Ethernet Compatibility Alliance (WECA) in 1999. WECA changed its name to the Wi-Fi Alliance in 2002. The Wi-Fi Alliance works to improve the interoperability, ubiquity, and Wi-Fi value (Wi-Fi Alliance, 2019b). Approximately four billion Wi-Fi devices shipped in 2018, with 13 billion devices estimated to be used (Wi-Fi Alliance, 2019a). Wi-Fi is the predominant wireless communication standard in the world.

Several passive wardriving captures were conducted on public Wi-Fi networks between two highly urbanized cities in Lebanon (Nasr, Jalloul, Bachalaany, & Maalouly, 2019). The researchers scanned approximately 10,000 access points and surveyed 116 Wi-Fi network operators. The research questions were to identify if knowledge of Wi-Fi encryption differed by (a) region, (b) education level, (c) if lack of Wi-Fi security awareness leads to interest in learning about cybersecurity, and (d) if knowledge of the severity of a Wi-Fi attack leads to more concern about data privacy. Nasr et al.'s (2019) findings revealed that (a) knowledge of encryption and interest is independent of location and education level, (b) lack of awareness leads to interest in learning about cybersecurity, and (c) knowledge of Wi-Fi attack severity relates to concerns about data privacy. Evans et al. (2016) also iterated that a lack of awareness led to an interest in learning in a study focusing on the human element in the United States. Similarly, Olmstead and Smith's (2017) findings are the corollaries to the Nasr et al. (2019) study. Lack of awareness of the severity of data breaches is a strong factor for lack of motivation in applying security best practices.

The results of the public Wi-Fi network scans were categorized into the following vulnerability risk assessment categories: (a) network access control, (b) data confidentiality, (c) data integrity, (d) authentication, and (e) data availability (Nasr et al., 2019). Access control measures are circumvented with Media Access Control (MAC) address spoofing or rogue access points. A breach of confidentiality, such as leakage of private information, is accomplished by eavesdropping and man-in-the-middle attacks (Nasr et al., 2019). Data integrity is defeated by data manipulation, such as frame injection. Authentication-related attacks can lead to identity theft and loss of personally identifiable information (PII), accomplished with credential theft. Moreover, the availability of the network and data is impacted by denial-of-service attacks. At the same time, about half of the survey respondents reported a lack of ability to check who is connected to their Wi-Fi network, half reported using strong Wi-Fi Wireless Application Protocol 2 (WPA2) infrastructure security (Nasr et al., 2019).

Wi-Fi security protocols. As of 2018, the four major Wi-Fi security protocols were the IEEE Wired Equivalent Protocol (WEP) and three releases of the Wi-Fi Alliance's Wi-Fi Protected Access (WPA), WPA2, and WPA3 (Kohlios & Hayajneh, 2018). WEP was included with the initial release of the IEEE 802.11 1999 WLAN standard to provide a level of security equivalent to a cable connecting segments of a Local Area Network (LAN). Though WEP achieved its purpose, it is severely limited in providing the security level required in enterprise networks. Zou, Zhu, Wang, and Hanzo (2016) support cryptographic techniques that assume the eavesdropper has limited computing power for making complex mathematical computations (p. 1,729). WEP is easily cracked by observing and capturing the encryption key challenge process partially in plaintext, reusing the initialization vector (IV), and reliance on static and single key management for each network (Zou et al., 2016). Despite some companies' early efforts to improve WEP security for enterprises, it is not recommended for use in any setting.

WPA was introduced in 2003 by the Wi-Fi Alliance to overcome WEP's weaknesses without requiring a hardware upgrade (Kohlios & Hayajneh, 2018; Zou et al., 2016). The encryption method was changed from WEP's RC4 to the Temporal Key Integrity Protocol (TKIP). TKIP dynamically encrypts each packet with a 128-bit key. It differs from WEP in that TKIP does not transmit shared keys over the air. TKIP also added Message Integrity Code (MIC) encrypted keys to prevent spoofing, a strict initialization vector (IV) sequence to prevent replay attacks, improved dynamic key generation, and periodically refreshed keys to prevent key replay attacks (Kohlios & Hayajneh, 2018). WPA has shortcomings in that it uses the RC4 encryption algorithm rather than the Advanced Encryption Standard (AES) Rijndael block cipher. Portions of RC4 key generation can still be replayed. WPA's main vulnerability is TKIP, which is susceptible to hash collisions and limited IV rekeys. An attacker that collects enough hashes within the period of a single IV can break the keys used to encrypt the data in real-time or offline (Kohlios & Hayajneh, 2018). WPA was slated to be disallowed in 2014, but much legacy equipment still relied on TKIP.

WPA2 was released in 2004 and works in conjunction with the IEEE 802.11i standard to provide enhanced security in the Medium Access Control (MAC) data link layer (Kohlios & Hayajneh, 2018). WPA2 introduced Counter Mode with Cipher Block Chaining Message

Authentication Code Protocol (CCMP), which uses AES for data encryption. AES requires upgraded hardware to handle increased processing demands. A four-way-handshake establishes an authenticated session. After a four-way-handshake, a Pairwise Transient Key (PTK) for unicast traffic, a Group Temporal Key (GTK) for broadcast traffic, and a key handshake for GTK renewal are generated to manage the core security processes. CCMP encryption is considered secure because of complexities in key extensions, a combination of permutations and substitutions in each round of encryption, and the number of key rounds based on the key size (Kohlios & Hayajneh, 2018). WPA2's main vulnerability is that it allows the reinitialization of keys. An attacker can exploit the four-way handshake during user authentication to the network, setting the counters to their initial values for message replay and decryption. This method is the KRACK exploit. WPA2 also allows Wi-Fi management frames to be transmitted in plaintext between the client and access points. An attacker can exploit this vulnerability by spoofing packets sent to the client device, for example, to cause it to de-authenticate (Kohlios & Hayajneh, 2018).

WPA3 was released in June 2018. It introduced a password-based Simultaneous Authentication of Equals (SAE) method to authenticate client devices to access points (Kohlios & Hayajneh, 2018). It uses a dragonfly handshake based on discrete logarithmic and elliptic curve cryptography. Elliptical curve cryptography uses large prime numbers for different parameters, such as the password element (PE). PE is used to generate keys. Passwords authenticate the client device to the access point and are used as the seed value for discrete logarithmic computations and hunting-and-pecking techniques (p. 15). SAE forces users to interact with each access point to derive a new Pairwise Master Key (PMK), preventing system replay attacks. Even if an attacker were to crack the password for a client device to access point session, the potential scope of the damage is limited to that access point during that session only.

The Wi-Fi CERTIFIED Enhanced Open program added a layer of encryption to each transmitted message (Kohlios & Hayajneh, 2018). No passwords are required to have a private connection. The IEEE 802.11w standard introduces Protection Management Frames (PMF) to encrypt management frames. WPA3 does not allow a rogue access point to de-authenticate a connected client. However, a connected client can still be lured away by a rogue access point using a stronger signal. By making it more challenging to get onto the network, WPA3 reduces the likelihood of ARP spoofing (Kohlios & Hayajneh, 2018). Without an authentication protocol for ARP requests, an attacker on the network can easily hijack user sessions. There were no improvements in preventing evil twin attacks, SSL stripping, nor DNS spoofing.

Device and Wi-Fi network interactions. An analysis of Android end-user device interactions in a Wi-Fi network revealed several features helpful in developing a model (Ananda, Ujwala, & Kemwal, 2017). The researchers addressed three typical scenarios prevalent in public Wi-Fi networks, MAC address spoofing, sources of information leakage such as apps and Bluetooth, and multicasting for efficient distribution of data such as video. Ananda et al. (2017) built upon network-use signature generation, mobile malware detection, and context-based access controls to develop a model that identifies all users and processes only legitimate inter-component software calls. The premise was that attackers prefer to hide their identity remaining invisible to the network. The findings led to increased network signature-based detection rates and reduced overhead by generating signatures based on network clusters (Ananda et al., 2017). A potential trade-off in a public Wi-Fi network setting is to keep the clusters sufficiently small to maintain detection difficulty and accuracy at a manageable level.

The DHS Cybersecurity Engineering division classifies Wi-Fi enterprise security into several threat types: (a) hidden or rogue access points, (b) misconfigured equipment, (c) banned devices, (d) client mis-association, (e) rogue client devices, (f) connection sharing and bridging client devices, (g) unauthorized association, (h) ad-hoc connections, (i) honeypot or Evil-Twin access points, and (j) Denial of Service (DoS) attacks (DHS, 2017). All threat types also apply to large public venue Wi-Fi networks, though priorities may differ between services offered for public versus private use.

Hidden or rogue access points connect to the enterprise or venue network with a potentially hidden Service Set Identifier (SSID) in an attempt by an attacker to remain invisible to the network (DHS, 2017). Nasr et al. (2019) support the prevalence of unidentified connections, with half of their respondents lacking knowledge of how to check who is connected to their network. Typical threat remediation for finding hidden or rogue access points is to have an active wireless intrusion detection and prevention system (WIDS/WIPS) scanning the wireless and wired network (DHS, 2017). However, once a hidden or rogue access point is found, the process for removal from the network can be labor-intensive. A large public venue operator is likely to be inundated with a high rate of rogue access point alerts since every device connected to their network could technically be identified as a rogue. There may not be enough human resources to track down all the alerts, making detection accuracy more critical.

Though more difficult to identify than hidden or rogue access points, honeypot or evil twin access points can be identified and managed by a WIDS/WIPS (DHS, 2017). Honeypot or evil twin access points do not require a connection to the enterprise or venue network. An attacker attempts to lure users into connecting to illegitimate equipment with a seemingly legitimate SSID to extract passwords and other credentials. End-user cybersecurity training plays an equally important role as a WIDS/WIPS since the attacks are on individuals (DHS, 2017). An individual identified to have network administration privileges may be targeted by an attacker to learn passwords and other credentials.

Rogue client devices and client devices sharing their connections also pose a threat to enterprise or venue networks. A rogue client is a device that is unauthorized to connect to a network but managed to bypass monitoring and security controls (DHS, 2017). A client that shares its connection may or may not be a rogue client but shares its network connection, such as *bridging*. A combination of strong access controls and WIDS/WIPS helps to defeat these types of unwanted connections.

In some cases, Wi-Fi access points and client device operating modes can be interchanged (DHS, 2017). While using access points with robust built-in security mechanisms can defeat attempts to change the access point to client mode, many client device models can be modified to operate in access point mode. Unauthorized associations, such as between two access points, can also bypass network security (DHS, 2017). Therefore, network access controls and WIDS/WIPS should identify and defeat that type of connection attempt.

Wi-Fi configuration and policies. Misconfigured access points can allow unauthorized devices to connect or expose a Wi-Fi network to sniffing and replay attacks (DHS, 2017). Misconfigured Wi-Fi controllers, switches, routers, and other network equipment can allow rogue access points on the Wi-Fi network. Equipment misconfiguration can be avoided with an appropriately sized and trained network management and security staff. However, as indicated in the Cybersecurity Insight Report on digital protection, a shortage of knowledgeable security staffing and insufficient budget is a problem across many industries (CDW, 2018).

Organizational policies should ban devices, such as wireless storage devices (DHS, 2017). IT managers should identify and decide whether to allow on their network devices with weak security, devices using Wi-Fi connection mode, and unauthorized or unnecessary services. Access controls, such as endpoint Wi-Fi security agents, typically enforce policies (Helgeson, Robberstad, Mohan, Eswaran, & Ranganathan, 2018). Wi-Fi ad-hoc uses peer-to-peer mechanisms for security and establishing connections, usually involving individuals sharing a password. Wi-Fi ad-hoc connections bypass enterprise infrastructure mode security mechanisms and should be prevented (DHS, 2017).

Denial of service attacks (DoS) overwhelms networks causing failures or service degradation (DHS, 2017). The attacks often combine other methods, such as honeypots and rogue access points. DoS attacks impact wired and wireless networks, but the wireless medium provides attackers with more opportunities for access. Attackers often use jamming or interference-generating techniques to initiate a DoS attack, followed by network-layer attacks (Abdalzaher et al., 2016). Most physical-layer research has been on eavesdropping attacks but has expanded to include DoS attacks on the physical layer (Zou et al., 2016). Some types of DoS attacks can further exploit weak data encryption methods for eavesdropping (Zou et al., 2016).

Network-layer DoS attacks include modifying routing information, selective packet forwarding, black hole attacks, sinkhole attacks, HELLO packet flood attacks, and others (Yarbrough & Wagner, 2018). A black hole attack is one in which a compromised node refuses to forward any packets. A selective forwarding attack occurs when a node refuses to send particular messages. A sinkhole attack exploits the routing algorithm to increase traffic to a specific node to increase the DoS attack's effects. With learning and patience, an attacker could orchestrate a data breach that begins with a DoS attack. Detecting and defending against DoS attacks is challenging, often requiring significant investments in monitoring, network redundancy, and complexity overhead (Yarbrough & Wagner, 2018).

Wi-Fi calling. Since 2016, all four United States cellular carriers have rolled out Wi-Fi calling services (Xie et al., 2018). By 2020, Wi-Fi calling is expected to surpass Voice over LTE (VoLTE) used by carriers and Voice over Internet Protocol (VoIP) services used in applications by more than double. When the network is unreachable, a security mechanism used by carriers is to drop Wi-Fi calls and switch back the voice call to the carrier network (Xie et al., 2018). Wi-Fi calls should be as secure as carrier-based calls, but there are at least four known vulnerabilities. One is that Wi-Fi calling services do not exclude insecure Wi-Fi networks. A second vulnerability is a lack of defense against ARP spoofing/poison attacks, which can lead to man-in-the-middle attacks. A third is a potential for privacy leakage using side-channel attacks, even when using IPSec for data encryption. The fourth is a lack of service continuity when the Wi-Fi call quality is compromised and switching to cellular does not occur. An attacker can infer user identity, call statistics, device information, personality information, mood, and others from a data privacy breach (Xie et al., 2018). An attacker can also perform DoS attacks such as shutting down devices or denying access to Wi-Fi networks.

Cellular networks. Long Term Evolution Advanced (LTE-A) is the mobile 3rd Generation Partnership Project (3GPP) communication standard. It is a fourth-generation (4G) mobile wireless technology that operators will likely continue using as the costlier and more complex fifth-generation (5G) wireless technologies are set to emerge through 2030 (3GPP, n.d.). The first commercial network to use LTE became operational in 2009. Since then, the standard has evolved. Though the official designation for 4G LTE is LTE-A, it is often referred to as LTE. The 3GPP will modify LTE for 5G, called New Radio (5G-NR), but it will coexist and share the core with 4G.

Changes made by several United States military and commercial agencies, including the Department of Defense (DoD) and Federal Communications Commission (FCC), have created a shared spectrum model in the 3.5GHz Citizens Band Broadcast Radio (CBRS) band for commercial use. As the incumbent, the United States Navy has primary access to the spectrum, as the band remains underused. Spectrum sharing with the commercial sector has been granted with a requisite enforcement function provided by a Spectrum Access System (SAS) (Parvez, Sriyananda, Güvenç, Bennis, & Sarwat, 2016). The decisions made by several of the United States agencies on sharing the CBRS 3.5GHz band released an additional 150MHz of spectrum for the commercial sector (Paolini, 2019). This decision can translate to a potential for 1Gbps network rates indoors and five times or higher rates outdoors when using radio signals within line-of-sight.

LTE will be around in the near future and will likely proliferate into the commercial sector beyond cellular carriers. Private CBRS LTE networks owned by venues may become a popular technical and business model as early as 2020. Neutral host CBRS LTE, where a third-party mobile operator owns the network, may also become attractive for venue operators for a share of revenues paid by cellular carriers and other service providers (Paolini, 2019). The CBRS Alliance, the commercial interoperability group for CBRS, announced in May 2019 that it would support 5G integration (Horwitz, 2019). This commitment puts the CBRS roadmap on par with the carrier-based LTE 3GPP standards roadmap, likely leading to faster adoption.

LTE has vulnerabilities that range from interference-related to others inherent to the standard. Interference-related vulnerabilities are inherent to the wireless medium. While carrier-based LTE systems benefit from a licensed spectrum to avoid spurious signals from other systems close to the licensed band, an attacker with readily available equipment (Mahmud, 2018) can jam signals. Jamming implies an attempt at a denial of service attack. However, it could also be used to cause service disruptions on the network, including resetting a session to reinitiate the authentication process (Abdalzaher et al., 2016; Zhang, Zhu, Chen, & Jiang, 2019). Authentication is an often-used vector to initiate several types of attacks.

Cellular protocol vulnerabilities. Vulnerabilities inherent to the LTE protocol are related to inter-layer communication and access device inter-radio interactions (Raza, Anwar, & Lu, 2017; Shaik, Borgaonkar, Asokan, Niemi, & Seifert, 2015). The vulnerabilities can be categorized as related to authentication, security association, and service availability. When a mobile handset comes out of idle mode, it continuously receives LTE messages from the network without authentication. An attacker can exploit the device by kicking it off the network. A weak security association can occur when a user session moves between radio connections and is assumed by the device to be authenticated by the source network (Shaik et al., 2015). An exploit in which the attacker changes the device's location information can render the device unable to connect to the network, essentially being kicked off. Service availability can be interrupted by exploiting devices' lack of access control and authorization by causing rapid battery drain. Attacks that exploit known protocol vulnerabilities can be performed without jamming (Raza et al., 2017). Although the attacks may not appear to cause substantial damage, the vulnerabilities can be exploited using creative variations of Raza et al.’s (2017) testing.

A man-in-the-middle attack allows the attacker to eavesdrop and modify data, while an impersonation attack allows taking over an LTE session over the air (Haddad, Mahmoud, Taha, & Saroit, 2015). Often, these types of attacks require a session initiation to reset the authentication process, which follows a predictable sequence and occurs before data payload IPSec encryption.

Three attack vectors in LTE OSI data link layer two were identified and tested (Rupprecht, Kohls, Holz, and Pöpper, 2019). The researchers first demonstrated a passive identity-mapping attack, which matches a temporary radio identity and location within a cell to longer-lasting network identities, which can be exploited with follow-up attacks on end-users. An attacker does not need to actively generate interference and conduct the attack passively and stealthily on any LTE network. Secondly, the researchers identified a website fingerprinting attack, which could be a follow-up to an identity-mapping attack. There is enough unencrypted resource-allocation side-channel meta-data to reveal the identity and websites even with encrypted data. Thirdly, an active attack called ALTER involves manipulating uplink packets by exploiting a weakness in integrity protection during encryption (Rupprecht et al., 2019). An attacker who installs an LTE relay may redirect user traffic to malicious servers for further exploitation. The ALTER attack vector is a vulnerability inherent to the LTE standard, requiring a change to the standard to eliminate the vulnerability (Rupprecht et al., 2019).

Findings from tests conducted on operational LTE networks uncovered 51 vulnerabilities principally caused by improper treatment of unprotected initialization processes, modified network requests in plain text, lack of message integrity protection, message replay, and bypassing security processes (Kim, Lee, Lee, & Kim, 2019). The researchers built on Raza et al.'s (2017) work and previous work done by Rupprecht et al. (2019) by systematically crafting messages to test each security property, including injecting every message available for each function. Kim et al. (2019) demonstrated a denial of service to users, impersonate control plane messages for privacy leakage, send modified Short Message Service (SMS) messages, and eavesdrop and modify data communication.

The test methodology stemmed from security properties related to specifications, generating test cases to violate the security properties, and classifying resulting vulnerabilities (Kim et al., 2019). The researchers used malicious input into active networks and conducted comparative analyses of the resulting vulnerabilities in commercial logs. In addition to verifying vulnerabilities subject to man-in-the-middle and denial of service attacks, the findings identified different vulnerabilities between two cells on the same carrier network and different vulnerabilities between carriers using the same equipment (Kim et al., 2019). An implication is that neither device vendors nor carriers check their network security in detail.

Large Attack Surface and High Density

Wireless networks are vulnerable to eavesdropping and impersonation attacks (Shivaramu et al., 2016). The risk increases with many nodes over a large area. In some instances, an environment with high node density resembles signal jamming, which an attacker can exploit to reset and hijack user sessions (Bottarelli et al., 2018). When a user session is reset, conventional symmetric encryption key generation methods create the secret keys for a new session using random numbers. Bottarelli et al. (2018), Hu, Zhang, Mitrokotsa, and Hancke (2018), and other researchers viewed the vulnerabilities in a wireless medium as opportunities for generating encryption keys based on generating random values from parameters characteristic of the wireless medium.

In a report about online trust over the next decade, the attack surface is growing faster than the ability to protect it (Rainie & Anderson, 2017). In another report by Booz Allen, new technologies such as IoT for building automation, safety, security, and industrial control functions pave the way for attackers to discover new means to expand further the attack surface (Booz Allen, 2019). Yarbrough and Wagner (2018) added that an attacker's ability to communicate with a node or connect an unmonitored node physically increases the attack surface wirelessly in wireless sensor networks. Similarly, mobile-connected autonomous vehicles face increased exploitable risk vulnerabilities with increased attack surfaces (Sheehan, Murphy, Mullins, & Ryan, 2018). Xie et al. (2018) researched real-world Telephony Harassment/Denial of Voice Service (THDoS) attacks that can significantly impact Wi-Fi calling in a university campus setting, like large attack surfaces in large public venues. Hong et al. (2018) saw that emerging network technologies caused continuously changing attack surfaces and developed moving target defense security metrics. Large attack surfaces are associated with increased risk vulnerabilities and exploits.

Cellular carriers offload congested traffic in areas with a high density of users (Hagos, 2016). Wireless networks offer open access, where legitimate users and eavesdroppers can receive signals equally. There are security and privacy concerns with dense networks, with characteristic dynamic network topologies, complex network components, high mobile device diversity, and mobile devices with resource constraints (Hagos, 2016). Several others within proximity might fall to the same attack if one network node or base station were compromised. In dense networks, base stations and access points are mounted close to each other and may cause interference. However, interference between nodes operating in nearby frequencies is unavoidable and additive (Kim, Kim, Lee, Griffith, & Golmie, 2017). Mobile macro-cell signals, unlicensed Wi-Fi signals, and user connections can generate sufficient interference to the node to disrupt services or become vulnerable to attacks. For example, in a dense Wi-Fi network, collisions introduced by hidden nodes are the primary source of frame errors (Zhang & Xiao, 2017).

Staffing

If an IT staff is undersized, employees may become overwhelmed and may not have the ability to perform necessary IT functions such as testing network resiliency and applying necessary cybersecurity controls such as applying patches and infrastructure vulnerability testing (Carmichael, 2015). Kraemer-Mbula, Tang, and Rush (2013) acknowledged that small businesses might be particularly vulnerable to cybercrime due to a lack of understanding of the operation of IT systems. Astani and Ready's (2016) study on data breaches to develop recommendations to mitigate security deficiencies in organizations highlighted an increasing desire for IT executives to quadruple their organizations' staff size. In another study, about 46% of 133 digital preservation respondents from several industries reported being understaffed and would ideally double the number of employees dedicated to digital preservation (Atkins et al., 2020). Eighty-seven percent of the respondents in Frenel's (2016) published survey reported concerns with employee errors or process failures, highlighting management concerns.

When applying critical infrastructure protection, the DHS control systems report categorizes security controls as organizational security sub-controls and operational sub-controls (Alcaraz & Zeadally, 2015). Organizational physical and cybersecurity controls include "security policy, organizational security, personnel security, physical and environmental security, strategic planning, security awareness and training, monitoring and reviewing" security policies, risk management, and assessment, as well as security program management (Alcaraz & Zeadally, 2015, pp. 59-60). Operational sub-controls add responsibilities for performing activities securely. Some of the controls include configuration management, information and document management, system and communications protection, incident management and response, access control, and audit and accountability (p. 60).

Standards related to information and SCADA systems, such as NIST 800-53 and NISTIR 7628, as well as IEC 62351, WirelessHART and ISA100.11a for smart grids, can be consolidated for infrastructure protection (Alcaraz & Zeadally, 2015). For traditional information system standards, practitioners can leverage ISA 99-1 and 99-2, ISO 17799, ISO 27001 and 27002, ISO 19791, and others. Several other standards for business alignment and physical protection exist. Critical infrastructure protection can consume many human resources and require appropriately sized staff to provide holistic protection, including protection against data breaches.

The DHS cybersecurity implementation guide for critical infrastructure commercial facilities recommends a risk-based approach to enable an organization to gauge resource estimates for staffing and funding (DHS, 2015). Foster (2015) supports a risk-management-driven approach to defining human resource requirements, specifically in passive unrealized risk acceptance. Appropriate staffing should include no more than a targeted 80% usage for primary cybersecurity duties, leaving 20% of the time to review information, troubleshoot problems, and look for process improvements (Foster, 2015).

Having a dedicated and well-trained staff is an essential factor in preventing data breaches and cybersecurity in general. Evans et al. (2016) found in their survey, 72% of the companies where the security policy was poorly understood had insider-related breaches. The researchers also believed part of the cause was a low ratio of employees to dedicated security staff. The DHS identifies security awareness and training of dedicated staff as one of the principal elements of organizational security sub-processes. It is portrayed as a security control in most of the seven NIST, IOS, and ISA organizational and operational standards mentioned

(Alcaraz & Zeadally, 2015). In the DHS (2015) sector-specific plan, the framework identifies awareness and training as part of prioritized funding and workforce development.

Large Public Venues

A study involving 66 semi-structured interviews with local stakeholders in 12 cities across Canada was conducted to understand their views on the use of arenas (Mason et al., 2018). Many interviewees saw opportunities and benefits in leveraging the facility beyond the anchor tenant or team. Critical to realizing the benefits is the ability of an arena to service the city. The resulting partnership fostered multiple uses, such as recreation, concerts, convention business, and regional and national amateur competitions. The city and the arena often pool resources, such as community volunteers and venue staff, to reconfigure the facility infrastructure and run the events. A relevant finding is that large public venues such as arenas may not survive without multiple purpose use (Mason et al., 2018).

Multiple purposes and even multiple tenant use of large public venues may require equipment reconfiguration to customize for events. Convention centers often add a custom Wi-Fi network (SSID) for event attendees. However, changes in system configuration and the introduction of new applications may reduce protection or create new vulnerabilities because of management (National Science and Technology Council Office of the President, 2016).

Stadiums are often near dining facilities, entertainment venues, and shopping areas (Jenkins & Evans, 2018). Wireless communication signals from the venue are often within reach of these facilities and can increase the venue's risk. With a large footprint, an attacker can hide in the environment, perform network data captures, and launch attacks during and after the event (Braun et al., 2018).

In addition to multiple purposes and multiple tenancies, sporting events bring together multiple vendor applications. Online and onsite ticket sales can expose fans to phishing scams, where before the 2008 Summer Olympics, fake sites stole personal and banking information from spectators (Jenkins & Evans, 2018). Fans accessing applications via public Wi-Fi networks are subject to man-in-the-middle attacks. Devices accessing Wi-Fi networks can also have applications that use Bluetooth and Near Field Communications (NFC) channels for location services or purchases, rendering them vulnerable to attacks (Jenkins & Evans, 2018). Some applications do not even sense an active Internet connection, leading to missed purchases for merchandisers operating on the venue's wireless network (Jenkins & Evans, 2018).

Widespread technology use in sports stadiums includes services for sporting events and athletes. During events, teams validate referee calls, record athletes' detailed performance statistics, provide medical care, and others (Greenwald, 2017). Device and storage security for collected data is essential for monitoring data breaches. Several best practices resulted from the 2014 World Anti-Doping Agency on Olympic athletes and the 2013 Houston Astros database hack (Greenwald, 2017). One is to perform routine security audits of all information systems. Another is to raise awareness and train the athletes and staff to use good security practices. Hire a dedicated security professional who would be more vigilant at protecting cyber and physical assets than, for example, a software engineer with no knowledge about security.

Greenwald (2017) further proposed measures to protect data and data privacy. Data should be taken offline when not in use, including wireless networks, Bluetooth devices, IoT, and wearable computers. Even if anonymized, data should not be sold; it can be reconstructed and correlated with often publicly available information (Greenwald, 2017). Another best practice is for venue operators to participate in communities that advocate protection for athletes, venue staff, sports infrastructures, and attendees to contribute to standardization efforts and share best practices. The Department of Homeland Security has critical infrastructure programs that advocate dedicated security professionals and provide standardized methods to protect stadiums (DHS, 2015).

Non-cyber-related systems could disrupt large public venue site operations systems. An electrical power failure at the 2013 Super Bowl in New Orleans was traced to a faulty electrical relay (Jenkins & Evans, 2018). The results of an analysis of the event highlight a need to embed cybersecurity countermeasures holistically into electrical power and other systems. A power failure, or a compromised operational system, can lead to confusion and panic and cause physical harm to many fans. Stadium utilities and surrounding areas should be protected from hackers.

Types of Large Public Venues

Large public venues are typically associated with stadiums, arenas, government buildings, large hospitals, and large hotels. One definition provided by the Tampa Sports Authority for a bid for staffing services at Raymond James Stadium is "a continuous building or campus of 250,000 square feet or more," a large hospital with 350 or more beds, and a large hotel with 100 or more rooms (Jones, 2019, p. 21). Brown (2016), in addition to stadiums and arenas, includes airports as public venues.

The Department of Homeland Security identifies locations in the public assembly subsector as arenas, stadiums, aquariums, zoos, museums, and convention centers (DHS, 2015). Large public venues consist of several of eight subsectors under The Commercial Facilities Sector as identified by DHS (2015):

- Entertainment and media (e.g., motion picture studios, broadcast media).
- Gaming (e.g., casinos).

- Lodging (e.g., hotels, motels, conference centers).
- Outdoor events (e.g., theme and amusement parks, fairs, campgrounds, parades).
- Public assembly (e.g., arenas, stadiums, aquariums, zoos, museums, convention centers).
- Real estate (e.g., office and apartment buildings, condominiums, mixed use facilities, self-storage).
- Retail (e.g., retail centers and districts, shopping malls).
- Sports leagues (e.g., professional sports leagues and federations). (para. 2)

Strategy Development

Moving Target Defense (MTD) has been applied to emerging network technologies, such as Cloud computing and Software-Defined Networking (SDN) (Hong et al., 2018). Networks are shifting from static hardware-based networks to dynamic software-driven networks (p. 33). The researchers use the graphical Temporal-Hierarchical Attack Representation Model (T-HARM) security model for developing dynamic security metrics, measuring the MTD effectiveness in a continuously changing attack surface to thwart cyber-attacks. Applying T-HARM first requires categorization of the attack and defense efforts within operational constraints. The next step is to incorporate and capture MTD techniques based on characteristics. Afterward, develop a new set of security metrics to measure effectiveness. The security characteristics of the network configuration are used to evaluate attack efforts.

Similarly, defense efforts are categorized based on attacks. The T-HARM is used in experiments to assess the MTD techniques' effectiveness by capturing changes in the network as network states (Hong et al., 2018). While some metrics, such as system risk, cannot be normalized, the metrics are customizable to user requirements by assigning weights to the factors.

In a review of information security, cybersecurity, and data breach events, researchers applied the planned behavior theory (PBT), deterrence theory (DT), and protection motivation theory (PMT) to help understand the gaps in developing a secure system (Loukaka & Rahman, 2017). The researchers found that the security posture can be improved by addressing IDS issues to improve proactive predictions on emerging attacks, using machine learning to build responses to specific exploits, and decreasing detection times. As a part of strategy development, the cybersecurity practitioner needs to understand the organizational goals, policies, applicable theories, and the security artifacts used in an organization.

In the NIST publication on improving critical infrastructure cybersecurity, the framework proposed provides a common organizing structure for multiple cybersecurity approaches by assembling standards, guidelines, and practices effectively (Barrett, 2018). The NIST framework is effective because it is technology-neutral and simultaneously addresses multiple standards, guidelines, and practices developed, managed, and updated by practitioners in the industry. The tools and methods used to apply the framework scale across the industry evolve with technological advances and business goals. Organizations applying the framework will address a unique set of risks based on different types of threats, vulnerabilities specific to their environment, and risk tolerances. Every organization identifies its activities that are important to service delivery and prioritizes its investments to maximize value. Examining the investments' effectiveness requires understanding organizational objectives, relationships between the objectives and cybersecurity outcomes, and implementing those outcomes (Barrett, 2018). Therefore, strategy development can be accomplished by applying known effective frameworks.

Synthesis of the Research Findings

The researcher identifies three common themes from the literature on effective strategies for protecting large public venues against data breaches. First, wireless networks are mainly vulnerable to man-in-the-middle and evil-twin attacks. Second, large public venue wireless networks can be complex and play a part in a broader operational complex ecosystem. Third, given several available standards and frameworks to help organizations apply cybersecurity strategies, much reliance is placed on intrusion detection. Consequently, an abundant amount of research focuses on improving intrusion detection accuracy within device performance constraints.

Vijayanand et al. (2018) worked on detection techniques for man-in-the-middle and evil-twin attacks in wireless mesh networks. Man-in-the-middle, evil twin, and honeypot attacks are closely related in that all methods deceive the device or the user into connecting to an illegitimate network. Nasr et al.’s (2019) analysis of public Wi-Fi networks identified several man-in-the-middle and potential evil twin attacks, which is a close copy of a legitimate network identifier (SSID). Xie et al.'s (2018) study on Wi-Fi calling over carrier networks found vulnerabilities leading to man-in-the-middle attacks and authentication exploits. Haddad et al. (2015) found that man-in-the-middle attacks on LTE networks could be used to take over a user session after resetting the connection with a jamming attack. Kim et al. (2019), Raza et al. (2017), and Rupprecht et al. (2019) built and tested an LTE vulnerability database, also finding the vulnerability to man-in-the-middle attacks is inherent to the 3GPP standard, and in many cases, attributable implementation practices. Jenkins and Evans’ (2018) study on stadium cybersecurity adds several instances where man-in-the-middle attacks were at the core of the exploits.

Large public venues can contain several interconnected systems, making them complex systems. A large public venue wireless network can also be a complex system for its propensity for high user density during events, multiple-purpose, and multiple-tenant use, and use of multiple applications for multiple vendors. Mason et al. (2018) established that many stadiums and arenas depend on public-private partnerships with multiple-purpose use for survival. In the National Science and Technology Council Office of the President (2016), references to multiple-purpose and multiple-tenancy use of public venues highlight changes to the network configuration that can render it vulnerable to attacks. Jenkins and Evans (2018) and Greenwald (2017) argued that staff and multiple-vendor application uses in stadiums, adding that hiring cybersecurity professionals and managing multiple-technology devices are acceptable practices for the environment. DHS and NIST frameworks contain guidance on strengthening the security and cybersecurity posture in public venues with multiple-purpose and multiple-application use.

In DHS (2017), guidance for securing Wi-Fi networks offers WIDS/WIPS as a necessary component to secure wireless LANs. In the NIST Cybersecurity Framework, detection is one of the five principal categories (Barrett, 2018). The framework references COBIT 5, ISA 62443-2-1, ISO/IEC 27001, NIST SP 800-53 Rev. 4, and CIS CSC for requirements, implementation, management, and continuous improvement. Even though government publications seem to reference WIDS/WIPS, commercial entities such as COBIT, CIS CSC, and ISO/IEC provide similar guidance.

Data breaches often result from viruses, malware, distributed denial of service attacks, and others (Borum et al., 2015). The researchers suggested using strategic intelligence to understand the cybersecurity environment and develop appropriate countermeasures. Evans et al.'s (2016) research supports the notion of a more holistic organizational approach than technical elements. Borhade and Kahate (2016) added that intrusion detection techniques that apply to many types of attacks are related to authentication, connect-back, connect availability use, and backdoors. Bamakan et al. (2015) elaborate on intrusion detection system design and offer particle swarm optimization techniques.

Much of the research on intrusion detection focuses on accuracy and optimization. Mazini et al. (2018) proposed a hybrid computer network topology design and anomaly-based selection to improve access to large heterogeneous and unbalanced data sets used in intrusion detection. Setiawan et al.'s (2017) literature review found that classification performance is improved by pre-processing data with an unsupervised k-means type clustering technique, then feeding the results into a supervised classifier. Carrasco & Sicilia (2018) focused on misuse detection algorithms to compare the actions expected of an attacker with a baseline.

Jabez and Muthukumar (2015) and Sajjad et al. (2015) improved machine learning and clustering techniques to further advance intrusion detection precision and stability. Jabbar and Aluvalu (2017) aggregated random forest techniques, while Saeed et al. (2016) used random neural network techniques to reduce processing requirements and maintain accuracy. Hidayanto et al. (2017), Landauer et al. (2018), and Veeramachaneni et al. (2016) applied machine-learning techniques to intrusion detection log files to improve detection rates, efficiency, and accuracy.

Tecuci et al. (2018) introduced automated cognitive assistants who learn from expert analysts how to investigate intrusions. Álvarez Cid-Fuentes et al. (2018), Shenfield et al. (2018), and Vijayanand et al. (2018) applied genetic and neural algorithms to wireless and wired networks to improve detection accuracy and efficiency. Wahl (2016) and Zulkefli et al. (2017) found that using multiple intrusion detection approaches and layers of hardware and software leverage the strengths of each and improve intrusion protection.

Critique of the Previous Research Methods

Data breach research varies from case studies to correlation studies. Much can be learned from data breach events, such as Perri and Perri’s (2018) pedagogical design for business students to be prepared for inevitable data breaches. Case studies are appropriate to understand the sequence of events and reactions as the events unfolded. Quantitative studies based on survey designs reveal knowledge and behaviors, as Olmstead and Smith's (2017) study on knowledge of significant data breaches. Similarly, correlational studies outline trends and validate predictive models, as in Edwards et al.’s (2016) predictions using Bayesian GBLMs to predict the next largest breach. Quantitative studies are appropriate for surveys and comparing repeating variables from, for instance, one year to another.

Much research on intrusion prevention and detection involves simulations, machine learning training, and validation with a known data set. IDS/IPS systems can be complex and should be modeled to understand and test improvements. Bamakan et al.'s (2015) study used particle swarm optimization to improve performance. Mazini et al. (2018) used statistical methods to refine an algorithm and then verified performance with several data sets. Simulations are appropriate since a controlled environment enables reproducible results. Similarly, discovering vulnerabilities in wireless systems is appropriately conducted in a simulated environment. However, Kim et al. (2019) tested in a live environment, revealing results not likely obtainable in a laboratory setting.

Taxonomies can be useful for the data analysis of this study. Several authors developed categories for research that encompass data breaches. Gerard (2016) described a Price Waterhouse Coopers report with data breaches commonly categorized into financial, healthcare, retail, education, and public sectors. Large public venues may not fit discretely into any of the categories but can appear under retail and partially under the public sector. Alcaraz and Zeadally (2015) described categories for critical information infrastructure information and communications technologies as an information system and network protection, fixed telecommunications, mobile telecommunications, radio communications and navigation, and satellite communications and broadcasting. Large public venues may fit into all the critical infrastructure categories, except perhaps satellite communications. Descriptions and categories related to large public venues are more accurately addressed in the DHS context of commercial sector critical infrastructure.

Nasr et al. (2019) describe vulnerability risk assessment categories of network access control, data confidentiality, data integrity, authentication, and data availability, in the context of Wi-Fi networks. Similarly, Raza et al. (2017), Shaik et al. (2015) categorize cellular network vulnerabilities as authentication, security association, and service availability. Also, researchers such as Hong et al. (2018), who develop models for data breach prevention or detection, first categorize attacks and defensive efforts. Categories derived from prior research can apply not only to the decomposition of the empirical data from this study but to synthesize the results and conclusions reproducibly.

Summary

Large public venues are likely to be used for multiple purposes by multiple tenants, for multiple applications, and multiple technologies. Data breaches continue to grow in incidence and frequency, with the potential for multiple occurrences before discovery (Mitra, 2016; Nazareth & Choi, 2015; Schatz & Bashroush, 2016). Large public venue wireless network operators who offer public access through their network infrastructure are vulnerable to many types of attacks. Any one of the attacks can lead to a data breach of corporate data, vendor data, or guest data, leaving the operator open to a data breach on a broad scale. Not only is there a risk of when the venue will have a data breach, but it is a matter of when and to which extent.

A data breach can hurt the venue operator in lost information, vendor reputation, and the entire market (Gerard, 2016). Newer wireless network technologies, such as private LTE, offer greater security and quality of service. However, LTE has vulnerabilities inherent to the standard and implementation practices (Raza et al., 2017; Shaik et al., 2015). Factors like having a dense environment, proximity to other wireless networks and facilities, and lack of control over guest handsets further increase the risk of a data breach (Hagos, 2016; Kim et al., 2017). Much research on intrusion protection and detection involve developing machine learning and cognitive assistance techniques, with improvements in false positives and false negatives (Loukaka & Rahman, 2017; Shenfield et al., 2018; Veeramachaneni et al., 2016; Zulkefli et al., 2017). Given that there has also been much research on counterterrorism on critical infrastructures, there are effective standards and guidelines for physical and cybersecurity protection.

No known studies consider a large public venue wireless network infrastructure security posture in a highly dense and complex environment. Organizations like the NFL, NBA, and NHL have established guidelines for securing Wi-Fi networks (DHS S&T, n.d.). However, the sports leagues do not appear to account for emerging wireless technologies and a systematic approach that accounts for the entire organization and provides holistic protection. By obtaining knowledge on effective strategies for large public venue wireless infrastructures, the researcher can make information available to inform CIOs and cybersecurity managers in the venue community on how to avoid a data breach and how to prepare for the inevitable event better.

Whether large or small, public venue operators can learn how to avoid costly and potentially embarrassing data breaches.

This qualitative, exploratory, multiple case study uncovered effective strategies to reduce the risk of cybersecurity data breaches of large public venue events wireless IT network infrastructures. To uncover the strategies, the researcher conducted seven cases of personal interviews with cybersecurity managers who typically work under a CIO's direction and decide on information security and wireless infrastructure protection in their large public venues. The themes obtained from the cases were triangulated with the extant literature, publicly available information on the Internet, and researcher notes. Using multiple cases enabled the researcher to capture from a cross-section of venue participants to reinforce similarities, explore, and contextualize the differences.

CHAPTER 3. METHODOLOGY

In Chapter 3, the researcher provides details for the methodology to conduct the study. The first part of the chapter includes the study's purpose and the research question foundational to the study. The next section includes a review of the research design and methodology, followed by a description of the target population and the sampling approach. Next is a discussion on the setting and analysis of the research question. Following is a discussion on case study credibility and dependability, as well as ethical considerations. The chapter concludes with a discussion of data collection and analysis.

Purpose of the Study

The purpose of this qualitative, exploratory, multiple case study was to uncover effective strategies to reduce the risk of cybersecurity data breaches of wireless IT network infrastructures at large public-event venues. The research was designed to understand common factors large public venues use to develop and determine the efficacy of strategies. The research was specifically designed to allow the researcher to identify the decision-making process chief information officers (CIOs) and cybersecurity managers use in formulating effective strategies. Cybersecurity decisions require an understanding of security threats and the ability to anticipate vulnerabilities (Barrett, 2018). The study's target population included a cross-section of IT managers and other persons responsible for cybersecurity. They typically work under a CIO's direction that operates a wireless network and identifies their organization as a *large public venue*. The sample population was appropriate, as researchers have found that owners, operators, or cybersecurity managers of similar size businesses lack the processes to control emerging cybersecurity risks and threats, which characterize the use of technologies (Njenga & Jordaan, 2016). Moreover, the information detailed by IT managers and others responsible for cybersecurity reflects on the decisions, training, and policies implemented by CIOs and cybersecurity managers.

A secondary purpose was to add to the body of knowledge in IT network security to reduce the effects of the long-standing data breach problem. Data breaches continue to increase in frequency as attackers adopt new tactics and circumvent preventative measures (Edwards et al., 2016). CIOs and cybersecurity managers who operate large public venues will have the opportunity to be more informed about the likelihood their venues might suffer a data breach and to help them to strengthen the cybersecurity posture of their IT organizations.

Research Question

The research question that guides the study is: What are effective strategies large public venue operators use to reduce the risk of data breaches in their wireless networks during and between venue events?

Research Design

The researcher did not select a quantitative research method because the focus would be to describe, explain, and predict outcomes using a quantifiable probabilistic sampling design. Quantitative research is often used to precisely measure behavior knowledge, opinions, or attitudes, as well as theory testing (Cooper & Schindler, 2014). The constructivist epistemological perspective for the study was appropriate as *meaning* was created from participants' unique experiences and multiple views (McCusker & Gunaydin, 2015). Qualitative research is designed to tell the researcher how and why a phenomenon occurs, as the research focus is to understand and interpret participant experiences (Cooper & Schindler, 2014).

Qualitative research methods include phenomenological, grounded theory, Delphi study, ethnographic, or case study. A phenomenological method focuses on understanding a problem by understanding a person’s perceptions and perspectives related to an event that is not external to the person (Burns et al., 2018; Leedy & Ormrod, 2014). A phenomenological method was not appropriate because the study focused on understanding participants’ perceptions and perspectives externally, including documentation and artifact review and observations to triangulate the research. A grounded theory typically focuses on a related process, including people’s actions and interactions, to develop a new theory about the process (Leedy & Ormrod, 2014). A grounded theory method was not appropriate because the study's goal was not to develop a theory about a process. This study’s focus was to identify effective strategies in which processes may influence strategy selection. A Delphi study is used to develop new theories based on experts' consensus in the field, given that experts can be found, and the problem can be solved based on subjective conclusions (Simon & Francis, 2004). It was expected to be difficult to find cybersecurity experts who also operate wireless networks in large public venues. An ethnographic study focuses on an entire group that shares a common culture (Leedy & Ormrod, 2014). It was not an appropriate research method because the study did not require an understanding of participants' cultural behaviors.

Case study research “investigates a contemporary phenomenon (the ‘case’) within its real-world context, especially when the boundaries between phenomenon and context may not be clearly evident” (Yin, 2017, p. 15). According to the university, case study research focuses on a program, event, activity, or process of one or more individuals. The case is the object of study, which is a complex functioning unit. The researcher selected a qualitative case study design for the study because it provides the means to investigate data breach prevention strategies in large public venues, using multiple analysis levels in a real-world context.

A research design should be described with enough depth so other researchers can replicate the study. Case study research designs usually address *how* or *why* research questions (Yin, 2017). In a case study, propositions help to focus on what should be examined within the study (Yin, 2017). The researcher examined IT-related decision-making, processes, process interactions, planning, and technological applications in this study, as viewed through the theoretical lens. Yin (2017) identified that an exploratory case study uses the theoretical lens to focus the research instead of using propositions. Each case study research is defined and bounded from the research question, followed by clarifications (Yin, 2017). In this case study, each was defined by a large public venue that operates a wireless network specifically during hosted events. The phenomenon under study was a data breach to understand the strategies used to prevent its occurrence. A holistic case study design uses a single unit of analysis, as each organization is examined in its entirety (Yin, 2017). Theoretical lenses were used in this study to focus on the processes and activities related to data breach prevention strategies within IT organizations holistically.

Using a multiple case study design informed the research with a cross-section of venue participants, reinforcing contextual similarities and exploring differences. Using this type of research design should help achieve an in-depth understanding of themes for effective strategies from the collected data. The emphasis on detail in a case study provides the researcher with valuable insight for problem-solving, evaluation, and strategy (Cooper & Schindler, 2014). Data collection and subsequent triangulation analysis entailed interviewing IT managers responsible for cybersecurity with open-ended and semi-structured questions, the extant literature, publicly available online information, and researcher notes.

There were time constraints based on the program of study and the availability of funds. The university defines acceptable research designs for dissertations based on the feasibility of time, access to resources, and available mentoring expertise. Among the acceptable designs is case study research, which can be completed within the allotted time of the program of study. The researcher considered the time and resources required to conduct the study, anticipating participant selection and interviews would take the longest to complete. The research study took three months to recruit and interview seven participants.

Target Population and Sample

Population

The target population was cybersecurity managers who typically work under a CIO's direction and decide on information security in large public venues that operate a shared wireless network in the United States. It included property owners who outsource shared wireless networks. It also included event or venue personnel who possessed cybersecurity knowledge of a venue with a shared wireless network. Excluded were locations such as parks that host temporary events.

Participants were selected from large public venues that operate wireless network infrastructures in the United States. In-depth knowledge obtained may offer insight to identify effective strategies, development and implementation methods, and prioritization. The details on the historical and social factors the researcher records about the context surrounding the cases help future researchers conclude the generalizability of the study to other situations (Cooper & Schindler, 2014). Even if the findings in this multiple case study may not be generalizable across industries, the results established a framework across different types of large public venues, such as sports stadiums, amusement parks, convention centers, or even smart cities with similar operating requirements and challenges.

The researcher expected large public venue IT departments to be similar in size to a small business. Small businesses are often defined by the number of employees and annual sales, such as up to 500 or fewer full-time employees and up to $10 million in annual sales (Cole & Mehran, 2018). In this study, small businesses were perceived to be based on departmental size and characteristics primarily. A criterion for participant selection was self-identification with their organization as a *large public venue*. A second criterion was to have a shared wireless network in the venue. A third criterion was to include IT managers and persons responsible for cybersecurity who typically work under the direction of a CIO or other designated persons responsible for and experienced in cybersecurity.

Sample

The researcher sought convergent evidence regarding the findings and conclusions, as suggested by Yin (2017). An objective of the study was to replicate the information from each case’s conclusions across the other cases. The number of cases depends on the researcher's certainty about the multiple-case results (Yin, 2017, p. 59). Two or three case studies might have been enough if similar results could be theoretically predicted without requiring a high degree of certainty. If the theory is not as obvious, and a high degree of certainty is required, the researcher should target five or more cases (Yin, 2017). Similar results were anticipated from the different case studies, except for instances where large public venues adhered to critical infrastructure guidelines contrasted with venues that did not adhere to those guidelines. The researcher regarded the theory as not obvious and required a high degree of certainty to predict the results theoretically. Based on Yin’s guidance and an understanding of theoretical predictions from the study, an estimate of five or more cases was required to achieve theoretical replications and data saturation.

In similar multiple case studies, researchers have examined cases ranging from three to fifteen. Saber (2016) received five responses for an online open-ended questionnaire, followed by three business leaders' subset samples to answer semistructured in-person interviews. Burton-Howard (2018) also used an online questionnaire with open-ended questions, followed by in-depth semistructured interviews on 10 participants with at least ten years working in cybersecurity. Nero (2018) examined 15 cases using semistructured interviews to reach data saturation. Patterson (2017) used a purposive sample of 10 business owners with open-ended questions to ensure data saturation. According to Cooper and Schindler (2014), a minimum of four cases with a maximum of 15 seems to be favored (p. 166). Given the range of cases used in other studies, the researcher initially chose to target nine cases while reviewing ongoing findings for data saturation. Data saturation was achieved with seven cases, at which point there was no need to seek more participants for the study.

Procedures

The following section describes the steps on how the research methods for this study were applied. First, the procedures used for participant selection and protection of participants are described. The following sections describe the procedures for data collection, data analysis, and presentation of the findings.

Participant Selection

Purposive sampling was used to select participants for the study. Purposive sampling selects samples based on knowledge, such as characteristics of interest, of the population being sampled (Edgar & Manz, 2017). The sampling frame initially consisted of members of LinkedIn groups that use wireless networks in their venues. The researcher read profile pages of individuals and their companies' descriptions to compare with the study's qualification criteria. Snowball sampling was also used when engaging with prospective participants. Snowball sampling can be useful when selecting from a population that is difficult to find without an existing sampling frame (Christensen, Johnson, & Turner, 2014). Snowball sampling was used in combination with the LinkedIn sampling frame to increase the probability of finding nine or more qualifying cases. Neither LinkedIn groups nor snowball sampling yielded any participants for the study.

As an alternative to LinkedIn as the sampling frame, the researcher requested research recruitment services from Focus Insite. Focus Insite was an established and well-known market and IT research company that provided several tiers of research services. Focus Insite developed a screening guide based on the research study's qualification screening questions to recruit and screen participants.

Protection of Participants

This study involved the participation of human subjects. The researcher followed the university's Institutional Review Board (IRB) guidelines to ensure the protection of the privacy and confidentiality of participants of the study and to apply a consistent ethical standard that complies with federal laws and maintains the integrity of the methodology of the study and the reputation of the university. Ethical considerations included respecting participants' autonomy and dignity, minimizing risks to participants, providing adequate information to allow participants to make an informed decision when deciding to participate in the study, and guarantee their anonymity. All personally identifiable information will remain confidential for seven years before being destroyed.

Data Collection

Data collection for the research was composed of semistructured interviews with cybersecurity managers who typically work under a CIO's direction and decide on information security and wireless infrastructure protection in their large public venues. The interview questions for this study are contained and described in the instruments section in this chapter. The interview is the primary data collection technique for collecting qualitative methodologies (Cooper & Schindler, 2014, p. 169). Case study interviews resemble guided conversations (Yin, 2017). Although the line of inquiry should be consistent, the actual questions should be adaptive to ask clarifying questions as needed (Yin, 2017). The researcher has two roles in a case study interview: (a) following the line of inquiry according to the research protocol and (b) verbalizing the questions in an unbiased manner (Yin, 2017). The researcher was also the instrument for data collection, which involved putting participants at ease and comfortable to directly capture their perceptions and attitudes about events and behaviors during the interview (Baškarada, 2015).

For this case study, the researcher put together a series of questions based on similar research. Permission was obtained to adapt interview questions from the original author. Researcher notes were taken on direct observation of the interviews. Other data sources, such as readily available online information, were used to triangulate the empirical data.

Data collection procedures included protecting human subjects, identifying likely data sources, and logistical considerations (Yin, 2017). To protect human subjects, the researcher worked with participants to conduct interviews to feel comfortable and safe, such as in their environment. Written informed consent forms were obtained from participants before conducting an interview, including informing participants of their right to stop the interview at any time. The primary data collection technique was the interview. The researcher’s notes and observations helped reinforce the empirical data. Information readily available online was also be used to strengthen and corroborate the interview data. All participant identification and collected data will be kept confidential through coded references known only to the researcher. As the data was collected, it was secured on an encrypted USB drive. The encrypted data will have a retention period of seven years before being destroyed.

As part of the data collection strategy, the researcher understood that the information collected during an interview needed to be accurate. One objective was to accurately document participants' viewpoints and meanings, which were accomplished by obtaining accurate transcripts and using low-inference descriptions in the report. Christensen et al. (2014) recommend participant feedback and low-inference descriptions, but participant feedback was not possible during a single engagement with each participant. The researcher did paraphrase portions of each interview to offer participants an opportunity to clarify and further explain their responses. Participants' thoughts were described using quotes and language close to their accounts. Efforts were made to capture the information accurately.

The researcher was the key measurement instrument in qualitative research. The role of the researcher was to interact with participants actively to obtain empirical data for the study. Interviewing skills, experience, and expertise on the topic were critical to conducting the study. The researcher put together a series of interview questions. Some questions were based on similar research modified for the research topic, while others were researcher-designed. Open-ended questions encouraged participants to speak about their experiences in as much detail as possible. If answers were not understood, participants were asked clarification questions. The semi-structured questions guided attention to concepts related to the research question. From observation, many case studies contain 10 open-ended questions, limiting the interview time to one and a half hours. This study contained more than 10 questions, but several were semi-structured guiding and follow-up questions rather than the primary open-ended questions.

Data Analysis

The data analysis for this study followed Yin's (2017) procedure for a multiple-case study. The analysis strategy was to rely on theoretical perspectives to extract themes on effective strategies for protecting against data breaches. Qualitative studies depend on the researcher's rigorous empirical thinking, sufficient presentation of evidence, and careful consideration of alternative interpretations (Yin, 2017). Empirical data was explored by coding and organizing it into arrays to reflect themes and subthemes found. Coding is the process of converting unstructured data into categorical or taxonomic data, such as participant feelings about their security practices fitted to high, medium, or low codes based on the language used (Edgar & Manz, 2017). Categories were derived and placed in a matrix to compare and contrast the themes.

According to Leedy and Ormrod (2014), the data is presented thoroughly and accurately, synthesized in tables, figures, or other concise depictions such as flowcharts. Flowcharts and diagrams were created to represent the data for viewing and further analysis. Events were identified and frequencies tabulated and organized chronologically or by frequency to understand the potential connections between events and activities. Observation notes and other supporting data were incorporated to support the interpretation of the interview data. Data exploration helped in preparing the data for further analysis and developing a more specific analysis strategy.

Data analysis strategies rely on theoretical perspectives, empirical data for inductive reasoning, developing a case description, and examining plausible rival interpretations (Yin, 2017). The researcher applied systems thinking and deferred action theories to identify key themes and subthemes. Systems thinking theory allows the researcher to examine a system, as described by Ing (2013), with a design approach to the relationships between: (a) *structure*, which involves the arrangement as a form of input; (b) *process*, which defines the activities and knowledge needed for desired results, and (c) *function*, which includes the contribution of individual elements to the system and delivers the actual results. Deferred action theory allows the researcher to examine a system, as described by Patel (2009), with *planned action design* and *deferred action flexible mechanisms* for adapting to emergent events. From an in-depth analysis of the empirical data, the researcher expected to identify and understand any themes and subthemes that may not have resulted from the theoretical perspectives. Also, as Leedy and Ormrod (2014) recommended, the researcher looked for subcategories and subthemes, then classified each piece of data accordingly. A case description follows a descriptive framework and is especially suited to help uncover themes and subthemes when the prior strategies fail to provide sufficient evidence (Yin, 2017). Case descriptions for this study were developed consistently and helped in uncovering themes and subthemes.

Examining plausible rival explanations works in combination with the three other strategies to support the analysis, contextualizing the interpretations, and strengthening the research towards generalizability (Baškarada, 2015; Christensen et al., 2014; Yin, 2017). Theoretical perspectives were chosen that could potentially elicit rival explanations. Systems thinking theory was used to develop controls to improve processes for a current problem, while deferred action theory helped identify controls to address emergent problems. Data analysis strategies helped to uncover themes and subthemes in preparation for a more in-depth analysis.

The researcher applied analytic techniques iteratively until a compelling case study emerged from the empirical data. Each case was analyzed and summarized before conducting a cross-case analysis. The analytic techniques used in this case study were pattern matching, thematic analysis, and cross-case synthesis. Researchers often use pattern-matching to create themes (Fletcher, Massis, & Nordqvist, 2016; Marshall & Rossman, 2016). Pattern-matching helps strengthen a case study's internal validity if empirical and predicted patterns appear similar (Yin, 2017). The pattern-matching technique helped to focus on the processes and outcomes used in data breach protection strategies. Pattern-matching focused on rival explanations that apply to the theoretical perspectives. Refuting rival explanations reinforces the findings of a case (Oyelami, 2018). Multiple-case study cross-case synthesis is designed to retain the entire case's integrity and then compare any case patterns across the cases (Baškarada, 2015; Yin, 2017). The resulting analysis yielded a consensus among the multiple cases. Thematic analysis requires expert knowledge and judgment to derive themes from the empirical data (Saldaña, 2016). Themes not directly derived from systems thinking or deferred action theories were captured by using thematic analysis.

The researcher used NVivo principally for computer-assisted coding and qualitative thematic analysis. Novice researchers find assistive research tools helpful, especially when there are a research focus and an analytic strategy (Yin, 2017). However, learning how to use Nvivo properly was time-consuming and cumbersome, as noted by Nero (2018). When reliability is a concern, Nvivo can help to establish a chain of evidence and organize the empirical data to assist with the analysis. A consistent analytic technique was applied to all cases.

Analysis of Research Question

The research question restated is: What are effective strategies large public venue operators use to reduce the risk of data breaches in their wireless networks during and between venue events?

The research question addresses IT processes and countermeasures applied to reduce the risk of a breach during events. Given that it is likely for a large public venue with a wireless infrastructure to have a data breach, it is critical to understand which successful strategies reduce the risk of attacks.

The research question was derived from research cybersecurity with organizations of similar size. Saber (2016) recommended extending an understanding of data breach prevention strategies to target information security professionals and replicated them in other environments. Nero (2018) recommended further research on factors influencing the decision-making process for IT network security outsourcing to businesses of different sizes and across a broader industry. Patterson (2017) recommended exploring the rationale for implementing effective and sustainable cybersecurity strategies across a larger population to establish robust security programs and risk-based controls. While most of the research that leads to the research question in this study focuses on small businesses, Saber (2016) described a common thread that organization size is not a factor when protecting data. Large public venues often have a small and dedicated IT staff, resembling a small business or small municipality in terms of team cohesion and size.

Credibility and Dependability

Case study research is subjective, which requires identification and avoiding introducing researcher bias, not the experiences described by the participant. For example, using purposive sampling introduces researcher bias in the selection of participants. However, by being aware and following logical and prior research to justify the selection criteria and the process, researcher bias can be reduced (Christensen et al., 2014). Snowball sampling can introduce a prospective participant's bias, adding unexpected or uncontrolled factors like being in the same geographic area (Emerson, 2015). However, following the research protocol also adds to the credibility of the design. One approach to remain objective was for the researcher to interview participants without personal affiliation (McElroy, 2018). The researcher could recall a professional relationship with a prospective participant but had no personal affiliations with large public venue owners or managers. The potential for conflicts of interest was mitigated by excluding prospective participants with personal affiliations.

Research designs are supposed to represent a logical set of statements, in which the quality of research designs can be judged according to a set of logical tests (Yin, 2017). Four tests are relevant to establish the quality of empirical social research, which includes case studies. The tests are for construct validity, internal validity, external validity, and reliability (Yin, 2017).

Construct Validity

Yin (2017) suggested that the researcher identifies the correct operational measures for the concepts being constructed to achieve construct validity. The pitfalls of failing to develop a sufficiently operational set of measures and confirming research outcomes of preconceived ideas due to subjective judgments were avoided. The development of a sufficiently operational set of measures entailed defining the phenomenon under study in terms of specific concepts related to the study's original objectives. The second was addressed by matching the operational measures to the concepts, citing other studies making the same matches. Also, key informants, or experts, can review the case study report to define each concept through a set of attributes to make it measurable (Baškarada, 2015). Multiple sources of evidence verified and encouraged convergent lines of inquiry during data collection, a tactic recommended by Yin (2017). A second recommended tactic was to establish a chain of evidence during data collection, which can be accomplished with a database or assistive research software such as NVivo (Cook, 2017).

Internal Validity

In qualitative research, internal validity is mainly a concern when conducting explanatory case studies, as the researcher tries to explain why and how one event leads to another (Baškarada, 2015; Yin, 2017). This case study was exploratory without a focus on describing or explaining causal relationships. Therefore, causal logic did not apply to this study. When conducting case study research, a concern for internal validity applies to make inferences (Yin, 2017). Because the researcher could not directly observe the phenomenon under study, past occurrences were inferred based on interviews and documentary evidence. The tests for internal validity determined if the inferences were correct, if the inferences were convergent and whether rival explanations and possibilities were explored. Internal validity can be tested during data analysis using pattern matching, explanation building, logic models, and by addressing rival explanations. Analytic use of logic models involves pattern matching empirically observed events to theoretically predicted events (Yin, 2017). An effort was made to match the empirical data from the study to the theory of deferred action principles for selecting and developing effective strategies designed to prevent data breaches.

External Validity

Researchers test for external validity by considering whether the study's findings are generalizable beyond the immediate study (Leedy & Ormrod, 2014; Yin, 2017). In case study research, the form of the research question can affect the decision to seek generalizations from the study. A research question that poses *how* or *why* questions may be more generalizable than one seeks to answer *what* question (Yin, 2017). This study addressed effective strategies large public venue operators use to reduce the risk of data breaches in their wireless networks during and between venue events. Process, decisions, and subsequent strategy development may be more generalizable than documenting the phenomenon in a particular environment. The groundwork for the generalizability of a study depends on identifying the appropriate theory during the design phase (Yin, 2017).

In case study research, using replication logic involves carefully selecting cases that will either help predict similar results, known as literal replication, or predict contrasting results but for expected reasons, known as theoretical replication (Yin, 2017). Although the study was exploratory, the researcher predicted that large public venue operators that choose to adhere to critical infrastructure guidelines have a higher maturity in preventing data breaches than large public venues that did not follow critical infrastructure guidelines. The differences can likely be explained through the theoretical perspective of systems thinking theory. Systems thinking theory was used to conceptualize elements as systems, leading to the development of controls (Checkland, 1999). Initially, the study sought two or three large public venues adhering to critical infrastructure guidelines, and two or three did not. There were three self-identified adherents to critical infrastructure guidelines, which enabled literal and theoretical replication.

Reliability

To achieve reliability, researchers who follow the procedures in this study in the future should arrive at the same findings and conclusions (Yin, 2017). The reliability goal is to minimize the errors and biases in a study (Yin, 2017, p. 46). To achieve both, the researcher documented the study procedures as the case study protocol. Furthermore, a case study database composed of the data or evidentiary base and report drafts, notes, and recordings was created for the study. NVivo or other qualitative data analysis software can provide the database to help the researcher store the case study data as an orderly compilation in narrative and numeric forms (Yin, 2017). As with maintaining construct validity, maintaining a chain of evidence adds to reliability.

Essential strategies to enhance the validity and reliability of the data to be collected are reflexibility, separating empirical data from research notes, and seeking exceptions and contradictory evidence (Leedy & Ormrod, 2014). Furthermore, strategies such as participant feedback or member checking, using low-inference descriptors, external audit or expert review, pattern matching, peer-review, and theory and data triangulation help enhance validity (Christensen et al., 2014). The researcher used most of the strategies, except for member checking and external review. Both member checking and external review were impractical.

Instruments

The researcher was the instrument for data collection. Though there was a preference to conduct the interviews at participant sites to obtain fuller and more meaningful researcher notes, an audio recording of a Zoom meeting session was a practical method for participants to fit the interview into their work schedule and provide a familiar setting. An audio recording allowed detailed collection of interview data. The video portion allowed live note-taking of tacit responses and helped to highlight interesting comments supporting the interview data. Researcher notes were also taken on direct observation during the interviews.

The researcher had previously engaged professionally with wireless network operators in large public venues. The researcher had more than 30 years of experience in IT and telecommunications, designing, implementing, and operating wired and wireless networks in various industries, including large public venues. Many engagements involved cybersecurity policy development and the application of appropriate security countermeasures. The field experience helped establish a rapport with participants. Researchers are also required to make significant decisions and judgments during the data collection and analysis processes that predispositions, expectations, biases, and values may affect the findings' validity and credibility (Leedy & Ormrod, 2014). As Christensen et al. (2014) recommended, the researcher should be self-aware and document critical-self reflections on the potential biases and predispositions that may affect the research process and conclusions. The research protocol was followed to reduce bias and remain objective.

Because information security information such as internal practices and defenses can be sensitive, participants may not readily disclose information. In order to fully understand participant knowledge and experience shared, the researcher conducted the interviews with a sense of gratitude and curious conversation, which was conducive to data collection in a setting familiar and comfortable for each participant.

The Role of the Researcher

The researcher conducted semi-structured interviews with IT managers and other persons responsible for the cybersecurity of wireless infrastructure in large public venues. The interview is the primary data collection technique for collecting qualitative methodologies (Cooper & Schindler, 2014, p. 169). Yin (2017) described interviews resemble guided conversations to conduct a consistent line of inquiry, with adaptive clarifying questions verbalized in an unbiased manner. As recommended, an interview guide was developed for this study with questions to guide the conversations. Baškarada (2015) describes the role of the researcher includes putting participants at ease and comfortable to directly capture their perceptions and attitudes about events and behaviors during the interview. The interviews were conducted with open-ended questions primarily and semi-structured questions to further guide the conversations. The questions were arranged first to establish a rapport and put participants at ease, followed by questions that elucidated perceptions and attitudes.

The researcher practiced conducting interviews that did not introduce bias and obtain resources to collect data effectively with backup systems to prepare for data collection. For example, if a video camera fails during an interview, a smartphone or video conferencing service could serve as a substitute for recording a video of the interview. Preparation was required to conduct consistent interviews with minimal bias. Data obtained from sources, such as readily available online information, triangulated the empirical data.

Guiding Interview Questions

The guiding interview questions were grounded in the literature on preventing data breaches and mitigating cybersecurity risk (Nero, 2018; Saber, 2016). The researcher contemplated each interview question, relying on decades of professional experience as well as the experience of other IT professionals, to evoke discussions that would answer the research question. The guiding interview questions consisted of two personal or professional questions, 11 open-ended questions, and 15 semi-structured questions. Some of the interview questions have been adapted from Saber (2016), with permission (see Footnote 1), for this study, and the remaining were researcher-designed.

Personal information. The personal questions helped establish the work experience and time at the large public venue.

1. How many years have you worked in this business?
2. What is your position, and how long have you been in this position?

Questions on the work environment. Questions on the work environment helped determine the characteristics inherent to the venue used to compare venues in the cross-case analysis. Questions on the knowledge of the wireless network and architecture helped validate participants' knowledge and experience of the wireless component. Questions on venue services and events helped establish the influences between departments and vendors for each venue.

1. Describe your department and work environment as it relates to cybersecurity and protecting against data breaches.
    - Do you have other roles not related to information technology?
    - How many are responsible for cybersecurity?

   - How is your department organized? For example, do you report to a CIO, a CTO, or a CEO?

2. Describe your wireless network infrastructure and architecture.
   - What is the size of your network, and how far does it extend?
   - Does your wireless network overlap with others?
   - Is your wireless network outsourced? Describe the setup.
3. Describe the services you provide for your customers and receive from vendors before and during events.
   - Can you describe your customer relationships?
   - Can you describe your vendor relationships?
4. Describe the events that are hosted in your venue.
   - How often are the events hosted?
   - What services are offered on top of a wireless network?
   - If the event staffs bring in their own wireless networks, how are they connected, and how do you protect your wireless network?

Questions on internal perspectives and communication. Questions on the perspectives and communications provided a deeper understanding of the influences between coworkers, the departments, and vendors.

5. What are your views concerning the importance of cybersecurity strategies to protect your wireless network from data breaches in your venue?[1]
6. What are your views on how employees recognize the importance of cybersecurity strategies for your venue?[1]

Questions on cybersecurity strategies. The remaining questions helped to capture the cybersecurity risks, and threats participants faced, especially data breaches.

7. What cybersecurity strategies are in place to protect your wireless network from data breaches at your venue?[1]
    - What types of resources do you use to protect your wireless network from data breaches at your venue?
    - How do you find and develop your cybersecurity strategies?
    - If you outsource your wireless network services, how does that affect your cybersecurity strategies?
    - What cybersecurity strategies do you apply to minimize the potential damage of a data breach?

[1] Adapted from *Determining Small Business Cybersecurity Strategies to Prevent Data Breaches* (Doctoral dissertation) by J. A. Saber, 2016. (Order No. 10181342). Copyright 2016 by Jennifer A. Saber. Adapted with permission.

8. Has your venue experienced any cyber-threats to your wireless network? If yes, can you describe the risk and action taken to mitigate it?
9. What cybersecurity strategies have you implemented but have found are not useful to your venue?
10. What types of cybersecurity strategies would you like to implement but have not?
11. What additional information would you like to share regarding wireless network information security strategies for your venue?

Ethical Considerations

The researcher was responsible for conducting the study with care and sensitivity to protect participants from any form of harm, including avoiding the use of deception in the study (Yin, 2017, p. 88). Participant interviews were encouraged to be in a familiar setting to feel comfortable and free from harm. According to university guidelines, academic, financial, or other personal interests may lead to conflicts of interest, compromising the objectivity required to conduct research and potentially putting participants at risk. Harm or discomfort anticipated in the research should not be greater than ordinarily encountered in daily life (Protection of Human Subjects, 2018). Once the IRB approved the research protocol for the study, every precaution was taken to minimize risk to participants. The researcher also worked to keep self-interests and biases out of the research. There could have been an inherent academic conflict of interest with the desire to finish a dissertation while remaining objective in conducting research.

Research participation was voluntary, requiring informed consent. In simple language, the researcher explicitly stated that participation in the study is not a requirement for employment and obtained written consent to proceed at the beginning of each interview. Also, the participants needed to be informed of the nature of the case study. Protection of human subjects applies to vulnerable persons, such as the homeless, illiterate, mentally ill, children, migrant workers, and others who can easily be coerced (U.S. Department of Health and Human Services, National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). The topic and selection criteria for participants in the study did not require and avoided vulnerable populations. Protection of human subjects can extend beyond participants in the study to include previously recorded data on the participants, such as personnel or client records (Yin, 2017). Though the researcher did not review data directly related to participants, it is protected using the same ethical protocol as participant privacy and confidentiality if data were exposed by unintended or accidental means.

According to university guidelines, the potential for conflicts of interest exists where there are academic, financial, or other personal interests, which can compromise the objectivity required in the research. Moreover, participants may be put at risk or unduly influenced by the researcher's conflict of interest. The researcher had discussed the feasibility of recruiting and data collection with an IT professional at a large public venue when developing the research proposal. Though a professional relationship, the researcher chose not to include the acquaintance in the study to avoid the potential for conflicts of interest or any undue influence.

The researcher maintained privacy and confidentiality for each potential participant, participant, organization, and individuals, anonymizing the data obtained during recruitment, screening, enrollment, data collection, analysis, and findings. Each participant was carefully assigned a pseudonym instead of their name so as not to reveal their identities. According to university guidelines, all collected and analyzed data will be kept on an isolated USB drive in a secure location. The data is encrypted for a minimum of seven years before destruction.

When using a forum such as LinkedIn to find participants, there is a risk of breaching confidentiality. LinkedIn groups contain small networks of individuals who may know each other (Damianakis & Woodford, 2012, p. 708). All communication with potential participants conducted within the LinkedIn platform was conducted privately. The university required the researcher to list the name and URLs for all groups where materials were posted. The LinkedIn group leader provided the researcher and the university with written consent to obtain participant contact information from the group members.

Once the IRB modification for using Focus Insite was approved, the researcher met with the research agency to review participant protection, anonymity, and data retention to ensure the agency’s practices and policies aligned with the university's informed consent process and the research protocol. The research agency had an established process, requiring no changes to align with this study.

Summary

The purpose of this qualitative, exploratory, multiple case study was to uncover effective strategies to reduce the risk of cybersecurity data breaches of wireless IT network infrastructures at large public-event venues. The research question, which was foundational to the study, was: What are effective strategies large public venue operators use to reduce the risk of data breaches in their wireless networks during and between venue events?

The research methodology and design was a qualitative exploratory and multiple case study. The target population was composed of IT managers and those responsible for cybersecurity who typically work for a CIO operating a wireless network in a large public venue. Purposive sampling was used to identify persons responsible for the cybersecurity of wireless networks in large public venues. The sampling frame was a LinkedIn group of enterprises and large public venues that operate or wireless service networks. Snowball sampling augmented the number of cases. A research-recruiting agency subsequently provided the sampling frame. The sample size comprised seven cases that reached data saturation.

The setting for conducting interviews was online, where participants' chose their location and time, so each person felt comfortable and secure enough to elicit responses. The researcher conducted the research ethically, which included bringing no harm or elevated risk to the participants.

A thorough discussion on credibility and dependability addressed tests for construct validity, internal validity, and external validity, as applicable to case study research. Ethical considerations and procedures established the ethical protocol applied. It included informed consent, protection of human subjects, preservation of privacy and confidentiality, and data protection and retention.

Data collection primarily consisted of semistructured interviews with IT managers and others responsible for cybersecurity who typically work under a CIO's direction in making decisions on information security and wireless infrastructure protection in their large public venues. Researcher notes and publicly available online information, such as company reports, supported data triangulation. Data analysis followed case study procedures, as suggested by Yin (2017). It included strategic and analytic techniques to explore the empirical data, organization, and extract themes and build explanations for events and activities. NVivo software was used as a tool to assist in organizing and analyzing the data. Once IRB approval was granted, the researcher completed data collection using a research-recruiting agency, then performed the analysis. The researcher adhered to the research, interview, and ethical protocols identified in this chapter. The results of the data collection and analysis are presented in Chapter 4.

CHAPTER 4. FINDINGS

The purpose of this qualitative, exploratory, multiple case study was to uncover effective strategies to reduce the risk of cybersecurity data breaches of wireless IT network infrastructures at large public-event venues. Each case was defined by a large public venue that operated a wireless network, specifically during hosted events. A knowledge gap existed between small businesses and large public venues. Though similar in staffing size, different operational characteristics made large public venues with wireless networks more vulnerable to a data breach. Chapter 4 began with a brief introduction to the study and the role of the researcher. A description of the purposive sample followed. Next was a description of the research methodology to analyze the data. The final section presented the data results and findings in detail with a summary of the chapter.

Introduction: The Study and the Researcher

In Chapter 4, the researcher documented the data collection, analysis, and interpretation of the empirical data. The phenomenon of a data breach was studied for its likelihood to occur at a venue and for its familiarity. Yin (2017) described holistic case study designs use a single unit of analysis examined in its entirety. Systems thinking theory and deferred action theory were used to help focus on the processes and activities of data breach prevention strategies within organizations holistically.

Chapter 4 fits into the overall qualitative multiple case study by providing first-hand evidence and analysis that informs the study to answer the research question. Data collection provided the evidence from a representative sample population in an interview format, along with associated researcher notes and publicly available information as the results for analysis. Findings were driven by a systematic analysis of the empirical data, which helped develop themes that answer the research question reproducibly. Subsequently, interpreting the themes in the research question and cross-referencing the extant literature led to the conclusions provided in Chapter 5.

The researcher's role in this chapter was that of the instrument for data collection. The researcher used interviews to capture participant perceptions. To prepare for the project, the researcher had to learn how to interview to put participants at ease and discuss the topic freely with minimal intervention and bias. Several sources were used for learning how to conduct an interview. Among the sources were people who have done qualitative research and videos, such as Payne (2015), which steps through field interviews for an ethnographic qualitative study.

The researcher had worked over 30 years in IT and telecommunications, including implementing network security countermeasures to prevent cybersecurity incidents such as data breaches. A study on cybersecurity in large public venues with wireless networks was appealing and beneficial to many in similar environments. Therefore, there was a natural interest in this topic and a desire to give back to the many venue owners and wireless network operators in the form of a formal research report that can be of value to strengthen their cybersecurity posture. This report's positive outcome was to inform and convince venue owners and leaders who operate a wireless network to act, such as allocating more funds, developing policies, and applying effective strategies to address the numerous vulnerabilities and threats inherent to their wireless networks.

Although the researcher has had a role as a vendor and as a solution provider in the past, the employment role at the time of this study was to develop technology strategies for internally facing corporate products and services. There was no motivation to sell a product or service to any venue, which could lead to a conflict of interest or undue influence on participants.

Cybersecurity remains a critical function that transcends venues and businesses. The researcher influenced a portion of the telecommunications industry and relied on evidence and facts obtained using research methods. This research study helped springboard the researcher into roles that are more grounded in research.

During the data collection and analysis processes, significant decisions and judgments are often required. Researcher predispositions, expectations, biases, and values may affect the findings' validity and credibility (Leedy & Ormrod, 2014). A researcher should also be self-aware and document critical-self reflections on the potential biases and predispositions that may affect the research process and conclusions (Christensen et al., 2014). After introspection and honest reflection, it was clear that modeling portions after recent and similar studies, such as Saber (2016) and Nero (2018), would improve this study. Initially, this study’s sampling frame was like Nero’s (2018). After the initial attempts at recruiting, it became clear that this study's target population was too difficult to find. Though acquaintances would have qualified for this study and may have provided insight into finding the target population, the potential for conflicts of interest and undue influence and bias was too great for inclusion in the study. Therefore, for the study, unknown persons were sought using a third-party research-recruiting agency.

The researcher prepared for case study research by reviewing several case studies in IT. Reading Yin’s (2017) book on case study research and applications helped develop a comprehensive approach to applying this study's methodology. Similar research conducted by Nero (2018), Patterson (2017), and Saber (2016), augmented relevant experience with examples of recent case study research. Preparations included learning about interviewing techniques for qualitative studies from several sources, including an ethnographic study conducted by Edith Cowan University (Payne, 2015). A review of other case studies and qualitative studies, in general, provided the steps for qualitative examination and reinforced the skills needed for this study. It was important to learn to be mindful not to insert personal experience or bias by becoming a good listener and viewing unexpected situations as learning opportunities.

Description of the Sample

The target population was composed of IT managers and other persons responsible for cybersecurity who likely worked under the direction of a CIO and made decisions on information security in large public venues that operate a shared wireless network in the United States. Included were also property owners who outsourced shared wireless networks. Subsequently, service providers and customers were added to the study. It was relevant to include those involved in cybersecurity planning and decision-making and those who practiced cybersecurity at the venue. Large public venues can have various governance models, where it may be possible for a technology manager to report to an executive that does not specialize in technology. The researcher found it difficult to recruit participants who have specifically not have experienced a data breach within a year while operating a wireless infrastructure at a large public venue. However, once participants became comfortable with the investigator during the interview, they were more likely to disclose experiences with data breaches. The study was designed to uncover strategies used by large public venues with wireless networks to prevent data breaches. Therefore, it was reasonable to relax the requirement for a large public venue not to have experienced a data breach within a year. If a participant were to mention a recent data breach during the interview, it would provide an opportunity to explore any lessons learned and factor that information into the analysis.

While developing the proposal for this study, it became apparent that the target sample population was difficult to reach. Initially, an adequate sampling frame was to choose two large

LinkedIn groups. Also, snowball sampling was used to find the hard-to-reach population and expand the sampling frame. LinkedIn group owners granted permission to make a posting and reach out to individuals within each group. A posting was first published in each group, followed by direct messages to group members and snowballing with every targeted message. Once there were no responses to the postings, the researcher looked through the group members and selected individuals who appeared to meet the inclusion criteria from their profile pages. Messages were sent only to individuals who met the study's inclusion criteria, along with the researcher’s contact information for snowballing. Attempts at recruiting within the two LinkedIn groups yielded no results.

Once the list of pre-qualified subjects in each LinkedIn group was exhausted, the inclusion criteria were modified, followed by enlisting the help of Focus Insite, a research-recruiting agency. The original inclusion criteria were unclear and needlessly restrictive. It was unclear that only venue owners or venue personnel qualified for the study. However, third-party service providers and even venue customers who have made service arrangements (i.e., providing or receiving) with the venue and possessed the knowledge required in the study should have also qualified.

The criteria that apply to time employed in cybersecurity, time at the location in question, and the period since the last data breach, were needlessly restrictive since there was no requirement for a participant to be a cybersecurity expert. Moreover, data breaches often go unreported. Also, the exclusion criteria for operators at high school stadiums and lower-division collegiate venues were needlessly restrictive because individuals in those types of venues may have qualified for the study. Examples were provided to the recruiting agency to help clarify the inclusion criteria.

Focus Insite was an established and well-known market and IT research company that provided tiers of research services. With Focus Insite's help, the researcher was able to interview seven participants over three months. None of the participants were excluded since all provided insight from different perspectives, and all qualified to have enough knowledge about cybersecurity at their venue.

Protection of Participants

As each respondent signaled their interest to participate with Focus Insite via email or telephone, the recruiter used the researcher's pre-approved script to pre-screen eligible participants. Eligible participants were asked to initial and sign an electronic version of the informed consent form after pre-screening. Participants then electronically signed the informed consent form and were received by the researcher at least 24-hours before the interview, as required by the Institutional Review Board. By using a pre-screening script and informed consent form, the researcher ensured the process was carried out accurately and completely to protect participants' rights, privacy, and secure handling and storage of the data.

Once the informed consent process was initiated, the researcher proceeded with an online interview based on each participant's schedule. During the interview, the first steps were to validate each participant's eligibility for the study and to ask questions to ensure informed consent. The recruiting agency set up each interview via telephone and email, pre-screened via phone, and exchanged the informed consent form online. The answers to the pre-screening questions were reviewed before scheduling each interview. During the interview, the researcher asked if there were any questions about the informed consent process and then conducted the audio-recorded interviews using a Zoom meeting format. Zoom meetings were selected over Skype and Facetime for their pervasiveness, ease of use, enterprise focus, recently improved end-to-end voice security, ability to record only the audio portion, and the ability for the researcher to take notes on tacit and other non-verbal responses during a video session.

Research Methodology Applied to the Data Analysis

Data triangulation consisted of three types of evidence or data sources. Yin (2017) identified the three types of evidence as interviews, documentation, and direct observation. The study used audio transcriptions of interviews as the primary data source, direct observations over video sessions, and documentation of publicly available information as secondary sources. The researcher conducted all interviews and direct observations online. Participant responses to the interview questions provided insight into their experiences and perceptions regarding preventing data breaches. During each interview, the researcher took notes of the direct observations. Documentary evidence was in the form of publicly available organizational or related topical data for each case. All data were assigned pseudonyms, such as *P1* (for participant 1) and *Case 1*, to protect participants' privacy. A within-case analysis report was then created for each case from the empirical and documentary data. When all case reports were completed, a cross-case analysis was conducted for further interpretation.

The researcher sought multiple cases to help strengthen the data by direct replication if analysis of independent cases agreed or by providing additional insight due to contrasting views. Yin (2017) indicated that the primary purpose of having multiple cases is to make the data stronger. Internal validity is strengthened by using a systematic analysis that is consistent and repeatable. The analytic methods used in this study were pattern-building and cross-case synthesis. For a consistent application of the analytic techniques, the researcher developed four propositions and two rival explanations to help in theory building. This chapter's primary purposes were to develop themes and organize the empirical data for use in theory building in Chapter 5.

NVivo 12 Computer-assisted Qualitative Data Analysis Software (CAQDAS) software was used for database analysis, exploration, and queries on the coded data. The researcher assembled a case study *database*. Yin (2017) identified a case study database as critical for maintaining a chain of evidence and increasing the study's quality substantially. The *memo* feature helped document how ideas and concepts were connected to develop insights as well as themes. The *query* feature helped in searching through the transcripts for similar language when following a train of thought. The *visualization* tools helped to view emphasis with word clouds and connections between participants with word trees. References to an NVivo guide helped determine the steps for using the software (Bazeley & Jackson, 2019). The researcher had practiced using the NVivo software for work-related content and had created reports on lessons learned before analyzing this study.

Participants were asked 11 open and semi-structured questions during the in-depth interviews, contained in Chapter 3. The format for conducting each interview was Zoom meetings, which differed from the original research proposal that included in-person interviews. The primary reason for conducting the interviews with Zoom meetings was the COVID-19 pandemic during data collection. A benefit of Zoom meeting interviews was that participants were likely to be more at ease and discuss the topic more freely while in a familiar, safe, and private environment. The audio portion was recorded, and live researcher notes were taken during each video interview.

The researcher analyzed each participant's response within the context of their organization with the triangulated data. Theme building occurred individually through the lens of systems thinking theory, then through the lens theory of deferred action. Pattern matching used the codes developed from the theoretical lenses to search for matching patterns within the empirical data. Thematic analysis was then used to build themes directly from the observed data. Once all within-case analyses were completed, a cross-case analysis was conducted. Using cross-case analysis, the data captured from a cross-section of venue participants helped to form a deeper understanding of the subject and then develop a cross-case synthesis. Cross-case analyses can lead to prescriptive inferences about best practices after completing case studies on multiple organizations (Cooper & Schindler, 2014).

The interview questions guided the conversation, which was not intended to be a question and answer session. One useful technique was to reference previous answers and ask the participant to elaborate in the context of a new question further. The technique also provided an opportunity for the participant to clarify and correct any responses that may not have been clear. The researcher maintained a collaborative setting by putting each participant at ease by being unassuming, asking for clarifications, being curious, respectful, and grateful. Any notes related to the setting were added to the researcher notes for analysis. Though the interviews were conducted using Zoom meetings with video, only the audio portion was recorded. After each interview, the audio recording was transcribed using Dragon Professional Individual for Mac 6 software. The software had a reputation for accurately transcribing audio files. Some of the recorded audio files were not clear enough for the software and were transcribed by Focus Insite's manual transcription service. The data was deleted from the Focus Insite server as soon as the researcher accepted the transcript. The researcher ensured that participant data was kept private and confidential.

A note-taking guide was developed as a reminder to notice and record unexpected and emerging concepts and themes. The notes included tacit responses and audio cues during each interview. These included powerful quotes that would back up the analysis, key actions and behaviors, unexpected comments, keywords that highlight the study, and repeated patterns that stood out. After each interview, the researcher looked up readily available online information about the venue and any details that would validate and add depth to the responses. Online information served as documentary evidence. The information included references to organizations such as sports leagues, vendors, and the wireless network. The extant literature supported or contradicted the information relative to the data. Researcher notes, online information, and extant literature helped the researcher to triangulate the empirical data.

A conceptual system process diagram modeled the potential interactions and influences that may prevent a data breach in a venue based on systems thinking theory. Systems thinking theory allowed finding themes in the data that depict the relationships between (a) structure, (b) process, and (c) function, as described by Ing (2013). The resulting coding terms extracted from the diagram helped to focus on the systems aspects for developing themes. The different factors in the systems from multiple cases emerged by applying systems thinking techniques to the collected data. Elements from various systems can be revealed when working with a common set of characteristics (Jonker, 2017; Matook & Brown, 2017). Large public venues with wireless networks were characterized by high density and capacity, a large coverage footprint, and shared resources to deliver a range of services to thousands of attendees, vendors, and tenants during events. Figure 1 illustrates the conceptual system process developed for the thematic analyses of the large public venues.

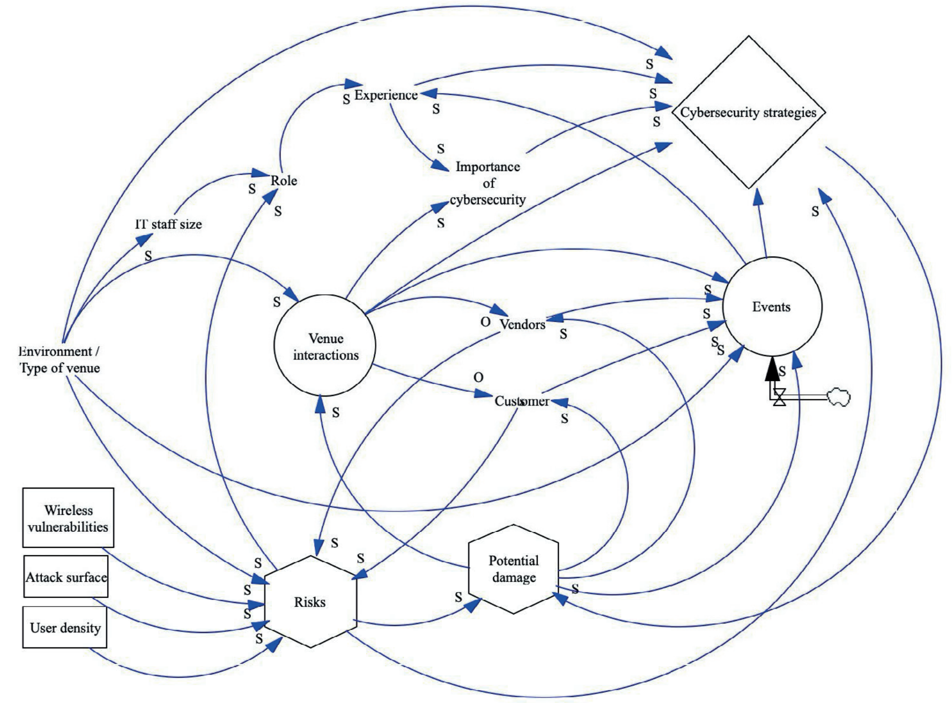

Figure 1. Conceptual system process based on systems thinking theory. *S* identifies supporting or direct influences. *O* depicts opposing influences or inverse relationships.

According to Patel (2009), the three central aspects of the deferred action theory are planned action, emergence, and deferred action. An organization or individual pursues a goal or a purpose with a plan (Tavanapour, Bittner, & Brügger, 2019). Planned and contingent approaches for enabling solutions with built-in feedback loops can withstand long-term emergent events in changing environments (Khan et al., 2010). The researcher was able to identify several cases in which organizations had planned and contingent approaches and feedback loops for cybersecurity protection. Since threat actors are always evolving methods and developing skills to exploit vulnerabilities or perform attacks, adaptable plans or cybersecurity strategies could be critical components for protective strategies.

The researcher identified constraining factors that could likely apply to developing and selecting strategies to detect and prevent data breaches. Limiting factors included physically, logically, and technologically related wireless network segmentation, service differentiation for multiple tenants, service provisioning for events, and application hosting or integration. As emergent events occur over time, every constraining factor can change. When viewed as a system, the varying levels of interactions and influences among multiple parties led to higher complexity. On the one hand, the wireless network operator enforces semi-autonomous or autonomous applications of organizational policies. On the other hand, other forms of automation, such as behavioral analysis on a network, can detect data breaches. Also, if a service level of performance had been established as a baseline, automated systems may lead to detecting a data breach by measuring degradation in performance.

Intrusion detection or intrusion protection systems (IDS/IPS) require purposeful investment in sensors and staff and vary in effectiveness and automation. The researcher expected to see manual and static applications of outdated policies. If the wireless network is given a lower priority than, for example, event attendants' physical security, funds allocated for cybersecurity defense may not be enough to be effective. The researcher looked for the venue's wireless operators' ability to perceive their changing goals in a dynamic environment. Changing goals in a dynamic environment requires a system, with actions performed by humans or sensors, to check environmental states and produce actionable information to re-align with the organization's changing goals (Geyda & Lysenko, 2019).

Concerning the modification to the interview format, the interview continued to be the primary data collection technique with no negative impact on the study if the audio recording was of high quality. The researcher observed that participants were comfortable and relaxed during the Zoom meeting interviews. Zoom meetings was a popular and easy-to-use platform. It offered high-quality audio recording with several options. Zoom had just updated its software to improve end-to-end security for paying customers. Therefore, subscription Zoom meetings met the requirements for conducting in-depth interviews with participant confidentiality and high-quality audio.

The researcher modified the exclusion criteria because it was needlessly restrictive. The inclusion criteria were clarified to include service providers and venue customers who would possess the knowledge required for this study. Another change was to remove the requirements that a *participant had to be in the cybersecurity industry for three years or more and at the venue for at least one year*. The requirement for *being in the cybersecurity industry* was an attempt to find participants who are cybersecurity experts. However, knowledge of cybersecurity strategies and decision-making roles do not always include cybersecurity experts. *Time at the venue* was a needless requirement because, as an example, service providers often have short periods of engagement but learn much about the venue. The researcher changed the inclusion and exclusion criteria to provide clarification and remove needless restrictions.

Focus Insite was enlisted to recruit participants. An unexpected result of changing the recruitment method was that all research recruiters pay an incentive to participants. The researcher turned in an IRB modification form to address the changes and ensure participants' protection. The modifications provided clarity so the study could proceed quickly after the research committee and the IRB approved the changes.

Presentation of Data and Results of the Analysis

The purpose of this qualitative, exploratory, multiple case study was to uncover effective strategies to reduce the risk of cybersecurity data breaches of wireless IT network infrastructures at large public-event venues. Seven representative cases were selected to explore the strategies used to protect against data breaches. The following section describes each case. Portions of participant responses have been altered to protect individuals and organizations; therefore, the case descriptions contain no identifying information.

Case 1

P1 was an assistant director for a stadium with an affiliation with a sports league. The IT staff that was responsible for cybersecurity consisted of three individuals. The venue had a large and complex Wi-Fi network that interacted with a cellular distributed antenna system (DAS). The DAS enhanced wireless reception. P1 commented that "it's a very complex system that implements the DAS, the distributed antenna system, and mixes with our Wi-Fi system." The venue owned and operated the Wi-Fi network. The DAS was, at least, partially owned and mostly managed by the venue. P2's department complied with the Department of Homeland Security and the league's policies and guidelines. P1 commented, "we follow [the league's] compliance…our location needs those policies…we follow that and structure ourselves around that." P1 further described the relationship between the stadium and the league:

> We work with them and see what they do and their facilities and what they could do because, when it's their game, it's their stadium; we're just there for support. They take over the stadium. We have to follow their structure too. We have our own structure as a facility that we do our own events too.

Moreover, as the venue's IT department, they were also "in charge of cybersecurity, HIPAA, and PCI DSS compliance" (P1). HIPAA compliance is applied only to the on-site clinic. The venue often processed credit card data where "you don't want people's data to get compromised…we do test the network all the time to make sure there's no bots, there's no rogue devices in our network" (P1). P1 emphasized the importance of cybersecurity as "we do a lot of cybersecurity because of credit card info…target[ing] all those places you don't want people's data getting breached." The principal focus of P1's venue was to protect its customers.

P1's venue sets the policies and service level agreements (SLAs) with tenants, vendors, and contractors. P1's team actively communicated cybersecurity topics monthly. Regarding periodic activities, P1 described:

> We do a monthly pen-test, penetration test in our location internally, externally, and we do provide them an overview of our network, how it goes and how we create their respective VLAN, and where does it get routed to and the equipment we use. We do sniff our network pre-event and during the event to make sure we don't have any bots or anybody doing malicious stuff through firewalls.

The IT command center was used during events for live monitoring and benchmarking for cybersecurity and capacity planning. The monitoring and configuration management system provided P1's team with visibility into "every single device connected and where they're going and what location in the building they are" (P1). Individuals were tracked "down to a specific area within five feet" (P1). The network was highly segmented with virtual local area networks (VLANs) throughout the building along with high-resolution tracking. VLANs, combined with a centralized cable patch system, allowed P1's team to shut down specific areas to contain threats.

The venue services included Wi-Fi guest access, Wi-Fi or wired access for vendors and concessionaires to process payments, and private Wi-Fi for events. There was also an arrangement with the DAS anchor tenant (i.e., primary cellular carrier) to push its subscribers onto the carrier's own Wi-Fi network. The venue provided separate Wi-Fi networks for each team during sporting events. Some of the services specific to the venue were Internet lines, phone lines, rack space to host network equipment, and customers' ability to rent walkie-talkies with dedicated frequencies. The venue also provided production teams, advertisers, and sponsors with network transport for the video to various endpoints throughout the building. The venue used a Ticketmaster network for event billing in addition to ticketing. Using the Ticketmaster network, P1's financial services network was kept small, allowing the venue to focus on service provisioning.

P1 tested and evaluated all the hardware and software in a segregated test environment. The IT team performed annual "audits to see what needs to be replaced, find a replacement, do proof-of-concepts" (P1). As part of planning, they "have a response protocol in case one is trying to shut down the specific area where the breach is, and we have to do an incident report and see what was the damage and investigate" (P1). P1's team performed multiple cybersecurity audits annually, such as the PCI-DSS, HIPAA, the sports league, Homeland Security, and internal to the venue.

Case 2

P2 was a network manager for a stadium affiliated with a sports league. The IT staff consisted of 10 individuals who were responsible for IT and cybersecurity at the venue. The venue had a large Wi-Fi network separate from an equally sizeable 4G network. Though the league-owned and operated the Wi-Fi and 4G networks, the network manager and staff helped with "hands-on issues, configuration issues, and drive policies and initiatives" (P2). One component was to use the network operations center (NOC) to monitor the network's health, transmission, and up or downtime. The second component was the security operations center (SOC), which was dedicated to monitoring network traffic.

Even with the league’s ownership and oversight, P2 stressed that cybersecurity was the responsibility of all the stadium employees, though the other employees looked to the IT staff for guidance. P2 described the employee relationship:

> We train our staff, and we make everybody responsible, so everybody has some element of responsibility from the help desk guys monitoring antivirus reports and providing us feedback on things that they're seeing being the hands-on, and that cycles all the way up through the organization straight to myself and then also up to our vice president.

The services provided by the venue to the customers, vendors, contractors, and tenants helped determine the risks for which the league, network manager, and staff developed cybersecurity strategies. In the last seven years, P2 had invested heavily in upgrading the Wi-Fi network and making changes to strengthen third-party access. The focus at the time was on “further securing third-party access that that really can be a blind spot that most organizations don't necessarily think about” (P2). As a part of the cybersecurity strategies to prevent data breaches, event staff, whether part-time or seasonal workers, were hired directly as employees of the venue to operate directly under the corporate policy umbrella. Similarly, P2 described third-party contracts were used to hold contractors to “a similar set of metrics to” their employees.

P2 received support from the league, which was the owner and operator of the venue’s network. P2 described the relationship with the league included facilitating regular monthly reviews:

> We do a monthly review of incidents with our vSOC. We go over every kind of metric initially, how many incidents, how many incidents were determined to be benign, and then the important ones. If there was anything critical or labeled critical, what it ultimately was, and how it was resolved.

P2 and the staff met annually with current and new vendors who would participate in the venue's cybersecurity. The vendors would meet with P2 to review the best practices and potential changes and updates to their programs. Some changes could have involved additional features and licensing to enable the vendors' expanded products or services. When combined with continuous input from the league, P2's organization maintained an environment with best-of-breed products and services and constantly evolving best practices. As a matter of practice, P2 did not typically use a single-vendor solution to reduce the risk of a zero-day flaw that would put the entire organization at risk.

Cybersecurity strategies affecting the venue infrastructure and access were to use multiple traffic isolation and segmentation techniques, user access control, and disallowing bridging to force neighbors in the vicinity to get off the venue's Wi-Fi network. P2 described a socially oriented cybersecurity strategy that involved empowering *power users* to communicate cybersecurity responsibilities and practices throughout the venue. The league operated and monitored the venue's network using its security operations center (SOC), generating incident data for monthly reviews. In addition to incident data, repeated in-house penetration tests provided evidence that could be used to make informed decisions in the future. Lastly, P2 explained that a "pre-designed cybersecurity response plan" had been developed to be activated, depending on the type of incursion.

Case 3

P3 was an IT Event Day technician at a stadium affiliated with a sports league. The IT staff consisted of an IT Director and an IT Manager assisted by eight event-day part-time technicians. All ten individuals were responsible for IT and cybersecurity at the facility, which P3 reported to be a "very small segment of the management company that runs everything inside the stadium." P3 described the IT department's responsibilities encompassing "everything from the wireless in the stadium to the ticket scanners at the front door to everything connected to the app created by the team to run the TVs from" the displays in the different suite venue levels. P3 also worked directly with performers and vendors to ensure good performance and to fulfill their IT-related needs during events.

The venue-owned Wi-Fi network covered the stadium and extended to the parking lot and into several city blocks. P3 also commented that when the league occupied the stadium, it belonged to the revenue-generating sports team, and the IT staff played a supporting role. If there were a data breach at the venue, safety concerns would probably be the number one problem. First responders used the venue's wireless network for surveillance, and a data breach would affect their operations. A data breach would also affect brand reputation, causing embarrassment to the venue and the sports league.

Once the event schedule for the league's team was established, the venue would meet with the vendors to identify their needs and for the IT department to assign the credentials each vendor would use during each event during the year. Every event had a different set of credentials for access by vendors. Access credentials were also often changed for the IT department. P3 commented that network access credentials sometimes changed weekly or after two or three events. The venue hosted a highly restrictive private network and a separate public network. The public network contained no servers that could be used maliciously, and access to the public network was also unavailable when there were no events. A separate Wi-Fi network, owned by a different company, supported all point-of-sale and concession services with a management (MDM) solution that helped strengthen the venue's security posture.

The relationships between the IT staff and the venue customers have developed from troublesome due to the volume and variety of requests for IT services several years before highly collaborative and predictable. P3's team was able to learn and develop the network over three to four years. During a period, the IT staff had contracted a consultant from the Wi-Fi equipment provider to help build and secure the venue's network. The local community of stadiums and arenas also provided a large amount of support by loaning experienced personnel and having annual reunions to share and exchange information about cybersecurity and other topics. Most of the training P3 received was informal but specific to the venue and other venues in the local community.

In P3's view, cybersecurity strategies that have worked well include having someone always monitor the network, constantly changing information such as access credentials, and being driven by an IT manager paranoid about cybersecurity. P3 discussed improvements such as connecting to a Cloud-based 2-factor authentication (2FA) system for credential management and bringing in a mobile device management (MDM) solution.

Case 4

P4 was an IT Specialist for a stadium that hosts a stadium affiliated with two sports leagues. The IT staff consisted of four individuals responsible for different tiers of IT and cybersecurity at the venue. The IT Director reported to the Vice President of Facilities, highlighting P4's perspective as being "a landlord to different tenants." The IT staff was responsible for “end-user support to networking, network admin, to some cybersecurity things, to mobility devices, to troubleshooting Wi-Fi issues” (P4). The venue had a small Wi-Fi network that was separate from the large Wi-Fi and DAS networks. The Wi-Fi networks were operated by a cellular carrier and professional sports teams. The DAS network was operated by the cellular carrier. Since the venue had several wireless networks with separate ownership, each network was managed with varying cybersecurity degrees. If a data breach occurred on P4’s Wi-Fi network, it would likely have little impact on the operation due to high network segmentation. The incident would trigger an investigation that would follow with appropriate corrective actions.

The venue was owned by a state authority, operated as a public-private partnership (PPP). The company that P4 worked for was a non-profit agency due to its revenue-generating capabilities. Therefore, though not compelled, the venue followed state-defined IT guidelines for best practices and applied them whenever possible to their tenants. The venue used network segmentation as the principal cybersecurity strategy to separate the internal private network from the public network, with a formal process for approving additional or elevated access via an encrypted virtual public network (VPN). Each guest or device that required Internet access was assigned a password. Network access was limited only to the Internet, with no access to the internal private network. Users who desired access to the internal private network were not allowed access to the public network until going through an authorization process and established that the devices being enrolled met the established minimum-security standards.

P4 further described how network segmentation benefits their venue by protecting them from the adjacent Wi-Fi networks, which have outdated settings because of their “laxed attitudes towards cybersecurity.” Thus, the venue mitigated risk by segregating from the adjacent Wi-Fi networks. P4 identified IoT devices like thermostats and HVAC equipment controls. P4 explained that IoT devices were often vulnerable because "those devices only update for a year, and then afterwards, whomever the company is that release that device, no longer pushes updates." IoT devices are often neglected. To make them more secure, P4 recommended "added precautions," as well as enabling two-factor authentication (2FA). IoT devices at the venue were managed on a segregated and adjacent network operated by a third party. A final cybersecurity approach reported by P4 was to lock down the work phones and devices to company-owned devices. Mobile device management (MDM) can then be used to apply cybersecurity settings and further mitigate the risks those devices present to the venue.

Case 5

P5 was a Desktop and Network Administrator with cybersecurity responsibilities representing a sports league assigned to a venue. The IT staff consisted of "eight workspace support engineers at each location" (P5). A combination of the venue staff and centralized resources included a Software Developer, Network Manager, IT Manager, and the Director, which totaled an IT staff of 12 supporting each venue. The IT Director reported to a CIO. P5 did not know precisely how extensive the Wi-Fi network was but commented that the staff supported tens of thousands of fans on an open Wi-Fi network in addition to digital ticketing, merchandise sales, coach plays, and athletes' health records. Suppose a data breach were to occur at the venue. In that case, the potential for harm was exposing personal information for the coaches, social security numbers for the athletes, financial information related to ticket sales, and personal credit card numbers. P5 described the Wi-Fi network at the venue as being 15-years old and outdated. The venue's Wi-Fi network required upgrades and significant changes just to bring cybersecurity up to date.

The relationship between the football league and the venue was that the league would pay “to use their venue” (P5). The league would bring containers with servers and network equipment plugged into data ports at the venue to enable many of the services needed during each game. P5 described network segmentation as the underlying means for separating the services and the different types of users. Different vendors provided different services on their respective networks. The printer provider had a dedicated network, while each third-party kiosk merchandiser also had its network as well. Password encryption and Cloud-based services provided additional security layers, including the ability to wipe device configurations if managed by the league. From an operational standpoint, P5 recognized that the IT staff’s weekly reviews, keeping up with break-fix, and timely device patching, were strategies that helped them maintain a high cybersecurity posture.

Future work involved upgrading and configuring the Wi-Fi network to enable security measures and improve performance. P5 also wanted to introduce penetration testing or network scans with a network analyzer. The managers and the director ensured the venue was kept secure, even by pushing the venue operators when necessary.

Case 6

P6 was an Institutional Research Specialist for a community college. Some of the responsibilities included support for faculty members and the Wi-Fi network that supported events. P6 described: “we may do so more than others because we're a community college, so people can rent out our space for events that aren't even connected to the college.” Though the wireless network at the college could not be considered to be an extensive and high-density network, the venue faced decisions attributable to the delivery of a range of services to hundreds or thousands of attendees and vendors during events at their facilities. Some of the events were vendor fairs and concerts, sometimes run entirely by the college, while other times in partnership with other organizations. The IT staff that supported events and the college's general IT operations consisted of 15-20 members. P6's team was headed by an IT director who reported to an executive responsible for the campus facilities.

Regarding cybersecurity, P6 shared that "everybody in IT is responsible for cybersecurity in one way or another." The "communication between all departments on campus is important as far as dealing with breaches" (P6). P6's venue was exposed to several global and targeted phishing attacks that convinced the staff to review and learn from every attack to make improvements.

Event coordination for the college was often a joint effort between the IT staff for managing the technical aspects, a media group for video production and photography, and marketing. The college always provided a wireless network for the event staff and visitors. Concert event staff that requested network transport were provided with a wired port that was completely separate from the college. An average of two events per month occurred at the venue. P6 iterated that the period between events gave them "time to advertise it" and make any changes to the network. With few exceptions, the private Wi-Fi network was only offered to the college staff and faculty.

The private Wi-Fi network was "reserved for the employees so that we're not all on the same network as guests" (P6). Even within the private network, the IT staff limited access by role such as faculty access only to enter grades and access their data. Access to more sensitive data required VPN access to the college network. When enrolling new faculty members, P6's team made "sure that any new faculty member has access rights to our certain sites … different users as far as different levels of access, whether they can edit or view certain items" (P6). The network systems department benchmarked and monitored traffic for changes in traffic patterns that appeared suspicious. The IT staff prepared and delivered information sessions periodically to the “faculty or staff familiar with the system” (P6). P6 elaborated that among the topics covered were email etiquette up to “cybersecurity concerns and things to look out for, things not to click on,” generally sharing best practices and illustrating how attacks appeared.

P6 reported cybersecurity as a collaborative effort in which information flowed from users to IT staff and back to all users. The IT staff emailed reports of attempted attacks globally to provide examples to users of attacks and request users to report any similar activities. P6’s view was that “everybody needs to share information,” regardless of the role or who is under attack. If neither IT nor the user knew what to look for because even one user did not report an attack, the attack could remain hidden and grow without notice.

Case 7

P7 was an IT Manager for a stadium affiliated with multiple sports leagues and a large conference center. The immediate IT staff consisted of the manager and “20 seasonal IT employees that assist every game” (P7). P7 described the role specifically:

> We set up and strike down any point of sales, any electronics, anything that communicates over the network before an event, as well as being on-site during game day to handle any type of real-time issues that come up.

A data breach at any of P7’s venues would have resulted in a damaged reputation, legal action, fraudulent activities, and others. P7’s role required responsibility for PCI-DSS compliance due to the point of sale equipment. Each venue was independently owned, but P7’s team and company managed the IT components.

Functionally, P7 also reported to each of the venue's general managers and the employer, the regional venue IT manager. Each of the venues had a sizeable Wi-Fi network. Each venue also had a cellular DAS network, which was "almost critical for the guest experience" (P7). However, the DAS networks were not managed at all by P7's company. The services provided at the venue were primarily delivered on Wi-Fi networks and wired ports in support of the events.

Before each event, P7's team created a plan for placing cash registers and point of sale equipment. While P7 always preferred to connect the equipment for sales transactions on wired ports, there were many instances, such as in the bowl during concerts, where wired data ports were out of reach, and the Wi-Fi network was the only option. P7's team worked with the network services team to improve coverage if the Wi-Fi signals were too weak. P7 viewed the event staff as "pretty much our own people," exhibiting a comradery that spread to working cooperatively with contractors. At one time, P7 was invited by the event staff to help improve their working relationship with contractors. Contractors were vigilant and had many contacts in the industry, sharing information about venue events and cybersecurity trends with P7. Concert and other third-party event staff would sometimes bring their temporary wireless equipment to plug into wired ports set up with Internet access only. P7 fostered an environment of cooperation and sharing, "my whole thing is that I believe in the team ... I realized that that's the only way to be successful based on my profession." P7 even aided other venues, not under P7's responsibility.

P7 encouraged employees to take IT and cybersecurity certifications for greater depth in understanding and help them in their careers. Trade magazines provided up-to-date information on trends and provided direction for continuous improvement. P7 also encouraged venue general managers to budget for a program to periodically review incidents and become more proactive.

However, the decision was more often not implemented due to the perception that IT did not generate revenues. P7, nevertheless, persisted and explained:

> I make it a point to have me as part of those staff meetings include a segment when it comes to data security. Get them to buy in, in terms of why they should do it. Sure, it may take a few more minutes, but having those explanations, showing them what a bad guy can do, actually drives the point home. If I get buy-in from the people that use technology, that solves most of my problems right there.

Sometimes one general manager would understand and implement a proposed change, but others would not see the value.

P7's parent company managed multiple venues and had their vendors vetted by a CTO who held cybersecurity certifications. Therefore, guidance and policies were provided by the parent company, and P7 applied and enforced them. The parent company had also developed policies that were "much stricter than what the [leagues] are" (P7). Though P7 did not directly monitor the venue's wireless networks, the regional venue IT management or the sports leagues would send alerts to the respective venues.

Among the security controls used at the venues were network segmentation using VLANs, two-factor authentication (2FA), and MAC authentication for point of sale and other controlled devices. Since the venues were PCI-DSS compliant, encryption and other applicable security controls were also used. P7 offered that since 2010 bring your own device (BYOD) spread and caused issues such as putting organizations with wireless networks at a higher risk. These organizations were caught unprepared for BYOD in that the upgrades and requirements to improve cybersecurity were not on their roadmap nor in their budget. A large organization with a large network is not necessarily more at risk than a smaller network if "they have very dynamic leadership" (P7). A smaller network, however, can have a higher risk due to insufficient funding. In summary, P7 saw most cybersecurity strategies for venues as striving for executive buy-in and agile leadership and having end-user buy-in.

Cross-Case Analysis

Once the researcher fully understood and analyzed each case, a cross-case analysis helped develop further concepts, categories, and themes that emerged consistently across all cases. The outcomes of all within-case and cross-case analyses were obtained directly from the answers provided by participant interviews, the observational researcher notes, and the publicly available documentation data collected. The data were coded according to systems thinking and deferred action theories and thematic analyses for the data that did not fall under the theoretical lenses. Coded data that did not appear related to the research question were kept for further clarification or review if needed later.

The coded data were organized into clusters and categories to link the data collection to an explanation of meaning in each case's context. Saldaña (2016) recollected Charmaz's description of coding as the *critical link* between data collection and their explanation of meaning (p. 4). Given that coded data is a researcher-created construct to classify the data for further interpretation, it was applied in this study systematically for replicability. Saldaña (2016) also referenced Vogt, Vogt, Gardner, and Haeffeke, to establish that the researcher "attributes interpreted meaning to each individual datum for later purposes of pattern detection, categorization, assertion or proposition development, theory building, and other analytic processes" (p. 4). The study data were grouped according to similarity, logical connections, and overlap.

Grouping the data allowed the researcher to view developing patterns that could emerge as themes. The first coding iteration followed the coding scheme developed mostly from systems thinking theory before the data collection. New codes were added and grouped as unexpected, and new ideas were introduced during the data collection. The coded data were then rearranged and classified during the second and third iterations to directly search for patterns in the data relevant to the research question. Several codes overlapped and were simultaneously coded in multiple cases, then placed under a common category. Lastly, the developing patterns were grouped according to the theory of deferred action as planned and deferred actions that could address emergent events. This pattern searching and arrangement process helped the researcher identify four themes related to preventing data breaches in large public venues with wireless networks.

The four themes that emerged from the data analysis were: (a) segmentation and separation, (b) compliance and policy, (c) continuous improvement, and (d) support system. These themes were directly related to the research question. Table 1 shows the themes identified in this study and each participant's contribution. Venue types were also determined to illustrate differences in perception. In some cases, participant responses may not have strongly contributed meaning to each theme but were inferred due to their actions and publicly available information. For example, P3 knew little about network security planning and monitoring but could describe how cybersecurity principles and functionality were applied at the venue. Information publicly available for P3’s venue confirmed that the network security architecture was planned, highly segmented, and subject to continuous testing.

Table 1

Themes Identified From Participants and Cross-Case Analysis

Participant	Venue Type	Segmentation and Separation	Compliance and Policy	Continuous Improvement	Support System
P1	Stadium	X	X	X	X
P2	Stadium	X	X	X	X
P3	Stadium	X	X	X	X
P4	Stadium	X	X	X	X
P5	League	X	X	X	X
P6	College	X	X	X	X
P7	Stadium	X	X	X	X

Note. All participants were given pseudonyms (i.e., P1, P2, P3, …) to protect the privacy of individuals. All venues refer to cases, which were also abstracted for the protection of privacy.

Table 2 identifies patterns that led to themes as represented by the participants. The participants viewed these themes as necessary cybersecurity strategies to prevent data breaches on the wireless networks at the venues. Patterns were developed from meanings attributable to each coded datum. Table 2 also contains data from the researcher's notes. The researcher notes were used to capture tacit responses and to highlight meanings that stood out. The following sections contain individual descriptions and direct quotes from the participants for each of the four themes.

Table 2

Themes With Pattern Descriptions

Theme	Pattern descriptions derived from participants
Segmentation and Separation	▪ Physical and logical segmentation of the wireless network provided separation of roles and to avoid unauthorized access. ▪ Chosen to keep the wireless network separate from ones that do not adhere to the same practices and policies as their own. ▪ Authentication accounted for appropriate levels of data protection and access authorization.
Compliance and Policy	▪ Compliance with industry standards and regulatory requirements pertinent to services. ▪ Use best practices and adherence to policies and guidelines provided by sports leagues, parent companies, or state IT departments. ▪ Large public venues must follow Homeland Security policies due to location and size.
Continuous Improvement	▪ Constant shifting or replacement components of the cybersecurity program helps the venue to evolve and continue improvement. ▪ Periodic network testing helps to find security weaknesses to mitigate and learn. ▪ A continuous cycle of obtaining expert information, individual research, policy decision-making, information sharing, and involvement helped keep the systems updated while implementing best practices.
Support	▪ Executive management buy-in, as well as serious consideration of employee recommendations, help to strengthen their venue’s cybersecurity posture. ▪ Communities that support large public venues establish strategic relationships and facilitate mutual information exchange to improve cybersecurity. ▪ Wireless and security consultants are called into large public venues to address chronic or material issues related to the network and security.

Note. Pattern descriptions are based on actual participant comments.

Segmentation and separation. Segmentation and Separation emerged as the most prevalent theme. All participants used network separation and isolation techniques to a degree. As the venue's wireless network grew in size and complexity, segmentation applications also increased by scope and type. P6 had the smallest venue with a guest and a private Wi-Fi network. P1 had an extensive Wi-Fi guest network, as well as several private, location-based, tiered, and role-based networks while overlapping with the (cellular) DAS networks. Segmentation was linked to network separation by user role, political separation from undesirable networks, data sensitivity, and level of protection. It was a way to contain a data breach or other unauthorized activities. The term *separation* distinguishes between network-specific architecture and infrastructure and different access controls related to the separation of roles and authorization.

Network segmentation was linked to logical network separation attributable to virtual local area networks (VLANs) and physically separated networks. P1 associated VLANs as "a lot of layers of security … some storage segmented" and segmented by location. When connected to the guest network, "you move directly to the Internet [skipping] routing and switching" (P1). Guests in specific areas would connect to a cellular carrier's Wi-Fi network over a segment of P1's wired network. P2 remarked, "for [fans and attendees], we provide fairly open internet access that you use at your own risk with the disclaimer-based acknowledgment." Network segments were further divided for point of sale, concession sales, events, and for each sports team.

Point of sale and concession sales require PCI-DSS compliance. P2 and P7 complied with the PCI-DSS by using more robust security and further network isolation. In some cases, physically separated networks were used instead of VLANs. P1 approached ticket sales, concession sales, point of sale, and even location-based access by bringing in Ticketmaster to take on those responsibilities. Therefore, P1 only rented the venue to the service providers. P4 also rented the venue to all service providers, remaining only responsible for several office areas, building operations, and a small guest network.

P5's wireless network during events combined the venue's guest network with the league's portable network. A section of the league's portable network was preconfigured to have the security controls to support ticket sales, point of sale, and concession sales. The league rented wired ports from the venue for backhaul connections to the Internet and other sections of the wireless network. P5 commented:

> Bringing our network to the venue, it's only plugged in for a certain amount of time. It's not like it's up for days or years or months. It's only for six or seven hours, and then we break it back down and bring it into the office.

Wi-Fi networks have a feature called AP-grouping, allowing base stations to be grouped by a configuration profile. P2 used AP-grouping as a technique to separate user access by location. Wi-Fi base stations typically broadcast a Service Set Identifier (SSID), so Wi-Fi client devices can find and connect to the base station. P2 explained:

> We also combine the factors of AP-grouping, where we don't necessarily broadcast every single SSID everywhere. There are certain areas of the ballpark where we like to dictate specific access for specific reasons, and there may be the areas where we have purposely created dead spots, for say, a public-facing area, because we are prioritizing other access needs there.

By purposely creating *dead spots*, P2 focused the wireless signals with specific network profiles to effectively create network separation. Another configuration setting that applied directly to Wi-Fi networks was to disable network bridging. P2's venue was close to a downtown area and noticed unexpected high bandwidth utilization by nearby businesses and homes. P2 and P7 could further separate their respective networks and block unwanted access by not allowing network bridging.

P2 was interested in future wireless networks. The fifth-generation (5G) of mobile (cellular) networks were designed to improve security controls in the radio access network, the core network, interconnections, and end-to-end user security. 5G was designed with many improvements over the widely deployed fourth generation (4G) mobile networks. P2 viewed a 5G mobile network as another separate wireless network, cautioning:

> 5G deployments are really being designed around private networks, 5G or CBRS networks that are designed to handle those back of house critical infrastructures, but ultimately there's nothing to say that they're more secure other than just saying that they're separate from everybody else.

5G or Citizens Broadband Radio Service (CBRS) networks have also been designed for private or commercial organizations to implement cellular-like networks. Organizations that deploy private cellular-like networks will be responsible for their cybersecurity. In P2's view, future private wireless networks should also be kept separate.

P2 was in the process of "further securing that third-party access that really can be a blind spot that most organizations don't necessarily think about heavily." P3, P4, and P5 also expressed the need for using two-factor (2FA) or multi-factor (MFA) and more encryption to further secure their networks for third parties, customers, and even IoT. P7 used 2FA and MAC authentication to admit their controlled devices onto their venues. P3 remarked that constant password changes were inconvenient and tedious but necessary for securing the multi-service network.

Segmentation, separation, and authentication are applied to all cases. Even P6's venue, which was the smallest and having only two logical Wi-Fi networks, had a complex set of access controls to admit authorized users to their corresponding areas. Even though authentication and access can often change in the short term, the segmentation and separation components can be viewed as more permanent. In a way, network segmentation and separation represent an architectural framework for a planned network infrastructure.

Compliance and policy. Compliance, together with policy, emerged as a prevalent theme. The theme encompasses industry standards such as the PCI-DSS, regulatory such as HIPAA, Homeland Security policies, and policies dictated by state agencies, sports leagues, and parent companies. Participants who did not explicitly identify *compliance* described it as guidelines or policies that must be followed. Audits were also linked to compliance since both were often described together and were inherent to verifying compliance. P1 described the importance of compliance:

> I think compliance is the backbone; then, we do our own physical part to implement that compliance of the backbone and then make sure you want to be above that compliance because you want to be better than compliance. You don't just want to be normal, complacent.

P5 remarked that compliance is essential "because of the sensitive data from the perspective of a league." Merchant data was protected in all the larger public venues through adherence to the PCI-DSS. HIPAA only had a role in P1, P4, and P5 venues due to onsite medical facilities. Moreover, P1, P5, and P7 were directly involved with PCI-DSS compliance and auditing.

Most of the participants who described compliance also described federal or state authorities that provided guidance or policies enforceable by their jurisdiction. P1, P2, and P7 identified that their venues followed the Department of Homeland Security guidelines and employee vigilance policies. The DHS also had the power to take over venue security during high-profile events. P3's venue had fired a security provider after the company had ignored state requirements. P5 added that the state protected personal data by requiring companies to comply with their policies. P4 voluntarily adopted the IT guidance given and the best practices given by a state agency even though the venue was not legally compelled.

Sports venues relied on policies established by the sports leagues. However, different sports leagues offered varying maturity levels and exerted influence based on factors such as generating revenue or other business arrangements. In some cases, such as P2, the wireless network was owned and operated by the league. In cases such as P3 and P4, the league did not own the wireless network but dictated policies because the league brought in most of the revenue. As in the case of P5, the sports league enforced PCI-DSS and HIPAA regulations.

Venues and venue management companies also enforced their policies. Participants considered their internal policies to be stricter than those of the sports leagues. As P7 articulated, "that's part of what the IT security team at my parent company does, that they make sure that we at least meet those if not exceed those." As an additional layer of protection, P2 was bringing in contractors and other third parties under the venue's policy umbrella by adding vocabulary to the contracts to hold them "to a similar set of metrics to your own employees." As a standard policy, P6 made it mandatory for newly hired employees to attend an orientation, to "provide that training so that everybody on campus has that general knowledge of best practices and things to look out for.” P7 described the desire to take new hire orientation a step further by implementing a certification program:

> I would like to implement almost like a certification for employees—a way of actually reinforcing the importance of having safety security as a mindset. I'm looking at it in terms of not only will it help them when it comes to protecting the company, but they can actually utilize this when it comes to their personal life. In terms of cellular phones, having credit cards on there, how to protect your data sets, everyone uses a mobile device. Every new hire gets a certification. It gets renewed maybe once a year or something like that.

P2 was pleased to point out that the venue's IT staff acted like a guardian driving the policies so employees and vendors would know “what they should do and shouldn’t do.” Ultimately, the venue would either be the target of a data breach or a data breach would occur at the venue. It was important for venues to protect against data breaches since it would affect all the organizations' brands. P2 also offered that there would be costs associated with data breaches, such as monetary losses, fines, but the public would remember the public relations aspects of the well-known venue.

All participants were subject to compliance and policies, regardless of awareness. In a way, compliance and policies reflected the *rules* each of the venues and types of service providers had to follow on top of the network infrastructure. These *rules* do not often change, so the rules could be adapted to address emerging trends for a few years.

Continuous improvement. All participants incorporated continuous improvement to a degree. Continuous improvement was linked to learning, training, security reviews, and security vendor and product management. Most participants studied or researched cybersecurity topics independently. Participants would obtain updated expert information from webinars, conferences, or different training types to share with their teams. P1 and P2 provided training for their teams annually, stressing cybersecurity such as protecting against spam and phishing emails, new software, recent trends, emerging threats, and policies. P2 highlighted the importance of sharing updated information to empower all employees to be responsible for cybersecurity. P7 encouraged employees to take IT and cybersecurity certifications to learn up-to-date information and would establish an employee security certification program if funds were available. Even without required certifications, venues such as P5 have provided "training mechanisms and training platforms that our staff can access and learn at their own pace" (P5). Once participants were more informed about cybersecurity, the IT staff was better equipped to evaluate and re-evaluate the hardware, software, programs, processes, and policies.

Compliance and regulatory guidelines often require planning for contingencies, such as having cybersecurity incident and response plans. P1 and P2 were involved in incident planning and identified having cybersecurity response plans in place. Executing a response plan can quickly contain a data breach and collect the information for any follow-up investigations by the FBI or state police. For example, the Department of Homeland Security requires an incident response plan for critical infrastructures such as stadiums and other large public venues (DHS, 2016). Though more specific to a venue, a cyber incident response plan provides a framework to generally plan, prepare for, and respond to cyber incidents. The PCI-DSS and other standards and regulations also require facilities to have incident response plans to be complying. Most importantly, incident and response plans provide a framework that fosters continuous improvement since plans are reviewed and updated annually.

Lessons learned were also linked to continuous improvement since knowledge drives the actions taken to make improvements. All participants offered strategic and tactical solutions to improve the cybersecurity of their respective venues. P2 did not like to depend on a single vendor for the long term and actively sought to put one vendor against another to select the best *breed* solution. Though having a single vendor would simplify management and monitoring, the product, appliance, system, or methodology used could become outdated. Also, a single vendor with a zero-day flaw could put the entire venue at risk.

P3 regarded the venue's IT architect diligence in keeping the hardware, software, and passwords up to date, as well as shortening response times to any incident, as paramount to cybersecurity. P3 added that having a mobile device management (MDM) solution would speed up making updates and providing more robust and consistent device security. P1, P3, P4, and P7 either desired or worked on gaining more control over their point of sale equipment and other devices. P7 remarked that many Wi-Fi networks could not be adequately upgraded after 2010 when BYOD was becoming popular. Multiple participants wanted to regain control of their devices after having used BYOD-like devices in their venues.

P5 advocated more league involvement to bring the outdated Wi-Fi network up to date. P6 repeatedly mentioned information sharing as the vehicle for continuous improvement. Sometimes, improvements went too far, as P7 described an incident when cybersecurity controls were so restrictive that a particular type of credit card triggered intrusion alerts, causing all its transactions to be blocked. There was some overlap between continuous improvement and authentication in that 2FA and MFA were also based on lessons learned.

Monitoring and testing emerged as a subtheme to continuous improvement. Monitoring results provided by P2's security operations center (SOC) were summarized during monthly incident-reporting meetings. In some cases, monitoring was used primarily to ascertain bandwidth requirements for capacity planning but understanding the expected network performance also helped the venue IT managers to identify devices that exhibited erratic behaviors. P1 stated, “we have about six big screens, and we have monitoring different things like the bandwidth, the Wi-Fi, statistics, the firewalls detecting anything rogue.” Periodic and ad-hoc incident reporting alerted the IT staff to problems for further evaluation. P2 described that incidents were analyzed for metrics, the number of benign incidents and instances, which ones were important or labeled critical, and their resolution. Most of the participants used intrusion detection to uncover rogue base stations or man-in-the-middle attacks. P7 would sometimes bring in a security consultant when there were not enough human resources or expertise to monitor and perform tests. P3 appropriately summed it up as: “my views are that having someone there 24/7 monitoring it is the best way that you can feel secure in that every day when I walk in, I'm not going to walk into chaos.”

P1, P2, P5, P6, and P7 conducted network penetration tests periodically. These tests would either validate that the security controls were working correctly or reveal controls requiring attention. P1 and P7 used packet sniffers to further evaluate their respective backhaul networks and report the results to the venue stakeholders. Though it might not be directly considered *testing*, most of the participants used different firewall filters and utilities to help them keep out unwanted traffic like protocols that consumed large amounts of bandwidth or destinations inappropriate for a public environment. Other types of testing included device, vendor product testing, and integration testing in a venue’s laboratory environment before implementing it on the live network.

Participants would apply the knowledge acquired from their independent study, training, expert information, and collective experience to inform their management and formulate proposed improvements, thus inserting their recommendations into their venue's decision-making cycle. P5 was delighted to point out, "my manager and our director … were very involved in our venues, so I know they made sure on our end, we were secure." The cycle for continuous improvement is both active and dynamic. All participants were diligent and open to learning and sharing their experiences. Continuous learning is like an engine driven by collective knowledge and the funding necessary to make improvements. The next section describes the support system that augments continuous improvement and provides the funds needed to make changes and improvements.

Support system. The final theme that emerged was the support system. It was closely linked to continuous improvement in that no improvements were possible without the funding and support provided by a venue's executive management. Community support was also linked to the support system. A community can be a source of knowledge, a source for a free labor pool for direct assistance when needed, and a potential trusted source that could influence executive management to allocate funds for improvements. P1 had the funding for registration and travel to conferences and attend vendor training. Inherent to the IT staff role, management would also allow time to be spent on self-study and reaching out to the cybersecurity community, the local community, or other venues. P1, P2, and P5 had the budget for training, conferences, and other annual events focused on cybersecurity and other areas. P3 received direct training from *the boss* or IT architect when it was necessary. P2 received support from certain power users for learning and disseminating information to the rest of the venue. P2's description was:

We do have power users. I like the phrase them as, who are maybe the more tech-savvy or technical ones who will have varying degrees of interest into maybe cybersecurity, and we definitely, as an organization, will leverage them to help me know and can spread the word in the policies to the remainder of the staff.

P6's support system consisted of all the staff and the faculty at the college. The IT department aggregated, evaluated, recommended, and disseminated the collective lessons learned. P7 proudly recalled that understanding the CTO's vision was linked to getting buy-in from the CTO. P7 was responsible for multiple venues and was able to compare and contrast the leadership at each location.

Nearly all participants identified the support system to be an integral part of improving cybersecurity. Executive support was especially important because they provided the funding to make improvements in incurring costs. As described by P7, sometimes executives had to defer proposals for cybersecurity improvements to activities that generated revenues, which were always a higher priority. Overall, the support system could be viewed as the *fuel* that powers the engine of continuous improvement.

Summary

This research study's findings were consistent with the research purpose: to address the problem by uncovering effective strategies to reduce the risk of data breaches. Using a multiple case study research methodology helped the researcher understand themes for effective strategies from the collected data. Data collection and subsequent triangulation analysis included interviews with cybersecurity managers and influencers with semi-structured and open-ended questions, analyzing themes according to the extant literature, reviewing publicly available information on the Internet, and using researcher notes. The participants were from large public venues that operated wireless network infrastructures in the United States. In-depth knowledge obtained from each case and subsequent cross-case analysis helped the researcher develop insight into effective strategies, development, implementation methods, and prioritization for applying strategies.

The four major themes that emerged from the data analysis were: (a) segmentation and separation, (b) compliance and policy, (c) continuous improvement, and (d) support system. The themes were directly related to the research question. Segmentation and separation represented a planned architectural framework. Authentication emerged as a sub-theme to segmentation and separation. Authentication served as a mechanism that would ensure users authorized access to specific network segments. Compliance and policy emerged as the rules venue operators must follow on top of the network infrastructure. Continuous improvement emerged as the engine that informs and drives change and improvement. Monitoring and testing emerged as a sub-theme to continuous improvement. It represented active measures venues would inform the effectiveness of their processes and validate devices and equipment that can meet the venue’s cybersecurity guidelines. Lastly, the support system reflected the need for executive buy-in to fund the changes and improvements necessary to reduce the risk of data breaches.

CHAPTER 5. DISCUSSION, IMPLICATIONS, RECOMMENDATIONS

The purpose of this qualitative, exploratory, multiple case study was to uncover effective strategies to reduce the risk of cybersecurity data breaches of wireless IT network infrastructures at large public-event venues. This chapter aims to assess how well the research findings address the research problem and provide recommendations for future studies. Chapter 5 is composed of a summary of the results and a discussion of the results of the data analysis. Following are conclusions based on the results considering previous literature and the broader community of interest. The next section discusses research design problems or limitations to identify improvements, followed by the implications for theory and practitioners. Recommendations for further research are then provided. The final section contains the conclusions of the study.

Summary of the Results

The need for the study was that wireless IT network infrastructures at large public venues are subject to an increased risk of data breaches, which continues to grow in frequency. The literature review provided a broad perspective on cybersecurity research in large public venues and wireless networks. Large public venue wireless networks exposed to large crowds can make them more susceptible to data breaches in increasing frequency and reoccurrence before discovery (Mitra, 2016; Nazareth & Choi, 2015; Schatz & Bashroush, 2016). Data breaches can also damage the vendor's reputation and the entire market (Gerard, 2016). Newer wireless network technologies, such as private LTE, have vulnerabilities inherent to the standard and are subject to variable implementation practices (Raza et al., 2017; Shaik et al., 2015).

The significance of this study to cybersecurity is to add to the existing body of knowledge information on cybersecurity strategies for security practitioners, stakeholders, and those who do not specialize in cybersecurity, to make more informed decisions relative to large public venues with shared wireless networks. No known studies have been undertaken to identify what cybersecurity strategies are used and developed in a large public venue setting. The cybersecurity strategies uncovered in this study reflect current cybersecurity trends for preventing and mitigating data breaches in large public venues.

A qualitative research methodology was used to uncover how or which strategies persons responsible for cybersecurity use prevent or mitigate data breaches in large public venues with shared wireless networks. The stated research question: What are effective strategies large public venue operators use to reduce the risk of data breaches in their wireless networks during and between venue events? Interviews were conducted using a case study design to answer the research question practically. The case study design was exploratory and holistic because, according to Yin (2017), a theoretical lens was used to focus the research and examined an organization in its entirety as a single unit of analysis. The unit of analysis was the large public venue.

Four major themes emerged from this study's data analysis: (a) segmentation and separation, (b) compliance and policy, (c) continuous improvement, and (d) support system. The themes answered the research question. Segmentation and separation represented a planned and mostly static architectural framework. An authentication subtheme served as a mechanism to permit authorized access to network segments. Compliance and policy represented the long-term rules venue operators adhere to avoid penalties and achieve corporate objectives. Continuous improvement informs large public venue operators about needed changes. A monitoring and testing subtheme informs the venue operator on the effectiveness of the measures taken to address cybersecurity issues. The support system reflected on obtaining funding to implement the changes and improvements that would reduce the risk and impact of data breaches.

Discussion of the Results

This study used a qualitative case study design to investigate data breach prevention strategies in contemporary large public venues using multiple analysis levels. The research question for this study was: What are effective strategies large public venue operators use to reduce the risk of data breaches in their wireless networks during and between venue events? The study answered the research question by providing a rich set of cybersecurity strategies specific to preventing data breaches on large public venue wireless networks and applying them to many other types of organizations and locations. The cases involved represented several large public venues, allowing identification of rival explanations to help determine the strategies' effectiveness.

Each case was defined by a large public venue operating a wireless network, specifically during hosted events. A knowledge gap exists between small businesses and large public venues, which, though similar in staffing size, have different operational characteristics that increase large public venues' vulnerability with wireless networks. The findings were examined using the theoretical lenses of systems thinking and deferred action theories. The findings were also examined in the extant literature to determine where this study fits the research body and make recommendations for further investigation.

While many wireless network operators may be aware of data breaches' pervasiveness and the likelihood of incidence, large public venues with shared resources face a higher risk. Data breaches are well-known but often misunderstood (Borum et al., 2015). Data breaches continue to occur at a growing rate (Dhameja, 2015; Giorgio, 2018; Ullah et al., 2018). Data breaches also appear to be more frequent and more destructive (Gunzel, 2017). Large public venues with shared wireless networks often have undersized IT staff. Large public venues are more vulnerable with characteristic large attack surfaces, wireless vulnerabilities, high-density usage, and greater physical security. The dense environment, proximity to other wireless networks and facilities, and lack of control over guest handsets further increase the risk of a data breach (Hagos, 2016; Kim et al., 2017). Several participants used segmentation techniques to reduce complexity and effectively isolate their wireless networks from others and guests.

From the literature review, data breaches can also damage vendor reputation and the entire market (Gerard, 2016). The study data confirmed a damaging reputation to the venue and the sports league. Newer wireless network technologies, such as private (cellular) LTE, have vulnerabilities inherent to the standard and are subject to variable implementation practices (Raza et al., 2017; Shaik et al., 2015). P2 assumed future wireless networks would be kept isolated from existing networks, thus mitigating potential defects and variable implementation practices. Much of the research on intrusion protection and detection uses smart automation with marked improvements in false positives and false negatives (Loukaka & Rahman, 2017; Shenfield et al., 2018; Veeramachaneni et al., 2016; Zulkefli et al., 2017). Participants who relied on active monitoring were unaware of the details of the heuristics or algorithms used by their IDS/IPS systems.

One implication from the extant literature is that large public venues with shared wireless networks will continue to grow the attack surface while data breaches' frequency increases. Secondly, damages caused by data breaches go beyond monetary value and may not be fully accountable. Participants described potential damages that could include loss of personal data, brand reputation, diversion of resources, the diminished ability for police surveillance, and even coach information that may include medical records. A third implication is that technological advances may fall behind data breaches, increasing in frequency if the countermeasures are not actively implemented periodically. *Continuous improvement* emerged as a theme that describes a cycle of active learning and ideation for improvements that would counteract the increased frequency of data breaches.

The literature review also resulted in three common themes: (a) wireless networks are mainly vulnerable to man-in-the-middle (MITM) and evil-twin attacks; (b) large public venue wireless networks can be complex and play a part in a broader operational complex ecosystem; and (c) given there are several available standards and frameworks to help organizations apply cybersecurity strategies, much reliance is placed on intrusion detection accuracy within device performance constraints. While this study's findings may not directly address wireless vulnerabilities, participants had consistent responses that address every theme taken from the literature review.

Participants implicitly addressed wireless network vulnerabilities. Most of the participants reported that their venue monitored several wireless network aspects that included an intrusion detection system (IDS). IDSs can potentially detect MITM and evil-twin attacks. However, these attacks are difficult to detect and subject to much research (e.g., Nasr et al., 2019; Vijayanand et al., 2018; Xie et al., 2018). Several of the participants also conducted network penetration tests, which can identify vulnerabilities that attackers might exploit. There was no indication of the efficacy of the monitoring and testing techniques used from the study data. It is likely that participants were unaware of the threat posed by MITM and evil-twin attacks or were not responsible for those types of attacks.

All participants described the complexities of operating a wireless network infrastructure at a large public venue and their dependency on an ecosystem that also functioned as a support system. Systems thinking theory helped break down the uncovered complexities by separating functions, structures, and processes into components and their influence on each other. For example, descriptions of the venue environments revealed the type of wireless network, network size, overlapping networks, IoT devices, and areas of responsibility. Some of the participants regularly contacted the managers of the overlapping networks to coordinate efforts (i.e., P2 and P3). Others met regularly with the local community members for information exchange, guidance, and even direct assistance when needed (i.e., P1, P2, and P7). Even Case 6, a college, depended on support from nearby colleges to prevent and address cybersecurity incidents. From the findings in this study, the theme of a *support system* emerged as help available from different sources to inform venues about incidents experienced by like facilities in the local community. However, the most essential and critical support came from a venue's executive management that would fund cybersecurity-related changes and improvements.

Most of the participants identified being compliant with the PCI-DSS. Several also adhered to the Department of Homeland Security guidelines and policies. Both require or recommend venues use an intrusion detection system (IDS) or techniques, which often fall under monitoring and testing. An IDS can be defeated by encryption since fingerprinting cannot match a pattern in a packet's payload that is encrypted. The accuracy of an IDS to avoid false positives and false negatives depends on training traffic data and the algorithms used. IDS and its accuracy remain the subject of much research as it is with MITM and evil-twin attacks.

Fulfillment of Research Purpose

The purpose of this qualitative, exploratory, multiple case study was to uncover effective strategies to reduce the risk of cybersecurity data breaches of wireless IT network infrastructures at large public-event venues. To achieve the purpose, participants needed to have the knowledge, influence, or possibly be decision-makers. This study achieved the stated research purpose by uncovering several cybersecurity strategies. Furthermore, a common framework emerged that could uncover issues and make improvements in large public venues with wireless networks.

Because of the low incidence of reporting data breaches, few participants were likely to admit to experiencing a data breach. A lack of reporting was expected and turned out to be true in this study. The researcher verified that none of the participants had direct knowledge of a data breach at their venue. P1 described a long-term coworker who had experienced a data breach for over 10 years since a network architect was hired to drive several cybersecurity improvements. Coincidently, the network architect purchased over $2 million in firewalls to segment the network highly. All participants referred to data breaches and other cybersecurity incidents as secondary information or described them hypothetically. The researcher viewed avoidance of a data breach disclosure as protecting the organization’s reputation and brand.

Conclusions Based on the Results

An implication of this study to the broader communities of interest, such as large businesses, city telecommunications commissioners, colleges, or smart community planners, is to inform which cybersecurity strategies are practical and applicable to facilities like large public venues. Also, large public venues with wireless networks may operate with similar types of relationships and communities of interest that can influence the adoption of cybersecurity strategies.

The theme of s*egmentation and separation* drew on systems thinking theory to decompose several methods for isolating users and managing access to wireless networks while drawing on deferred action theory to exhibit its planned nature. *Compliance and policy* drew on systems thinking theory to derive the set of rules a venue must or should follow while serving as a source for applying best practices. The theme of *rules* drew on the theory of deferred action to address long-term emergent trends. *Continuous improvement* drew on systems thinking to reveal cyclical processes built on the two previous themes to generate proposals for improvements and influence change. In turn, the improvements drew on the theory of deferred action to identify dynamic changes that address short-term emergent events. The *support system* drew on systems thinking theory, highlighting the importance of funding while drawing on the theory of deferred action to link funding for planned systems and emergent events.

Yin (2017) indicated that the researcher seeks convergent evidence regarding the findings and conclusions for each case in a case study. It was during the cross-case analysis that the evidence converged on the findings. Generally, there were similar results from the different case studies, where conclusions drawn from each of the cases replicated the information from the findings. Rather than achieving contrasting results such as efficacy between venues that adhered to DHS critical infrastructure guidelines versus none, the maturity of the cybersecurity continuous improvement cycle and executive buy-in had a more significant impact. The information obtained from all seven cases was consistent and strongly reinforced theoretical predictions. Based on Yin's (2017) guidance and an understanding of theoretical predictions from this study, the estimated five or more cases achieved data saturation. The seven cases recruited for this case study achieved data saturation.

Yin (2017) stated it is useful to indicate a proposition when designing research to help reflect on critical theoretical issues and where the researcher should look for relevant evidence. The researcher used results from prior research and the literature review to develop the following propositions: (a) cybersecurity strategies can be considered effective at a large public venue with a wireless infrastructure if the venue has never had a data breach; (b) for cybersecurity strategies to be effective, cybersecurity managers are required to have implemented a plan to protect information assets; (c) if a data breach occurs in a large public venue with a wireless infrastructure that has established cybersecurity strategies, the time to detect and recover is less than a recent trend of 30 days; and (d) if a data breach occurs in a large public venue with a wireless infrastructure that has established cybersecurity strategies, the monetary and brand impact is minimal. The rival explanations are: (a) organizations that do not have or apply cybersecurity plans may never have a data breach; and (b) organizations that have a static wireless network, with security controls put into place during deployment, may never experience a data breach.

The empirical data did not address Proposition 1 because no one reported a recent data breach. This result is consistent with LiCalzi (2107), in which data breaches often go unreported. Proposition 2 relates to all cases in that all followed guidelines, policies, and applied best practices to protect their information assets. Even Case 6, a college rather than a sports venue, exhibited a planned cybersecurity approach. Though the venue had a smaller and simpler wireless network, it had more IT resources available than the sports venues taken individually. Proposition 3 fits the empirical data in that an established monthly security review is more likely to catch a data breach if it has occurred within 30 days.

By systematically reviewing metrics, incidents, and criticality, cybersecurity teams are more likely to detect a data breach. Cases 1 and 2 had detailed and structured monthly incident reviews; thus, there was a high likelihood of catching a data breach within the 30-day period. Proposition 4 applied to all the cases. However, none of the participants reported a data breach that could be evaluated for mitigation or containment effectiveness. All employed planned and highly segmented wireless networks with strong access controls. One description given about Case 3 was that the "stadium's vast Wi-Fi network has been sliced 'n' diced into a series of smaller Wi-Fi networks that, presumably, will each work independently and dependably" (P3).

The part of the research question attributed to the *effectiveness* of strategies can also be addressed by selecting a case that can draw from rival explanations to the study's propositions. A rival explanation can affect the study and is analogous to having a control group in an experimental study (Yin, 2017). In this study, Case 6 was a small college that rented several facilities to the public. It had a small Wi-Fi network that provided services to two major groups, guests and employees. Also, the staff size was larger than the other large public venues studied. In some ways, Case 6 was like an enterprise Wi-Fi network.

Though the theme of *compliance and policy* did not appear as strong as the other cases, all of the themes that emerged from this study applied to Case 6. P6 also stood out from the other participants by putting information exchange and collaboration at the forefront of a cybersecurity strategy. P2 and P7 also mentioned collaboration, but not to the degree of P6. Comparatively, P6 also had a lesser role in cybersecurity than most participants. When weighing the differences and similarities between Case 6 and the other cases, Case 6's cybersecurity strategies were not substantially different. All cases replicated the information from the findings.

The information gathered from the sample population was the number of years in the business, the job role, and the time in the current position. The number of years in the business helped to get an idea of the maturity and expertise. The job role and subsequent description helped to understand the IT organizational structure, its relation, and influences, and cybersecurity responsibility. The time in the current position helped to understand the level of knowledge attributable to this study's topic.

The summary of the findings comprises four main themes that developed into a conceptual framework. The themes that emerged from this study were (a) segmentation and separation, (b) compliance and policy, (c) continuous improvement, and (d) support system. *Segmentation and separation* refer to establishing a type of infrastructure upon which authorized users are granted access based on any one or combination of attributes. A highly segmented network reduces complexity and makes its size irrelevant for cybersecurity. *Authentication* emerged as a subtheme that addresses access controls primarily. *Compliance and policy* refer to the rules venues, and venue vendors must follow to ensure programs and controls are in place for self-protection and that of the customers. Venues rely heavily on compliance and cybersecurity frameworks for delivering services. The creation of incident response plans and periodic audits must also become compliant with standards and policies.

Continuous improvement refers to an active and dynamic learning cycle that generates ideas and proposals that will, if applied, strengthen the security posture of a venue. Given that there are always evolving cybersecurity vulnerabilities and exploits, venues should always support learning from multiple sources, including testing the network. *Monitoring and testing* emerged as a subtheme that generates field evidence. *Support system* refers mainly to funding continuous improvement and additional sources for obtaining information to generate the ideas for continuous improvement. It is easier to gain executive buy-in if an IT department generates revenue. Figure 2 illustrates a framework based on the interpretation of the findings.

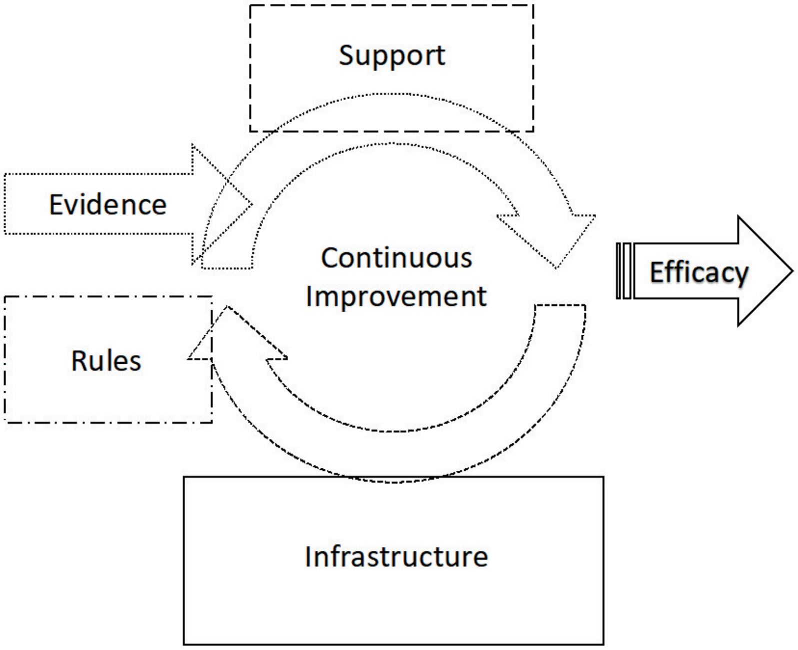

Figure 2. Effective strategies based on systems thinking and deferred action theories. Framework elements were derived from systems thinking theoretical concepts. Actions, such as continuous improvement efforts, were derived from deferred action theory planning design concepts for emergent events.

The results of this study add to the existing body of knowledge by providing information on cybersecurity strategies applicable to large public venues with wireless networks. No known studies have been undertaken to identify what cybersecurity strategies are used and developed in a large public venue setting. The cybersecurity strategies uncovered in this study reflect current cybersecurity mitigation trends and reveal a framework for identifying and generating future cybersecurity improvements in large public venues. When designing a wireless network for a large public venue, planning for high segmentation provides the foundational infrastructure to support venue operations securely. This study revealed a framework that venue operators could adopt to help them create cybersecurity policies and practices and make informed decisions. The process demonstrates how different elements influence each other when tailoring cybersecurity solutions for a venue. This research may raise awareness of cybersecurity trends and communicate a process for cybersecurity practitioners in large public venues.

New and unique knowledge being added is a framework that reduces complexity in large public venues and empowers cybersecurity practitioners to engage in continuous cybersecurity improvements actively. Although frameworks already exist for critical infrastructures and IT security in general, the large public venue IT framework (LPV-ITF) from this study specifically simplifies the large public venue setting and equally applies to non-cyber security-related IT.

A practical application of the research findings is to make available specific and easy-to-understand processes to venue operators. Practitioners who adopt the large public venue IT framework (LPV-ITF) may find a more significant benefit from later adopting frameworks such as the Department of Homeland Security Critical Infrastructure Commercial Facilities Sector-Specific Plan, ITIL, or NIST. The LPV-ITF could be viewed by non-IT venue staff to understand how non-IT staff and the venue management fit into the venue ecosystem. Cybersecurity practitioners can effectively communicate with non-technical staff the need to employ cybersecurity improvements and show how those improvements add value and contribute indirectly to the large public venue. The LPV-ITF can function as a practical tool for identifying necessary cybersecurity improvements and communicating evidence-based information to obtain the funds for implementation.

Extraordinary information provided by the data analysis is the development of a conceptual framework. At one point, the coded data was organized into eight discrete categories or themes. However, using the deferred action theory lens helped organize the themes into themes and subthemes that naturally fell into place. These themes were organized into categories that would be part of the planned infrastructure, reflecting segmentation and separation as the most permanent component. *Compliance and policy and continuous improvement* followed as the ability to address emergent events. The support system theme emerged as a moderating or enabling function that is integral to the entire process. Up to that point, the researcher was going to report segmentation, multi-factor authentication (MFA), device control, and executive buy-in as the cybersecurity strategies used by large public venues. Though untested, the LPV-ITF was developed logically from the study data and should simplify the influences and requirements for large public venue network cybersecurity and wireless network security.

Comparison of the Findings With the Theoretical Framework and Previous Literature

All the themes resulting from the study draw from the systems thinking theoretical lens. Application of systems thinking theory to the empirical data reduced complexity in the large public venue environment, allowing the researcher to break down functions, structures, and applying cybersecurity strategies. Under the systems thinking theoretical lens, emergent themes were also represented by their influence on other components of the venue system and by sub-themes. The study's themes also draw on the deferred action theoretical lens to group actions that are planned, or mostly permanent and actions that result from a feedback loop to address emergent events.

Findings that differed from the researcher’s expectations were a lack of data on wireless-specific vulnerabilities except for rogue base stations and a lack of data on Wi-Fi-specific strategies or even mechanisms other than the threat of rogue base stations. None of the participants mentioned man-in-the-middle (MITM) or evil-twin attacks. The literature review identified both attacks as significant exploits that impact wireless networks. When considering that perhaps IT managers place the responsibility of those attacks on the equipment manufacturers or security operations center (SOC) intrusion detection systems (IDS), the result could be that some significant vulnerabilities may be overlooked.

Except for mentioning the existence of an intrusion detection system (IDS), conducting network penetration testing, packet capture, and analysis, no study data could be directly linked to those types of attacks. Suppose IT managers are unaware of the pervasiveness and the threat of MITTM and evil-twin attacks pose. In that case, there is value in informing IT managers of large public venues to take measures to address those vulnerabilities. IT managers may ignore these attacks due to a lack of training and a lack of specialized equipment. IT staff may not likely view the attacks as likely to occur or likely to have a high impact on the venue. From the perspective of responsibility, those types of attacks are left to third-party experts such as a security operations center (SOC), or it might not be considered an IT issue altogether.

Lacking data on Wi-Fi-specific strategies could result from a protectionist behavior typical of IT managers who may not want to disclose cybersecurity details about their venues. However, being a common theme among all cases, it may appear the IT managers and staff in the study were not directly responsible for evaluating and implementing measures such as WPA3 nor upgrading Wi-Fi networks to the latest standards. The responsibility may belong to IT network architects, which were not in this study's target population.

In general, the literature review and the findings match, though there is a gap between the focus of research on wireless-specific vulnerabilities and participant awareness or responsibility. An example of the gap is that none of the study data addressed the relationship between wireless networks and susceptibility to data breaches.

Interpretation of the Findings

This research study complements Saber's (2016) research by highlighting the importance of having internal policies to ensure responsibility for the data even if it is offloaded into the Cloud. Also, large public venues have relatively small IT staff, which is comparable to small businesses. Many of the decisions a venue non-revenue producing IT staff face have costs associated with which there may not be funds or considered necessary. Small businesses face similar challenges. Employee training is also vital to both venues and small businesses. Both venues and small businesses must have up-to-date information to improve internal behavior, processes and learn about new technologies. This research differs from Saber's (2016) research in the setting, in which a large public venue can contain several small businesses, adding complexity. The complexity and scale of a large public venue vastly differ from a small business office setting. An implication is that a venue IT infrastructure may not be as agile as that of a small business, forcing long-term planning requirements.

This study's findings support existing research by stressing cybersecurity training and learning, outsourcing network security device testing, or experimentation for devices. Large public venues and small businesses benefit from regular cybersecurity training. Saber (2016) concluded that small business leaders should foster a cybersecurity culture by offering training programs for themselves and their employees. This study’s data agrees with training and adds self-study as a standard method for learning about cybersecurity incidents supported by management because it could affect the venue. Saber (2016) and Nero (2018) supported outsourcing of network security, placing the experts in charge of monitoring and mitigating cybersecurity issues. The study data support using a security operations center (SOC) to leverage their expertise and become more effective in catching a data breach within a 30-day period.

Nero (2018) recommended identifying decision-making criteria and factors when hiring a third-party IT security provider. The study data provide insight into focusing on measures that mitigate specific risks to the environment. For example, P2 required best-in-breed technologies and used a replacement cycle approach to eliminate vendors who could not keep up with the changing cybersecurity landscape. Nero (2018) also recommended engaging larger businesses to understand decision-making factors that would influence a broad IT network outsourcing industry. In this study, large public venue wireless networks and their service providers or owners provided insight into some factors that can influence a broader scale. The owner and operator of P2's network used the collective experiences and best-in-breed technologies to make decisions for continuous improvement of its program and resulting overall security posture.

Kamin (2017) concluded that device testing or experimentation is necessary with IoT devices due to the many unknown cybersecurity factors. The study data agree that device and equipment testing should be conducted in a laboratory environment before deployment. *Segmentation and separation* techniques appear in the research in the form of access controls. *Compliance and policy* matched Patterson's (2017) focus, referring to continuous evaluation and policy decisions. The findings in this study agree with and support the existing research.

The following is a summary of learning from this research study. This study's first learning is that the missing study data pointed at a gap in addressing wireless-specific vulnerabilities. That result led to much speculation as to the reason why. A related perspective that emerged is that large public venues view wireless networks, mostly Wi-Fi, as a network operating at the logical link layer. Wireless networks are not primarily wireless networks with a wired backhaul but are treated as a wired network with a small segment attributed to the wireless medium. An implication is that the wireless medium would remain mostly ignored. The lack of data supports that interpretation.

The second learning is how the prevalence of segmentation and separation applies to every case and divides networks according to the physical, logical, political, role, location, and data sensitivity. A physical network can be separate Wi-Fi networks with no coexistence mechanisms or be separated by technology such as a Wi-Fi network next to a mobile (cellular) 4G LTE distributed antenna system (DAS) network. A logical network is separated by virtual local area networks (VLANs), often treated as security mechanisms. However, VLANs were originally designed to control the broadcast traffic in a local area network (LAN). Political separation results from ownership or influence, such as a football league that generates large revenues. Owners of different Wi-Fi or DAS networks may feel no obligation to owners of neighboring networks. Different network operators may have different timelines for cybersecurity updates or may abandon upgrades altogether. P4's data supports a lack of cooperation between large Wi-Fi and DAS providers.

Separation by role is access control based on the user profile. It is likely to be the most often used separation technique since it is pervasive and requires minimal effort. P2 described separation by location as not broadcasting access to a network in certain areas to create a *dead spot* where guests are not allowed. Separation by location is commonly used in planned Wi-Fi networks. The sensitivity of data determines storage and security mechanisms for certain types of data such as medical, purchase, or personally identifiable information (PII). Segmentation and separation cover a broad range but is foundational for shared infrastructure.

The third learning is that device control appeared as a trend. To have robust security and consistent user experience, IT departments use device control systems. One type of device control is a mobile device manager (MDM), which manages security such as certificates and enforces password or biometric device policies. Older building control systems can benefit from device control since many may have been in use for decades with few security mechanisms or updates. The point of sale and tablets used for merchandising can also be brought under a device management platform. One participant wished to have device control over guest smartphones. Companies often push policies to BYODs to exercise limited control over the corporate data and employee behaviors. However, the device control from the study data appears to be for total control for venue-owned devices, including asset management and protection against loss or theft. Having device control often requires testing to certify that the device is secure and provides a good user experience.

The fourth learning is to use multifactor authentication (MFA) whenever possible. It applies to venue private and secure networks used by anyone except guests. Guests can benefit from MFA, but it would be expensive and difficult to manage on a large scale. MFA can be enabled over-controlled devices easily, without the need to program every device manually.

The last learning described is to have executive buy-in for making cybersecurity improvements. Whenever several proposals are being considered, it may be necessary to rank them according to the impact or other funding criteria. Evidence-based information from testing, research articles, or local community support may help convince the venue leadership about the value of preventing data breaches or increasing revenues because of the changes.

Learning from this study can apply to large business IT managers, municipality or city telecommunications commissioners, colleges, smart community planners, and service providers for recurring temporary events like festivals and concerts. The LPV-ITF can be used to tailor cybersecurity improvements to their facilities. One of the proposed benefits of the LPV-ITF is that it simplifies large public venues into infrastructure planning, purpose and use of applicable rules, a learning and improvement cycle, and getting the support to ensure successful improvements.

This study yielded findings consistent with Saber (2016) due to a close replication of systems thinking theory, case study design, a similar line of inquiry for participants, a focus on characteristically small businesses, and the use of thematic analysis. Similarly, this study replicated Maahs' (2018) application of systems thinking theory and case study design. Although Nero (2018) did not apply systems thinking theory, the data analysis included thematic analysis. This study also achieved a sample between Saber (2016) and Nero (2018), further reinforcing outcomes with detailed descriptions, consistent analysis, and findings that are more likely to be reproducible.

As a theoretical lens and analysis tool, systems thinking theory turned out to be a powerful cybersecurity modeling tool for finding, characterizing, understanding, evaluating, and predicting cybersecurity, as described by Edgar and Manz (2017). The application of deferred action theory complemented systems thinking, which offers corrective measures, with a design planning perspective that adds preventative measures. Khan et al. (2010) describe that deferred action helps in understanding how processes and tools can be developed using plans and contingencies to meet current and emergent events. The research study further benefited from the complementary information derived from systems thinking and deferred action theories.

Limitations

This study was conducted with a limited budget and time constraints. Time constraints were due to full-time employment while a student and due to unexpected events, such as multiple deaths in the family. Acceptable university research methods are also defined based on the feasibility of time, access to resources, and available mentoring expertise. As a novice researcher, acceptable writing skills, lack of document organization, delays in obtaining IRB approval, changing the sampling frame (LinkedIn to a research agency), and referencing incorrect dissertation chapter guides, contributed to delays. Also, the sample population was defined initially too narrowly to reach practically. Even attempts to use snowball sampling to recruit participants were ineffective.

A delimiter originally applied to collegiate and lower-division sports stadiums. It would have been beneficial to include the venues, as the cybersecurity issues are similar and can be equally as complex as professional sports stadiums. Expanding the sample population to collegiate and lower-division stadiums would also have addressed the narrow definition initially proposed in the study.

Implications of the Study

This study was needed to help CIOs, cybersecurity managers, and even non-IT persons who operate large public venues to have the opportunity to be informed about the likelihood their venues will suffer a data breach and to help them to strengthen the cybersecurity posture of their IT organizations. This study also determined which strategies significantly affect a large public venue with a shared infrastructure for a higher return on investment. This study related the current literature as a culmination of the available strategies, discoveries, and applications as a set of strategies to assist CIOs and IT managers with cybersecurity responsibilities of large public venues in preventing data breaches.

This study indicates that large public venues with small staff sizes have more considerable resources than small businesses with similar size IT staffing. Large public venues and small businesses have similar cybersecurity and business continuity requirements. Growing businesses can benefit from cyber and business continuity planning as their attack surface is also likely to increase. In one case study, offsite backups were offered as a measure to prevent data breaches. IT research on small businesses can contribute to large public venue research and vice versa.

Another result from this study reinforces compliance as a baseline for security and policy creation as important for cybersecurity and business continuity. For example, to comply with the PCI-DSS, businesses must have an incident response plan and conduct periodic reviews. Periodic reviews and audits can lead businesses to identify improvements and prioritize the proposed changes. Monthly reviews of incident reports can even lead to catching data breaches early, which often last longer than 30 days, as iterated by Schatz and Bashroush (2016). Large public venues or their vendor businesses adhere to the PCI-DSS, DHS policies, state policies, and internal corporate policies, which are often stricter than any single program.

Medium and large businesses are likely to implement high-capacity wireless networks. As part of business operations, medium to large businesses may have to provide guest access, process merchant data, electrical device controls, and IoT for building operations. Since a data breach is a business technical problem, results from this study offer planned segmentation techniques, compliance, and device testing as measures to increase cybersecurity. Businesses of different sizes can benefit from the knowledge and application of effective strategies in data breach prevention.

The application of multiple strategies can potentially reduce the effects of the long-standing data breach problem. By focusing on IT managers who influence cybersecurity prevention of data breaches, this study's results advance the research in IT.

Increasing cybersecurity data breach incidents in large public venues is a business problem because of the loss of privacy information, loss of credit card data, fines, loss of organizational credibility, and market credibility loss. The study data supports several matching personal and business losses. Even personal losses can affect organizational credibility and the market, such as a sports league. A data breach in the network could lead to attacks on the corporate network or individuals compromising their personal information, leading to an eroding brand reputation (Wang et al., 2016). The study data support loss of reputation, public relations issues, or embarrassment.

CIOs and cybersecurity practitioners entrusted with financial, human resources, and policy-making decisions add value to customers who align with the IT organization’s information assurance and business objectives. The study data support that security and IT trained executives readily create stricter internal policies than those afforded by compliance and external policies to revenue values. The study helped the researcher uncover effective strategies to help large public venue owners, CIOs, and cybersecurity practitioners have a stronger security posture. By using an effective security strategy, CIOs and cybersecurity practitioners who read this report will likely be able to create social change to achieve increased revenues, higher savings, and maintain credibility with their customers within markets served by large public venues.

Recommendations for Further Research

Recommendations Developed Directly From the Data

A recommendation for further research is to perform a quantitative study that surveys CIOs, CTOs, CISOs, league or venue owners, and other decision-makers on cybersecurity in general. Knowledge and effects of data breaches can be embedded with different types of vulnerabilities and threats. By asking about a cross-section of vulnerabilities and threats, anonymous respondents would more likely reveal their experiences. If most data breaches remain unreported, then a survey will likely draw out positive responses without perceived repercussions. An understanding of the relationship for decisions for reported and unreported data breaches can benefit the broader IT community by informing on motivations surrounding decisions relevant to protecting against data breaches.

Recommendations Derived From Methodological, Research Design, or Other Limitations of the Study

There should have been no need for snowball sampling, which is often reserved for difficult populations to identify and contact. Snowball sampling can fail when researchers are perceived as outsiders or when the research topic is considered sensitive or problematic, subsequently considered too risky by potential participants (Parker, Scott, & Geddes, 2019). A difficulty with snowball sampling is that subjects that would make referrals may not fully understand how those hard-to-find traits apply to the study (Parker et al., 2019). In this study, the researcher sought cybersecurity professionals in an area where cybersecurity is not the primary security concern. Those charged with operating large public venues and critical infrastructures are primarily concerned with the staff and event attendants' physical security and health. Cybersecurity can be a secondary or tertiary consideration (Hassan, 2016).

A methodological improvement that can strengthen the study is to limit the empirical data analysis to two or three most appropriate techniques. This study deals with strategies and processes on how to find or develop the strategies. Systems thinking theory is an appropriate theoretical lens to find how one process or function influences another, especially if most functions can be mapped (Ing, 2013). The theory of deferred action is an appropriate theoretical lens to use when goal-oriented planned and contingent approaches enable solutions with feedback loops to withstand long-term emergent events in changing environments (Khan et al., 2010). Another appropriate analysis method is thematic analysis, which requires the researcher to use expert knowledge and judgment to derive themes from the empirical data (Saldaña, 2016).

Once the design, sampling, and methodological improvements are made to this study, it should be replicated as a longitudinal study. Wireless networks are often refreshed every three to five years. A longitudinal study conducted at the same venues three years into the future will highlight the most effective long-term cybersecurity strategies.

Recommendations Based on Delimitations

If this study were to be replicated, a suggested improvement based on delimitations is to establish a broader population that could inform the study during the proposal stage. In this study, the researcher started with such a narrow focus that there seemed to be little room left for potential participants to agree to the study. The researcher speculates that asking potential participants to reveal their cybersecurity *secrets* in an interview setting may create distrust and cause the subject to decide not to participate in the study. While none of the potential participants recruited via LinkedIn offered reasons for not participating, most participants in the study appeared to guard detailed information about their venues. The sample population should have included persons who are likely to possess knowledge of cybersecurity planning or application.

The sample population may have consisted of venue operators, service providers to the venue with whom the venue operator would have consulted on cybersecurity, or the venue's wireless network users. Some potential participants may have provided further insight for the study after having experienced contract negotiations that included terms for indemnification of cybersecurity policies and contingencies.

Recommendations to Investigate Issues Not Supported by the Data But Relevant to the Research Problem

This study observes that no responses addressed man-in-the-middle (MITM) nor evil-twin attacks, to which wireless networks are mainly vulnerable. All versions of Wi-Fi, Wi-Fi calling, 4G LTE mobile networks, and 5G NR mobile networks are vulnerable to MITM and evil-twin attacks. It is also uncertain whether IT security practitioners should address these vulnerabilities or be left to wireless engineers and equipment manufacturers. It is questionable whether it is an IT problem because it involves specialized knowledge and skills that the IT community may not easily understand. Therefore, the security of wireless networks that are vulnerable to MITM and evil-twin attacks may remain unaddressed. A research study with a target population that includes wireless engineers and IT security practitioners may adequately address that knowledge gap.

Research involving large public venues with wireless networks is likely to evolve as more large public venues are built and older venues are retrofitted with wireless networks. Several venues have dated wireless networks that present unique challenges to data security. Large public venues are a microcosm of businesses, each with specific requirements. Given this study's result that the wireless medium is mostly ignored, more attention is needed to address the vulnerabilities common to all wireless networks. Bad actors are already aware of the vulnerabilities. It is just a matter of time before purchasing the necessary equipment and obtaining the skills to attack venues, businesses, municipalities, and cities. More research is needed for IT security practitioners to be better informed regarding decision-making for cybersecurity.

Conclusions

This study identified effective cybersecurity strategies to prevent data breaches in large public venues with wireless networks. Several attributes specific to large public venues with wireless networks were considered and evaluated to provide context for each case. IT managers and IT staff with knowledge of venue cybersecurity explained their perceptions on the importance of cybersecurity and what measures were in place to prevent and mitigate data breaches.

Participants described the different segmentation techniques built into their venue infrastructure and user access to connect to the wireless network and access the services. Participants also described how compliance, frameworks, and policies provided a set of rules for daily operation and how periodic reviews and audits helped keep them updated with cybersecurity knowledge and establish incident response plans. A continuous improvement cycle provided learning to generate informed proposals for changes that would strengthen the venue's cybersecurity posture. Monitoring and testing were used for intrusion detection systems and network penetration testing to detect data breaches and find other network weaknesses. Participants described how executive buy-in is necessary to fund and drive continuous improvement in cybersecurity.

The cybersecurity strategies identified in this study were developed into a framework specific to large public venues. Segmentation reflects a planned and more permanent component whose outcome is a network architecture or infrastructure. Compliance and policy reference a semi-permanent component with a feedback loop for long-term adjustments, such as the PCI-DSS requirement to incorporate EMV chip and card support into merchant terminals. The continuous improvement cycle reflects an active and dynamic process with a feedback loop for short-term changes, such as implementing a multi-factor authentication solution. Monitoring and testing are in the feedback loop for learning and evidence-creation that supports decision-making for continuous improvement. The support system accounts for social networking, community involvement, and, most importantly, executive buy-in that funds continuous improvement and significant upgrades. A potential use-case for the sizeable public venue IT framework is for an IT manager or cybersecurity practitioner to communicate proposed changes with general managers or business executives for adequate funding.

Multi-factor authentication was often recommended as a mechanism to overcome password management and weak endpoint security. While at different development stages, device control was recommended to lock down the security of devices used for venue business and operations. It included testing and certification for venue business, building electrical controls, and IoT. The last finding was to have executive buy-in to fund and enable continuous improvement.

This study focused on uncovering effective cybersecurity strategies for preventing data breaches in large public venues with wireless networks. The study results provided cybersecurity strategies useful for addressing other cybersecurity issues and IT issues in general.

REFERENCES

3GPP (n.d.). About 3GPP Home. Retrieved May 26, 2019, from https://www.3gpp.org/about-3gpp/about-3gpp

Abdalzaher, M. S., Seddik, K., Elsabrouty, M., Muta, O., Furukawa, H., & Abdel-Rahman, A. (2016). Game theory meets wireless sensor networks security requirements and threats mitigation: A survey. *Sensors, 16*(7), 1003. doi:10.3390/s16071003

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection, 8*, 53–66. doi:10.1016/j.ijcip.2014.12.002

Alneyadi, S., Sithirasenan, E., & Muthukkumarasamy, V. (2016). A survey on data leakage prevention systems. *Journal of Network and Computer Applications, 62*, 137–152. doi:10.1016/j.jnca.2016.01.008

Álvarez Cid-Fuentes, J., Szabo, C., & Falkner, K. (2018). An adaptive framework for the detection of novel botnets. *Computers & Security, 79*, 148–161. doi:10.1016/j.cose.2018.07.019

Amadeo, K. (2018). Current U.S. federal government tax revenue. *The Balance.* Retrieved from https://www.thebalance.com/current-u-s-federal-government-tax-revenue-3305762

Ananda, K., Ujwala, P., & Kemwal, H. (2017). Protection against information leakage and malware with risk free public Wi-Fi usage. *International Journal of Research in Engineering and Technology, 6*(04), 64–66. doi:10.15623/ijret.2017.0604015.

Arfaoui, G., Bisson, P., Blom, R., Borgaonkar, R., Englund, H., Felix, E., Zahariev, A. (2018). A security architecture for 5G networks. *IEEE Access, 6*, 22466–22479. doi:10.1109/access.2018.2827419

Armenia, S., Ferreira Franco, E., Nonino, F., Spagnoli, E., & Medaglia, C. M. (2019). Towards the definition of a dynamic and systemic assessment for cybersecurity risks. *Systems Research and Behavioral Science, 36*(4), 404–423. doi:10.1002/sres.2556

Astani, M., & Ready, K. J. (2016). Trends and preventive strategies for mitigating cybersecurity breaches in organizations. *Issues in Information Systems*, *17*(2), 208–214. doi:10.48009/2_iis_2016_208-214

Atkins, W., Ghering, C., Kidd, M., Kussmann, C., Perrin, J. M., Phillips, M., & Talbot, K. (2020, April 28). Staffing for effective digital preservation 2017: An NDSA report. *National Digital Stewardship Alliance.* doi:10.17605/osf.io/3rcqk

Bamakan, S. M. H., Amiri, B., Mirzabagheri, M., & Shi, Y. (2015). A new intrusion detection approach using PSO based multiple criteria linear programming. *Procedia Computer Science*, *55*, 231–237. doi:10.1016/j.procs.2015.07.040

Bartoli, A., Medvet, E., & Onesti, F. (2018). Evil twins and WPA2 enterprise: A coming security disaster? *Computers and Security*, *74*(2018), 1–11. doi:10.1016/j.cose.2017.12.011

Barrett, M. P. (2018, April 16). *Framework for improving critical infrastructure cybersecurity* (Version 1.1.). National Institute of Standards and Technology. doi:10.6028/nist.cwsp.04162018

Baškarada, S. (2015). Qualitative case study guidelines. *The Qualitative Report*, *19*(40), 1–18. doi:10.46743/2160-3715/2014.1008

Bazeley, P., & Jackson, K. (2019). *Qualitative data analysis with NVivo* (3rd ed.). Thousand Oaks, CA: Sage.

Borhade, S. R., & Kahate, S. A. (2016). Intrusion detection system based on hashing technique. *Global Journal of Engineering Science and Researches, 3*(6), 31–34. doi:10.5281/zenodo.55494

Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic cyber intelligence. *Information and Computer Security, 23*(3), 317–332. doi:10.1108/ICS-09-2014-0064

Botha, J., Eloff, M., & Swart, I. (2016, March). Pro-active data breach detection: Examining accuracy and applicability on personal information detected. In T. Zlateva & V. A. Greiman (Eds.), *Proceedings of the 11th International Conference on Cyber Warfare and Security (ICCWS): Vol. 12* (pp. 47–55). Academic Conferences and Publishing International.

Booz Allen. (2019). *2019 Cyber threat outlook, eight ways threat actors will make waves in 2019* (Report). Retrieved from https://www.boozallen.com

Bottarelli, M., Epiphaniou, G., Ismail, D., Karadimas, P., & Al-Khateeb, H. (2018). Physical characteristics of wireless communication channels for secret key establishment: A survey of the research. *Computers & Security, 78*, 454–476. doi:10.1016/j.cose.2018.08.001

Bovee, M., & Read, H. (2018, June). Super bowl 50: Can football teach students to become better cybersecurity professionals? In *17th European Conference on Cyber Warfare and Security (ECCWS 2018): Vol. 2* (pp. 49–56). Academic Conferences International. Retrieved from ProQuest Central database.

Braun, T., Fung, B. C. M., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. *Sustainable Cities and Society, 39*, 499–507. doi:10.1016/j.scs.2018.02.039

Brillat, B. T. (2018, March 17). Four trends in stadium technology infrastructure to watch in 2018. *SportTechie*. Retrieved from https://www.sporttechie.com/4-trends-stadium-technology-infrastructure-watch-2018

Brinkmann, S. (2016). Methodological breaching experiments: Steps toward theorizing the qualitative interview. *Culture & Psychology, 22*, 520–533. doi:10.1177/1354067x16650816

Brown, G. (2016). *Mobile edge computing use cases and deployment options* [White paper]. Juniper. https://www.juniper.net/assets/us/en/local/pdf/whitepapers/2000642-en.pdf

Burns, K. A., Reber, T., Theodore, K., Welch, B., Roy, D., & Siedlecki, S. L. (2018). Enhanced early warning system impact on nursing practice: A phenomenological study. *Journal of advanced nursing*, *74*, 1150–1156. doi:10.1111/jan.13517

Burton-Howard, V. (2018). *Protecting small business information from cyber security criminals: A qualitative study* (Doctoral dissertation). Retrieved from ProQuest & Theses Global. (Order No. 10928879).

Butler, B. (2018, August). *Evaluating the new 802.11ax Wi-Fi standard and what it will mean for enterprises* [White paper]. IDC. https://webresources.ruckuswireless.com/pdf/wp/wp-idc-evaluating-802.11ax-wi-fi-standard.pdf

Carmichael, S. G. (2015, August 19). *The research is clear: Long hours backfire for people and for companies*. Retrieved from https://hbr.org/2015/08/the-research-is-clear-long-hours-backfire-for-people-and-for-companies

Carrasco, R. S. M., & Sicilia, M. (2018). Unsupervised intrusion detection through skip-gram models of network behavior. *Computers & Security,78*, 187–197. doi:10.1016/j.cose.2018.07.003

CDW. (2018). *The Cybersecurity Insight Report*. Retrieved from https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/solutions/cybersecurity/cdw-cybersecurity-insight-report.pdf

Ceric, A. (2015). An alternative model of the ICT value creation process based on cross-impact analysis. *Contemporary Management Research, 11*(3), 223–247. doi:10.7903/cmr.13574

Checkland, P. (2000). The emergent properties of SSM in use: A symposium by reflective practitioners. *Systemic Practice and Action Research*, 13(6), 799-823. doi:10.1023/A:1026431613200

Checkland, P. (1999). *Systems thinking, systems practice*. Chichester, UK: Wiley and Sons.

Checkland, P. (2012). Four conditions for serious systems thinking and action. *Systems Research & Behavioral Science, 29*, 465–469. doi:10.1002/sres.2158

Checkland, P., & Winter, M. (2006). Process and content: Two ways of using SSM. *Journal of the Operational Research Society, 57*(12), 1435-1441. doi:10.1057/palgrave.jors.2602118

Christensen, L., Johnson, R., & Turner, L. (2014). *Research methods, design and analysis* (12th ed.). Upper Saddle River, NJ: Pearson Education.

Cisco Systems. (2015). *Cisco connected stadium solution* [Data sheet]. Retrieved from https://www.cisco.com/c/dam/en_us/solutions/industries/docs/sports/connected_stadium_datasheet.pdf

Cole, R. A., & Mehran, H. (2018). Gender and the availability of credit to privately held firms: evidence from the surveys of small business finances. *FRB of New York Staff Report*, (383). doi:10.2139/ssrn.1799649

Collins, C. S., & Stockton, C. M. (2018). The central role of theory in qualitative research. *International Journal of Qualitative Methods*, 17(1). doi:10.1177/1609406918797475

Cook, K. D. (2017). *Effective cyber security strategies for small businesses* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses (Order No. 10602149).

Cooper, D. R., & Schindler, P. S. (2014). *Business research methods* (12th ed.). New York, NY: McGraw-Hill.

Damianakis, T., & Woodford, M. R. (2012). Qualitative research with small connected communities: Generating new knowledge while upholding research ethics. *Qualitative Health Research, 22*, 708–718. doi:10.1177/1049732311431444

Décary-hétu, D., & Leppänen, A. (2016). Criminals and signals: An assessment of criminal performance in the carding underworld. *Security Journal, 29*(3), 442–460. doi:10.1057/sj.2013.39

Densham, B. (2015). Three cyber-security strategies to mitigate the impact of a data breach. *Network Security, 2015*(1), 5–8. doi:10.1016/S1353-4858(15)70007-3

Dhameja, K. (2015). Cyber-security measures in ivy league colleges and other higher educational institutions. *International Journal of Engineering Trends in Science and Technology*, *2*(4), 2196–2201. Retrieved from http://citeseerx.ist.psu.edu

Dingman, A., & Russo, G. (2015, March 31). Risk-based vulnerability disclosure: Towards optimal policy. *The 43rd Research Conference on Communication, Information and Internet Policy Paper (TPRC 43), USA.* doi:10.2139/ssrn.2601191

Drack, M., & Schwarz, G. (2010). Recent developments in general system theory. *Systems Research & Behavioral Science, 27*(6), 601–610. doi:10.1002/sres.1013

Edgar, T. W., & Manz, D. O. (2017). *Research methods for cyber security*. Cambridge, MA: Syngress

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

Eichensehr, K. E. (2016). Public-private cybersecurity. *Texas Law Review*, *95*(3), 467. Retrieved from https://texaslawreview.org

Emerson, R. W. (2015). Convenience sampling, random sampling, and snowball sampling: How does sampling affect the validity of research? *Journal of Visual Impairment & Blindness*, *109*(2), 164–168. doi:10.1177/0145482X1510900215

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks, 9*(17), 4667–4679. doi:10.1002/sec.1657

Federal Bureau of Investigation Internet Crime Complaint Center [FBI IC3]. (2017). *2017 Internet crime report*. Retrieved from https://pdf.ic3.gov/2017_ic3report.pdf

Fletcher, D., Massis, A. D., & Nordqvist, M. (2016). Qualitative research practices and family business scholarship: A review and future research agenda. *Journal of Family Business Strategy, 7*(1), 8–25. doi:10.1016/j.jfbs.2015.08.001

Foster, B. K. (2015). Ten recommendations for improving government (or anyone's) IT security. *US CyberWarrior*. Retrieved from https://www.uscyberwarrior.com

Frenel, K. (2016). *Why security pros are always under pressure*. Retrieved from http://www.cioinsight.com/security

Fulks, D. L. (2016). *Revenues and expenses 2004-15* [Report]. Indianapolis, IN: NCAA. Retrieved from http://www.ncaapublications.com/productdownloads/D1REVEXP2015.pdf

Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security, 28*(1-2), 18-28. doi:10.1016/j.cose.2008.08.003

Gerard, Z. (2016). What after the Sony hack? Examination of the development of cybersecurity law in the United States and in France and its impact on lawyers. *Entertainment and Sports Lawyer, 32*(3), 28–33. Retrieved from HeinOnline database.

Geyda, A., & Lysenko, I. (2019). Modeling of Information Operations Effects: Technological Systems Example. *Future Internet*, 11(3), 62. doi:10.3390/fi11030062

Giorgio, P. (2018). Deloitte's sports industry starting lineup: Trends expected to disrupt and dominate 2018. *Deloitte*. Retrieved from https://www2.deloitte.com

Goel, R., Kumar, A., & Haddow, J. (2020). PRISM: A strategic decision framework for cybersecurity risk assessment. *Information & Computer Security, 28*(4), 591–625. doi:10.1108/ICS-11-2018-0131

Golden, D., Tyler, R., Eucker, D., & Meyers, J. (2016). Prioritizing information technology spending through cyber risk assessments. *The Journal of Government Financial Management*, *65*(3), 26–31.

Gordon, L.A., Loeb, M.P., Lucyshyn, W., & Zhou, L. (2015). Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb Model. *Journal of Information Security, 6*(1), 24–30. doi:10.4236/jis.2015.61003

Greenwald, M. (2017). *Cybersecurity in sports, questions of privacy and ethics*. Tufts University: Unpublished essay. Retrieved from http://www.cs.tufts.edu/comp/116/archive/fall2017/mgreenwald.pdf

Gunzel, J. A. (2017). Tackling the cyber threat: The impact of the DoD's network penetration reporting and contracting for cloud services rule on DoD contractor cybersecurity. *Public Contract Law Journal*, *46*(3), 687–712. Retrieved from ProQuest Central database.

HHS Office of the Secretary Office for Civil Rights. (2013, July 26). *Summary of the HIPAA security rule*. Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Haddad, Z., Mahmoud, M., Taha, S., & Saroit, I. A. (2015). Secure and privacy-preserving AMI-utility communications via LTE-A networks. *Wireless and Mobile Computing, Networking and Communications (WiMob), 5*(5), 193–203. doi:10.1109/wimob.2015.7348037

Hagos, D. (2016). The performance of network-controlled mobile data offloading from LTE to WiFi networks. *Telecommunication Systems, 61*(4), 675–694. doi:10.1007/s11235-015-0061-2

Hamamoto, A. H., Carvalho, L. F., Sampaio, L. D. H., Abrão, T., & Proença Jr, M. L. (2018). Network anomaly detection system using genetic algorithm and fuzzy logic. *Expert Systems with Applications*, *92*, 390–402. doi:10.1016/j.eswa.2017.09.013

Hassan, D. (2016). Surveillance by proxy: Sport and security in a modern age. *American Behavioral Scientist, 60*(9), 1043–1056. doi:10.1177/0002764216632840

Helgeson, S., Robberstad, C., Mohan, J. P., Eswaran, S., & Ranganathan, P. (2018). A comprehensive survey on wireless vulnerabilities through the OSI and IEEE model. In *Proceedings of the International Conference on Modeling, Simulation and Visualization Methods (MSV'18)* (pp. 76–80). Retrieved from https://csce.ucmss.com/cr/books/2018/lfs/csrea2018/msv4203.pdf

Hennick, C. (2016, July 20). Stadiums need physical and digital security to keep players and fans safe. *BizTech*. Retrieved from https://biztechmagazine.com/article/2016/07/stadiums-need-physical-and-digital-security-keep-players-and-fans-safe

Hidayanto, B. C., Muhammad, R. F., Kusumawardani, R. P., & Syafaat, A. (2017). Network intrusion detection systems analysis using frequent item set mining algorithm FP-max and apriori. *Procedia Computer Science, 124*, 751–758. doi:10.1016/j.procs.2017.12.214

Hoeper, K., & Chen, L. (2009). Recommendation for EAP methods used in wireless network access authentication (NIST Special Publication, 800-120). Retrieved from https://nvlpubs.nist.gov/nistpubs

Homeland Security Act of 2002, Pub. L. No. 107-296

Hong, J. B., Enoch, S. Y., Kim, D. S., Nhlabatsi, A., Fetais, N., & Khan, K. M. (2018). Dynamic security metrics for measuring the effectiveness of moving target defense techniques. *Computers & Security, 79*, 33–52. doi:10.1016/j.cose.2018.08.003

Horwitz, J. (2019, March 20). CBRS Alliance plans U.S. 5G service on global 3.5GHz band in 2020 [Press release]. https://www.cbrsalliance.org/news/cbrs-alliance-plans-u-s-5g-service-on-global-3-5ghz-band-in-2020

Hu, Q., Zhang, J., Mitrokotsa, A., & Hancke, G. (2018). Tangible security: Survey of methods supporting secure ad-hoc connects of edge devices with physical context. *Computers & Security, 78*, 281-300. doi:10.1016/j.cose.2018.06.009

Hughes, B. B., Bohl, D., Irfan, M., Margolese-Malin, E., & Solórzano, J. R. (2017). ICT/cyber benefits and costs: Reconciling competing perspectives on the current and future balance. *Technological Forecasting & Social Change, 115*, 117–130. doi:10.1016/j.techfore.2016.09.027

Ing, D. (2013). Rethinking systems thinking: Learning and coevolving with the world. *Systems Research & Behavioral Science*, *30*(5), 527–547. doi:10.1002/sres.2229

Intel IoT. (2016). *Smart stadiums take the lead in profitability, fan experience, and security* (Solution brief). Retrieved from https://www.intel.com

International Association of Emergency Medical Services Chiefs (IAEMSC). (2017). *The active shooter planning and response guide*. Retrieved from https://www.jointcommission.org/-/media/tjc/documents/resources/emergency-management/2017_active_shooter_planning_response_healthcare_settingpdf.pdf

Jabbar, M. A., & Aluvalu, R. (2017). RFAODE: A novel ensemble intrusion detection system. *Procedia computer science*, *115*, 226–234. doi:10.1016/j.procs.2017.09.129

Jabez, J., & Muthukumar, B. (2015). Intrusion detection system (IDS): Anomaly detection using outlier detection approach. *Procedia Computer Science, 48*, 338–346. doi:10.1016/j.procs.2015.04.191

Jenkins, S., & Evans, N. (2018). The growing threat of cybersecurity attacks in sports. In *Cyber Sensing 2018* (Vol. 10630, p. 1063003). *International Society for Optics and Photonics*. doi:10.1117/12.2303840

Jia, Y., Zhou, Z., Chen, F., Duan, P., Guo, Z., & Mumtaz, S. (2017). A non-intrusive cyber physical social sensing solution to people behavior tracking: Mechanism, prototype, and field Experiments. *Sensors (Switzerland)*, *17*(1), 143. doi:10.3390/s17010143

Jones, D. (2019, May). *Bid #18-18 Tampa sports authority staffing services, Raymond James Stadium*. Tampa, FL: Tampa Sports Authority. Retrieved from https://static1.squarespace.com/static/54245dc1e4b0cee499909324/t/5cdd828aae87bf00012f61f9/1558020747355/Bid Document - TSA Staffing Services - Bid 18-18.pdf

Jonker, M. (2017, June 17). Embracing complex systems thinking. *Accountancy SA.* 50–52.

Kamin, D. A. (2017). *Exploring security, privacy, and reliability strategies to enable the adoption of IoT* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10640866).

Kashmiri, S., Nicol, C. D., & Hsu, L. (2017). Birds of a feather: Intra-industry spillover of the target customer data breach and the shielding role of IT, marketing, and CSR. *Journal of the Academy of Marketing Science, 45*(2), 208–228. doi:10.1007/s11747-016-0486-5

Khan, T. M., Patel, N. V., & Eldabi, T. (2010). Theory of deferred action: Agent-based simulation model for designing complex adaptive systems. *Journal of Enterprise Information Management, 23*(4), 521–537. doi:10.1108/17410391011061799

Kim, Y., Kim, M. S., Lee, S., Griffith, D., & Golmie, N. (2017, March). AP selection algorithm with adaptive CCAT for dense wireless networks. In *2017 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1–6). doi:10.1109/WCNC.2017.7925822

Kim, H., Lee, J., Lee, E., & Kim, Y. (2019, May). Touching the untouchables: Dynamic security analysis of the LTE control plane. In *2019 IEEE Symposium on Security and Privacy (SP): Vol. 1.* (pp. 646−661). doi:10.1109/SP.2019.00038

Kirkwood, A., & Price, L. (2013). Examining some assumptions and limitations of research on the effects of emerging technologies for teaching and learning in higher education: Examining assumptions and limitations of research. *British Journal of Educational Technology, 44*(4), 536–543. doi:10.1111/bjet.12049

Kohlios, C., & Hayajneh, T. (2018). A comprehensive attack flow model and security analysis for Wi-Fi and WPA3. *Electronics*, *7*(11), 284. doi:10.3390/electronics7110284

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting & Social Change, 80*(3), 541–555. doi:10.1016/j.techfore.2012.07.002

Kubler, S., Robert, J., Hefnawy, A., Framling, K., Cherifi, C., & Bouras, A. (2017). Open IoT ecosystem for sporting event management. *Special Section in IEEE Access: Emergent Topics for Mobile and Ubiquitous Systems in Smartphone, IoT, and Cloud Computing Era*, *5*, 7064–7079. doi:10.1109/access.2017.2692247

Lainhart, J., Conboy, M., & Saull, R. (2018). *COBIT 2019 framework: Introduction & methodology* [Enterprise Governance of Information and Technology]. Schaumburg, IL.

Landauer, M., Wurzenberger, M., Skopik, F., Settanni, G., & Filzmoser, P. (2018). Dynamic log file analysis: An unsupervised cluster evolution approach for anomaly detection. *Computers & Security, 79*, 94–116. doi:10.1016/j.cose.2018.08.009

Leedy, P., & Ormrod, J. (2014). *Practical research: Planning and design* (11th ed.). Upper Saddle River, NJ: Pearson

Leslie, N. O., Harang, R. E., Knachel, L. P., & Kott, A. (2018). Statistical models for the number of successful cyber intrusions. *Journal of Defense Modeling & Simulation, 15*(1), pp. 49–63. doi:10.1177/1548512917715342

LiCalzi, C. (2017). Computer crimes. *The American Criminal Law Review, 54*(4), 1025. Retrieved from LexisNexis Academic ISSN:0164-0364

Liu, S., & Kuhn, R. (2010 April). Data loss prevention. *IT Professional*, *12*(2), 10–13. doi:10.1109/MITP.2010.52.

Loosemore, M., & Cheung, E. (2015). Implementing systems thinking to manage risk in public private partnership projects. *International Journal of Project Management, 33*(6), 1325–1334. doi:10.1016/j.ijproman.2015.02.005

Loukaka, A., & Rahman, S. (2017). Discovering new cyber protection approaches from a security professional prospective. *International Journal of Computer Networks & Communications (IJCNC), 9*. doi:10.5121/ijcnc.2017.9402

Love, J. H., & Roper, S. (2015). SME innovation, exporting and growth: A review of existing evidence. *International Small Business Journal, 33*(1), 28–48. doi:10.1177/0266242614550190

Maahs, D. L. (2018). *Managerial strategies small businesses use to prevent cybercrime* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10936342).

Mahmud, N. (2018). *Vulnerabilities of LTE and LTE-advanced communication* [White paper]. Rhode & Schwarz. https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1ma245/1MA245_2e_LTE_Vulnerabilities.pdf

Marshall, C., & Rossman, G. B. (2016). *Designing qualitative research* (6th ed.). Thousand Oaks, CA: Sage.

Mason, D., Sant, S. L., & Misener, L. (2018). Leveraging sport and entertainment facilities in small-to mid-sized cities. *Marketing Intelligence & Planning*, *36*(2), 154–167. doi:10.1108/MIP-04-2017-0065

Matinmikko, M., Latva-aho, M., Ahokangas, P., & Seppänen, V. (2018). On regulations for 5G: Micro licensing for locally operated networks. *Telecommunications Policy, 42*(8), 622–635. doi:10.1016/j.telpol.2017.09.004

Matook, S., & Brown, S. A. (2017). Characteristics of IT artifacts: A systems thinking-based framework for delineating and theorizing IT artifacts. *Information Systems Journal, 27*(3), 309–346. doi:10.1111/isj.12108

Mazini, M., Shirazi, B., & Mahdavi, I. (2018). Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. *Journal of King Saud University - Computer and Information Sciences*. doi:10.1016/j.jksuci.2018.03.011

McCandless, D. (n.d.). World's biggest data breaches & hacks [Data file]. *Information is Beautiful*. Retrieved December 6, 2018, from https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative, or mixed methods and choice based on the research. *Sage Journals, 30*, 537–542. Retrieved from http://online.sagepub.com

McElroy, V. G. (2018). *An examination of the effect of instructional timing of web-based scenarios on student recall* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10827565).

McGuire, C. F. (2015). TIM lecture series - the expanding cybersecurity threat. *Technology Innovation Management Review*, *5*(3), 56–48. doi:10.22215/timreview/881

Melander, B. A. (2016). Smart stadiums: An illustration of how the internet of things is revolutionizing the world. *Arizona State University Sports & Entertainment Law Journal*, *6*, 349. Retrieved from HeinOnline database.

Mickulicz, N. D., Drolia, U., Narasimhan, P., & Gandhi, R. (2016). Zephyr: First-person wireless analytics from high-density in-stadium deployments. In *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)* (pp. 1–10). doi:10.1109/WoWMoM.2016.7523552

Miklai, M. (2018). *Roles and skills of the chief information security officer of a large bank in the United States: A qualitative single case study* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10822627).

Mitra, S. (2016). *A quantitative investigation of the security factors affecting the use of IT systems in public networks* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10148523).

Morgan, S. (2016, January 17). Cyber crime costs projected to reach $2 trillion by 2019. *Forbes*. Retrieved from https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019

Morovati, K., Kadam, S., & Ghorbani, A. (2016). A network based document management model to prevent data extrusion. *Computers & Security, 59*, 71–91. doi:10.1016/j.cose.2016.02.003

Muller, H. (2015). *The big shift in IT leadership: How great CIOs leverage the power of technology for strategic business growth in the customer-centric economy*. [VitalSource Bookshelf version]. Retrieved from vbk://9781119123262

Munaiah, N., & Meneely, A. (2016, November). Vulnerability severity scoring and bounties: Why the disconnect? In *Proceedings of the 2nd International Workshop on Software Analytics (SWAN 2016)*. *Association for Computing Machinery*, *USA*, 8–14. doi:10.1145/2989238.2989239

Nasr, E., Jalloul, M., Bachalaany, J., & Maalouly, R. (2019). Wi-fi network vulnerability analysis and risk assessment in Lebanon. *MATEC Web of Conferences, 281*, 5002. doi:10.1051/matecconf/201928105002

National Science and Technology Council Office of the President. (2016, February). *Federal cybersecurity research and development strategic plan.* Retrieved from https://www.nitrd.gov/pubs/2016-Federal-Cybersecurity-Research-and-Development-Strategic-Plan.pdf

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management, 52*(1), 123–134. doi:10.1016/j.im.2014.10.009

National Institute of Standards and Technology [NIST] (n.d.). *National vulnerability database* [Data file]. Retrieved February 6, 2019, from https://nvd.nist.gov/vuln/search/statistics?form_type=Advanced&results_type=statistics&query=NBA&search_type=all&pub_start_date=01/01/2004&pub_end_date=12/29/2018

Nero, R. L. (2018). *Risks, benefits, and perceived effectiveness of outsourcing it network security in small businesses: A multiple-case study* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10790920).

Nicholls, R. (2016). Spectrum management issues for heterogeneous networks in commons spectrum. *Info: The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media, 18*(4), 1–11. doi:10.1108/info-02-2016-0010

Njenga, K., & Jordaan, P. (2016). We want to do it our way: The neutralisation approach to managing information systems security by small businesses. *The African Journal of Information Systems, 8*(1), 3. 42–63. Retrieved from http://digitalcommons.kennesaw.edu/ajis

Ohta, T., Takenaka, M., Katou, M., Masuoka, R., Kayama, K., Fukushima, N., & Imai, H. (2018). Cybersecurity solutions for major international events. *Fujitsu Scientific & Technical Journal*, *54*(4), 57–65. Retrieved from https://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol54-4/paper06.pdf

Olmstead, K., & Smith, A. (2017). Americans and cybersecurity. *Pew Research Center, 26*, 311-327. Retrieved from https://assets.pewresearch.org

Oyelami, O. O. (2018). *Case study research as a method for digital forensic evidence examinations* (Unpublished master's thesis). University of Pretoria, South Africa.

Oxford Economics. (2018). *Economic significance of meetings to the US economy: Economic significance study (ESS) report for the Events Industry Council*. Retrieved from https://eventscouncil.org

Panchanathan, S., McDaniel, T., Tadayon, R., Rukkila, A., & Venkateswara, H. (2019). Smart stadia as testbeds for smart cities: Enriching fan experiences and improving accessibility. In *2019 International Conference on Computing, Networking and Communications (ICNC)* (pp. 542–546). doi:10.1109/ICCNC.2019.8685580

Paolini, M. (2019). *CBRS: Should the enterprise and venue owners care?* Retrieved from https://ongoalliance.org/wp-content/uploads/2019/02/SenzaFili_CBRS_DeepDiveReport.pdf

Parker, C., Scott, S., & Geddes, A. (2019). Snowball sampling. In P. Atkinson, S. Delamont, A. Cernat, J.W. Sakshaug, & R.A. Williams (Eds.), *SAGE Research Methods Foundations*. doi:10.4135/9781526421036831710

Parvez, I., Sriyananda, M. G. S., Güvenç, İ, Bennis, M., & Sarwat, A. (2016). CBRS spectrum sharing between LTE-U and WiFi: A multiarmed bandit approach. *Mobile Information Systems, 2016*, 1–12. doi:10.1155/2016/5909801

Patel, N. V. (2009). The theory of deferred action: Informing the design of information systems for complexity. In *Handbook of Research on Contemporary Theoretical Models in Information Systems*, 164-191. doi:10.4018/9781605666594.ch010

Patel, N. V., & Hackney, R. (2008). Designing information systems requirements in context: Insights from the theory of deferred action.

Patterson, J. (2017). *Cyber-security policy decisions in small businesses* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10680962).

Payne, C. (2015). *Education for sustainability: An ethnographic study of 15 year-2/3 rural Western Australian children's attitudes on sustainability*. Retrieved from https://ro.ecu.edu.au/theses/1630

Perri, D. F., & Perri, E. D. (2018). Acknowledging the "M" in MIS: Managing a data breach crisis. *Journal of the Academy of Business Education*, *19*, 9-32.

Protection of Human Subjects, 45 C.F.R. § 46 (2018).

Puuska, S., Rummukainen, L., Timonen, J., Lääperi, L., Klemetti, M., Oksama, L., & Vankka, J. (2018). Nationwide critical infrastructure monitoring using a common operating picture framework. *International Journal of Critical Infrastructure Protection, 20*, 28–47. doi:10.1016/j.ijcip.2017.11.005

Qualcomm Technologies (2018). *Accelerating the mobile ecosystem expansion in the 5G Era with LTE advanced pro*. Retrieved from https://www.qualcomm.com/media/documents/files/accelerating-the-mobile-ecosystem-expansion-in-the-5g-era-with-lte-advanced-pro.pdf

Rainie, L., & Anderson, J. (2017, August 10). The fate of online trust in the next decade. *Pew Research Center*. Retrieved from https://www.pewresearch.org/internet/2017/08/10/the-fate-of-online-trust-in-the-next-decade

Ramachandran, M. (2016). Software security requirements management as an emerging cloud computing service. *International Journal of Information Management*, *36*(4), 580–590. doi:10.1016/j.ijinfomgt.2016.03.008

Raza, M. T., Anwar, F. M., & Lu, S. (2017, October). Exposing LTE security weaknesses at protocol inter-layer, and inter-radio interactions. *International Conference on Security and Privacy in Communication Systems* (pp. 312–338). Springer, Cham. doi:10.1007/978-3-319-78813-5_16

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

Rupprecht, D., Kohls, K., Holz, T., & Pöpper, C. (2019, May). Breaking LTE on layer two. In *IEEE Symposium on Security & Privacy (SP), 1*, 91–106. doi:10.1109/SP.2019.00006

Saber, J. A. (2016). *Determining small business cybersecurity strategies to prevent data breaches* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10181342).

Saeed, A., Ahmadinia, A., Javed, A., & Larijani, H. (2016). Random neural network based intelligent intrusion detection for wireless sensor networks. *Procedia Computer Science, 80*, 2372–2376. doi:10.1016/j.procs.2016.05.453

SAFETY Act of 2002. (n.d.). DHS Safety Act. Retrieved from https://www.safetyact.gov/lit/h/p

Sajjad, S. M., Bouk, S. H., & Yousaf, M. (2015). Neighbor node trust based intrusion detection system for WSN. *Procedia Computer Science, 63*, 183–188. doi:10.1016/j.procs.2015.08.331

Saldaña, J. (2016). *The coding manual for qualitative researchers* (3rd ed.). Los Angeles, CA, CA: SAGE.

Sarabi, A., Naghizadeh, P., Liu, Y., & Liu, M. (2016). Risky business: Fine-grained data breach prediction using business profiles. *Journal of Cybersecurity*, *2*(1), 15–28. doi:10.1093/cybsec/tyw004

Schatz, D., & Bashroush, R. (2016). The impact of repeated data breach events on organisations' market value. *Information and Computer Security, 24*(1), 73–92. doi:10.1108/ICS-03-014-0020

Selznick, L. F., & LaMacchia, C. (2017). Cybersecurity liability: How technically savvy can we expect small business owners to be. *Journal of Business and Technology Law*, *13*(2), 217–253. Retrieved from http://digitalcommons.law.umaryland.edu/jbtl

Setiawan, B., Djanali, S., & Ahmad, T. (2017). A Study on intrusion detection using centroid-based classification. *Procedia Computer Science*, *124*, 672–681. doi:10.1016/j.procs.2017.12.204

Shaik, A., Borgaonkar, R., Asokan, N., Niemi, V., & Seifert, J. P. (2015). Practical attacks against privacy and availability in 4G/LTE mobile communication systems. doi:10.14722/ndss.2016.23236

Sheehan, B., Murphy, F., Mullins, M., & Ryan, C. (2018). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part A,* doi:10.1016/j.tra.2018.06.033

Shenfield, A., Day, D., & Ayesh, A. (2018). Intelligent intrusion detection systems using artificial neural networks. *ICT Express, 4*(2), 95–99. doi:10.1016/j.icte.2018.04.003

Shivaramu, K. N., Prasobh, P. S., & Poti, N. (2016). A survey on security vulnerabilities in wireless ad hoc high performance clusters. *Procedia Technology, 25*, 489–496. doi:10.1016/j.protcy.2016.08.136

Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017, January 18). Breaking the target: An analysis of target data breach and lessons learned. Retrieved from arXiv database. (abs/1701.04940).

Simon, M. K., & Francis, B. J. (2004). *The dissertation cookbook: From soup to nuts a practical guide to start and complete your dissertation* (3rd. ed.). Dubuque, Iowa: Kendall/Hunt.

Sritapan, V., & Eldefrawy, K. (2018). Security threats, defenses, and recommended practices for enterprise mobility. *ISSA Journal, 16*(5), 25–31.

Stair, R., & Reynolds, G. (2017). *Fundamentals of information systems* (6th ed.). Boston, MA: Cengage Learning.

Stanton, N., Salmon, P., & Walker, G. H. (2018). *Systems thinking in practice: Applications of the event analysis of systemic teamwork method*. Boca Raton, FL: CRC Press.

Sullivan, R. J., & Maniff, J. L. (2016). Data breach notification laws. *Economic Review - Federal Reserve Bank of Kansas City (01612387), 101*(1).

Sunnucks, M. (2019, January 28). How data delivers on the game-day experience (Tips and Trends). Retrieved from Stadium1 Software website: https://www.stadium1.com/how-data-delivers-on-the-game-day-experience

Svensson, L. & Doumas, K. (2013). Contextual and analytic qualities of research methods exemplified in research on teaching. *Qualitative Inquiry, 19*(6), 441–450. doi:10.1177/1077800413482097

Taguchi, N. (2018). Description and explanation of pragmatic development: Quantitative, qualitative, and mixed methods research. *System, 75*, 23–32. doi:10.1016/j.system.2018.03.010

Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as “compliance managers” for businesses. *Law & Social Inquiry, 43*(02), 417–440. doi:10.1111/lsi.12303

Tecuci, G., Marcu, D., Meckl, S., & Boicu, M. (2018). Evidence-based detection of advanced persistent threats. *Computing in Science & Engineering, 20*(6), 54–65. doi:10.1109/MCSE.2018.2873854

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals’ behavior. *Computers & Security, 79*, 68–79. doi:10.1016/j.cose.2018.08.007

Tavanapour, N., Bittner, E. A. C., & Brügger, M. (2019). Theory-driven-design for open digital human collaboration systems. In *Americas Conference on Information Systems Proceedings (AMCIS), Cancún*, 1–10.

Ullah, A. & Lai, R. (2013). A systematic review of business and information technology alignment. *ACM Transactions on Management Information Systems, 4*(1), 1–30. doi:10.1145/2445560.2445564

Ullah, F., Edwards, M., Ramdhany, R., Chitchyan, R., Babar, M. A., & Rashid, A. (2018). Data exfiltration: A review of external attack vectors and countermeasures. *Journal of Network and Computer Applications, 101*, 18–54. doi:10.1016/j.jnca.2017.10.016

Trading Economics. (n.d.). *United States GDP* [Data file]. Retrieved May 20, 2018, from https://tradingeconomics.com/united-states/gdp

Urrico, R. (2017, October 13). Hyatt breached again: Hawaii, Guam & Puerto Rico locations affected. *Credit Union Times*. Retrieved from https://www.grafwebcuso.com/hyatt-breached-again-hawaii-guam-puerto-rico-locations-affected

U.S. Department of Health and Human Services, 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* (45 CFR 46). Retrieved from http://www.hhs.gov/ohrp/regulations-and-policy/belmont-report

U.S. Department of Homeland Security [DHS]. (2015). *Commercial facilities sector-specific plan: An annex to the NIPP 2013*. Retrieved from https://www.cisa.gov/sites/default/files/publications/nipp-ssp-commercial-facilities-2015-508.pdf

U.S. Department of Homeland Security [DHS]. (2016, December). *National cyber incident response plan*. Retrieved from https://us-cert.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

U.S. Department of Homeland Security [DHS]. (2017). *A Guide to securing networks for Wi-Fi (IEEE 802.11 family)*. Retrieved from https://www.us-cert.gov

U.S. Department of Homeland Security [DHS]. (2018, September 28). *Joint national priorities for critical infrastructure security and resilience*. Retrieved from https://www.cisa.gov/sites/default/files/publications/Joint-National-Priorities-Fact-Sheet-20180928-508.pdf

U.S. Department of Homeland Security Commercial Facilities Sector. (2020, May). *Cybersecurity framework implementation guidance.* Retrieved from https://www.cisa.gov/sites/default/files/publications/Commercial_Facilities_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf

U.S. Department of Homeland Security Science and Technology. (n.d.). DHS SAFETY Act approved technologies. Retrieved from https://www.safetyact.gov/lit/at/aa

U.S. Federal Emergency Management Agency. (n.d.). Integrated public alert & warning system. Retrieved from https://www.fema.gov/integrated-public-alert-warning-system

Van Roy, P. (2009). *Scalaris: Scalable transactional storage for web 2.0 services* [Brochure]. Author. Retrieved from https://ist-selfman.org/images/1/17/scalaris_paper.pdf

Van Roy, P., Haridi, S., Reinefeld, A., Stefani, J., Yap, R., & Coupaye, T. (2008). Self management for large-scale distributed systems: An overview of the SELFMAN project. In *Formal Methods for Components and Objects* (pp. 153–178). Berlin, Heidelberg: Springer. doi:10.1007/978-3-540-92188-2_7

Veeramachaneni, K., Arnaldo, I., Korrapati, V., Bassias, C., & Li, K. (2016, April). AI^ 2: Training a big data machine to defend. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (Big Data Security), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)* (pp. 49–54). doi:10.1109/bigdatasecurity-hpsc-ids.2016.79

Vijayanand, R., Devaraj, D., & Kannapiran, B. (2018). Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection. *Computers & Security, 77*, 304–314. doi:10.1016/j.cose.2018.04.010

von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of Management Journal. Academy of Management*, *15*(4), 407–426. doi:10.2307/255139

von Bertalanffy, L. (2015). *General system theory: Foundations, development, applications*. New York, NY: Braziller

Wahl, R. S. (2016). *Latency in intrusion detection systems (IDS) and cyber-attacks: A quantitative comparative study* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10132049).

Wagenen, J. V. (2017, March 2). Little cities see big benefits in smart city investment. *State Tech*. Retrieved from https://statetechmagazine.com

Wang, T. (2016). Study on intelligent stadiums system and development trend based on the internet of things. *Revista Ibérica De Sistemas E Tecnologias De Informação,* (E8), 80–92.

Wang, Y., Miao, Z., & Jiao, L. (2016). Safeguarding the Ultra-dense networks with the aid of physical layer security: A review and a case study. *IEEE Access*, *4*, 9082–9092. doi:10.1109/access.2016.2635698

Weick, K. E. (1989, October). Theory construction as disciplined imagination. *The Academy of Management Review, 14*(4), 516–531. doi:10.5465/amr.1989.4308376

Theoretical assumptions and research methodology selection. In F. W. McFarlan (Ed.), *The Information Systems Research Challenge* (111–132). USA: Harvard Business School

Wi-Fi Alliance. (2019a). Discover Wi-Fi. Retrieved from https://www.wi-fi.org/discover-wi-fi

Wi-Fi Alliance. (2019b). History. Retrieved from https://www.wi-fi.org/who-we-are/history

Yan, D. (2020, January 16). A systems thinking for cybersecurity modeling. Retrieved from arXiv database. (abs/2001.05734).

Yarbrough, B., & Wagner, N. (April 15, 2018). Assessing security risk for wireless sensor networks under cyber attack. In *Proceedings of the Annual Simulation Symposium. Society for Computer Simulation International* (pp. 1–12). doi:10.5555/3213032

Yin, R. (2017). *Case study research and applications: Design and methods* (6th ed.). Thousand Oaks, CA: Sage.

Xie, T., Tu, G. H., Yin, B., Li, C. Y., Peng, C., Zhang, M., & Liu, X. (2018). The untold secrets of operational Wi-Fi calling services: Vulnerabilities, attacks, and countermeasures. *ACM Trans. Priv. Sec., 1*(1), 1–30. Retrieved from arXiv database. (abs/1811.11274).

Zhang, P., Zhu, J., Chen, Y., & Jiang, X. (2019). End-to-end physical layer authentication for dual-hop wireless networks. *IEEE Access, 7*, 38322-38336. doi:10.1109/ACCESS.2019.2906699

Zhang, Q., & Xiao, J. (2017). Improve security of wireless sensor networks through reluctant checksum. *International Journal of Distributed Sensor Networks, 13*(9), doi:10.1177/1550147717731041

Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. In *Proceedings of the IEEE, 104*(9), 1727–1765. doi:10.1109/JPROC.2016.2558521

Zulkefli, Z., Singh, M. M., Mohd Shariff, A. R., & Samsudin, A. (2017). Typosquat cyber crime attack detection via smartphone. *Procedia Computer Science*, *124*, 664–671. doi:10.1016/j.procs.2017.12.203

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346 USA