AN ANALYSIS OF TECHNOLOGY SECURITY GOVERNANCE FACTORS IMPACTING THE ADOPTION OF COMPUTERIZED MAINTENANCE MANAGEMENT SYSTEMS (CMMS): A QUANTITATIVE STUDY

by

Jonathan Bagnall

CELESTE CHAMBERLAIN, DSc, Faculty Mentor and Chair

RANDALL VALENTINE, PhD, Committee Member

PAMELYN WITTEMAN, PhD, Committee Member

Todd C. Wilson, PhD, Dean, School of Business and Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Capella University

July 2020

Abstract

The topic of this study is information security governance. This quantitative, nonexperimental, correlational study investigates the extent that performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance effectiveness impact on the adoption of computerized maintenance management systems by IT managers in the healthcare industry (Busdicker, & Upendra, 2017). Research does not indicate what security governance and behavioral factors are the prime inhibitors of the widespread adoption of CMMS. The research explores the behavior influence effects of the adoption of CMMS by IT managers in the Healthcare industry using a survey to determine if there is a statistically significant relationship between behavior influence effects and the adoption of CMMS. (Sabi, Uzoka, Langmia, & Njeh, 2016). The proposed study tests to confirm the unified theory of acceptance and use of technology developed by Venkatesh, Morris, Davis, & Davis (2003) contributing information about application in information security governance. The primary research question addressed in this study determines the extent performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance effectiveness correlate to the adoption of a computerized maintenance management system. The study also addresses how well performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance predict the adoption of computerized maintenance management systems. The population targeted for this study consists of IT managers working for healthcare delivery organizations with a minimum of 5 years' experience in the healthcare industry. The sampling using Qualtrics survey platform to collect data for the healthcare IT manager probability sampling. This study uses the Qualtrics survey to collect data and IBM SPSS to conduct the statistical analysis. Spearman's correlation analyses conducted

among the independent and dependent variables outlines relationships between data points. An assessment of the measurement model performed using the partial least squares (PLS) regression technique. The survey examining how healthcare personnel, in the United States, understand the benefits of CMMS completed by 77 IT managers. The study used Spearman's rank-order correlation coefficient and PLS to determine the relational analysis for this quantitative study. The results of the analysis indicate that IT managers in the healthcare industry relate UTAUT variables, PE, EE, SI, FC, and TSGE to the adoption of CMMS. The results from this study may not represent sectors found outside the United States and researchers can extend the geographic boundary of the study by gaining insight into multiple regions to understand the differences between adoption cultures.

Dedication

This dissertation is dedicated to my parents, my wife, and children who challenged me to pursue higher learning and added joy to life along the way. Their endless support and encouragement helped throughout the journey. I have great admiration for fellow academians and professors who have been such fun to work with. My extended family and friends continue to be supportive and enthusiastic, and I can never thank enough.

Acknowledgments

I am grateful to my doctoral study chair Dr. Celeste Chamberlain, committee members Dr. Randall Valentine and Dr. Pamelyn Witteman, for their comments, guidance, and support. I am excited that I have finally managed to finish the dissertation and capture the information from a scholarly and academic viewpoint. Many people have played an essential role in this lifetime achievement. My mentor's guidance and advice, along with the committees' feedback, allowed me to develop the final study.

Table of Contents

Acknowledgments v

List of Tables ix

List of Figures xi

CHAPTER 1. INTRODUCTION 1

Background of the Problem 1

Statement of the Problem 5

Purpose of the Study 6

Significance of the Study 9

Research Questions 10

Definition of Terms 10

Research Design 12

Assumptions and Limitations 13

Assumptions 13

Limitations 15

Organization of the Remainder of the Study 16

CHAPTER 2. LITERATURE REVIEW 17

Methods of Searching 17

Theoretical Orientation for the Study 18

Review of the Literature 19

Synthesis of Research Findings 43

Critique of Previous Research Methods 47

Summary 49
CHAPTER 3. METHODOLOGY 51
Research Questions and Hypotheses 52
Research Design 54
Target Population and Sample 56
Population 57
Sample 58
Power Analysis 58
Procedures 59
Participant Selection 59
Protection of Participants 60
Data Collection 60
Data Analysis 61
Instruments 64
Factors Impacting the Adoption of CMMS 65
Ethical Considerations 66
Summary 66
CHAPTER 4. RESULTS 68
Background 68
Description of the Sample 68
Hypothesis Testing 70
Summary 89

CHAPTER 5. DISCUSSION, IMPLICATIONS, RECOMMENDATIONS 90

Summary of the Results 90

Discussion of the Results 95

Conclusions Based on the Results 97

Limitations 98

Implications for Practice 98

Recommendations for Further Research 100

Conclusion 103

REFERENCES 105

List of Tables

Table 1: Coding for Age Demographic Information 62

Table 2: Coding for Job Title Demographic Information 62

Table 3: Coding for Organization Size Demographic Information 63

Table 4: Research Question Data Types 65

Table 5: Missing Data 69

Table 6: Participants' Familiarity with Computerized Maintenance Management Systems 69

Table 7: Age 69

Table 8: Job Title 70

Table 9: Organization Size 70

Table 10: Extreme Values 76

Table 11: Descriptive Statistics Performance Expectancy 77

Table 12: Correlations Performance Expectancy 77

Table 13: Descriptive Statistics Effort Expectancy 78

Table 14: Correlations Effort Expectancy 78

Table 15: Descriptive Statistics Social Influence 79

Table 16: Correlations Social Influence 80

Table 17: Descriptive Statistics Facilitating Conditions 81

Table 18: Correlations Facilitating Conditions 81

Table 19: Descriptive Statistics Technology Security Governance Effectiveness 82

Table 20: Correlations Technology Security Governance Effectiveness 82

Table 21. Outer Loadings for PE 84

Table 22. Outer Loadings for EE 85

Table 23. Outer Loadings for SI 85

Table 24. Outer Loadings for FC 86

Table 25. Outer Loadings for TSGE 87

Table 26. Outer Loadings for CMMS 87

Table 27. Bootstrap Statistical Output 88

Table 28. R square of CMMS adoption 89

List of Figures

Figure 1: Scatterplot diagram performance expectancy 73

Figure 2: Scatterplot diagram effort expectancy..... 73

Figure 3: Scatterplot diagram social influence 74

Figure 4: Scatterplot diagram facilitating conditions..... 74

Figure 5: Scatterplot diagram technology security governance effectiveness..... 75

Figure 6: Partial least squares path model 84

CHAPTER 1. INTRODUCTION

Computerized maintenance management systems (CMMS) are emerging technology that permits decision analysis capability based on the system containing master data on organizations' maintenance operations (Rastegari & Mobin, 2016). The application of automated systems is expanding rapidly in different industries, and CMMS plays an essential role in the automation of production systems (Jamkhaneh, Pool, Khaksar, Arabzad, & Kazemi, 2018). CMMS technologies have grown in the past 50 years with web-based connectivity and assist firms with enterprise resource planning that provides seamless information about the flow for main business processes and decision-making data (Wan, Li, Gao, Roy, & Tong, 2017). Information security governance provides a framework and structure to ensure the adequate mitigation of risk, while management ensures that controls implemented promote the successful enterprise-wide adoption of new technologies.

Research indicates that health delivery organizations (HDO) cybersecurity threats are increasing resulting in security breaches that interrupt patient services, impact patient safety, and theft of patient data, these cybersecurity threats should be the highest priority for HDO's. Continued research in this area is required to support HDO's abilities to manage medical system security and assess security risks across vast technology landscapes, multi-platform environments, and medical devices. By providing the influencing factors of the adoption of CMMS, IT managers in the Healthcare industry can use this study to improve security controls lowering the risks of cybersecurity threats (Ehrenfeld, 2017).

Background of the Problem

The topic of this study is information security governance (Ehrenfeld, 2017; Martin, Ghafur, Kinross, Hankin, & Darzi, 2018; Olavsrud, 2017). This study will investigate,

technology security governance effectiveness, performance expectancy, effort expectancy, social influence, and facilitating conditions on the impact on the adoption of Computerized Maintenance Management System (CMMS) (Busdicker, & Upendra, 2017; Copeland, 2018; Dwivedi, Rana, Jeyaraj, Clement, & Williams, 2019). Further research is needed to implement acceptable information security governance for asset management, continuous monitoring, and maintenance of healthcare solutions contributing to the increase in data breaches (Ehrenfeld, 2017; Martin et al., 2018; Olavsrud, 2017). These security governance gaps proliferate because measures toward ubiquitous Electronic Health Records (EHR) platforms, increase cybersecurity risks to HDO's (Copeland, 2018; Fortin, Bloomfield, Mahaz, & Alfaqih, 2018; Groves, Kayyali, Knott, & Kuiken, 2016; Lemberg, 2017; Malhotra, 2018;). Research does not indicate what security governance and behavioral factors are the prime inhibitors of the widespread adoption of CMMS in healthcare delivery organizations (HDO) (Martin et al., 2018; Ostherr et al., 2017). This study will investigate information security governance and behavioral factors characteristics of Healthcare Delivery Organizations (HDO) influences of adopting CMMS.

This quantitative, nonexperimental, correlative study advanced Venkatesh et al. (2003) unified theory of acceptance and use of technology, specifically, how it applies to computerized maintenance management systems. The UTAUT framework identifies how performance expectancy, effort expectancy, social influence, and facilitating conditions explain user intentions to use information systems. The theory consolidates the constructs of eight previously founded research models that explains information systems usage behavior. Venkatesh et al. (2003) identify that the four independent variables account for 70% of the variance in behavioral intention to use information technology. Researchers have studied organizations and measured how various factors influence the decision to adopt computerized

maintenance management systems (Fortin et al., 2018; Jamkhaneh et al., 2018). Results of the research indicate that lack of funding, training, and system complexities contribute to the challenges of implementing CMMS within organizations (Jamkhaneh et al., 2018). Several studies evaluate CMMS implementation (Sharma & Tewari, 2019; Sher, Talley, Yang, & Kuo, 2017); however, current research fall short of a comprehensive evaluation of the technology security governance aspects of adoption and use. The research lacks clarity on the governance factors that may impact the decision to adopt and use computerized maintenance management systems across the enterprise. This quantitative, correlative, nonexperimental study may further the UTAUT framework by showing the factors influencing the success of CMMS adoption.

The outcome of this study may provide information and understanding to HDO's about the characteristics influencing the adoption of computerized maintenance management systems (Davis, 1989; Martin et al., 2018; Mceachan et al., 2016; Venkatesh, Thong, & Xu, 2012). Advancing this research in information security governance and the awareness of behavioral and organizational influences will help HDO's develop the security safeguards against recognized security threats (Ehrenfeld, 2017; Olavsrud, 2017). The study will further contribute to a body of knowledge that guides industry professionals interested in managing healthcare information based risks and may help advance the effectiveness of overall information security governance (Davis, 1989; Ehrenfeld, 2017; Mceachan et al., 2016; Olavsrud, 2017; Venkatesh et al., 2012; Williams & Woodward, 2015). The target population for this study is IT managers working in the healthcare industry for large and medium HDO's with a minimum of five years' experience.

The literature on information security governance indicates that Healthcare Delivery Organizations (HDO) compliance with regulatory controls protecting Electronic Healthcare Record (EHR) solutions, privacy and security of patient health records (PHR) is a primary

concern. (Rantos, Fysarakis, & Manifavas, 2012; Yang, Qu, Qian, Dai, & Zhu, 2019). Research further defines this concern as embedded in the HIPAA law that a breach of personal health information will result in high penalties and probable loss of reputation to HDO's (Rantos et al., 2012). As healthcare medical solutions and EHR solutions expand their interoperability and interconnection to multiple platform compliance with information security governance controls becomes more complex; they challenge the ability to assess and determine the reliability of security controls and HIPAA compliance (Griebel et al., 2015; Kruse, Smith, Vanderlinden, & Nealand, 2017; Lee, Walker, Delbanco, & Elmore, 2016; Lemberg, 2017; Rantos et al., 2012).

Current research indicates that HDO cybersecurity threats are increasing resulting in security breaches that interrupt patient services and the loss of patient data solutions (Ehrenfeld, 2017; Griebel et al., 2015; Kruse et al., 2017; Lee, Walker, et al., 2016; Lemberg, 2017; Martin et al., 2018; Olavsrud, 2017; Rantos et al., 2012). The literature asserts that it is essential to learn from cybersecurity mistakes and incorporate those lessons learned into identifying cybersecurity framework gaps and make improvements (Knowles, Prince, Hutchison, Disso, & Jones, 2015). Over the past decades, healthcare technology continued to evolve and improve at an incredible rate. Healthcare medical devices, platforms, and the Internet of Things (IoT) device cybersecurity preparedness is a relatively new field of study in the scholarly community compared to their standard technology industry driven counterparts (Knowles et al., 2015). Standard technology-driven industries such as Finance, Government, Commercial, and Manufacturing secure technologies through standard NIST, ISO, or IEE security controls (Au et al., 2017). Studies indicate that the complexity of healthcare environments is a reason why they are not implementing security programs and the proper cybersecurity governance control

measures at a faster pace to protect against cyber threats (Chen, Hwang, Sher, & Lin, 2016; Copeland, 2018; Ehrenfeld, 2017; Martin et al., 2018; Olavsrud, 2017).

Completing this study on the adoption of Computerized Management Maintenance Systems (CMMS) may contribute to the field of information technology assurance and security by providing HDO IT managers crucial information about organizational tools enabling appropriate medical device, solutions, and platforms to be maintained (Chen et al., 2016; Ehrenfeld, 2017; Martin et al., 2018; Olavsrud, 2017). A CMMS can support HDO organizational efforts in this regard (Ehrenfeld, 2017). HDO environments demand a mature approach to the management and maintenance of technology within healthcare, particularly during times of fast-paced growth in medical equipment portfolios and technological advancement (Martin et al., 2018). HDO's that effectively manage medical equipment, capital assets, and infrastructure together are well-positioned to provide a robust, more integrated cybersecurity strategy (Garner, 2017).

Statement of the Problem

The research literature on information security governance indicates that targeted cybersecurity threats in healthcare are increasing and the management and maintenance of medical solutions are a challenge, and that established cybersecurity frameworks are the best defense (Busdicker, & Upendra, 2017; Copeland, 2018; Dwivedi et al., 2019; Ehrenfeld, 2017; Olavsrud, 2017). The cybersecurity threat landscape indicates that healthcare environments are a primary target for cybersecurity threats that seek to impact service and access patient information for monetary gains (Ehrenfeld, 2017; Olavsrud, 2017).

Furthermore, the lack of standard cybersecurity framework controls and security maintenance management of medical solutions decrease cybersecurity effectiveness that enables

cybersecurity breaches (Busdicker, & Upendra, 2017; Copeland, 2018; Dwivedi et al., 2019; Ehrenfeld, 2017; Olavsrud, 2017). The extensive interconnected healthcare medical devices and solutions increase the probability of security breaches and public data disclosures (Ehrenfeld, 2017; Olavsrud, 2017). There is a gap in the body of knowledge as behavioral characteristics of HDO's influence, acceptance, and perceived usefulness of CMMS is not known (Ehrenfeld, 2017; Olavsrud, 2017; Venkatesh et al., 2012).

Purpose of the Study

This quantitative, nonexperimental, correlative study examines relationships between the UTAUT variables and CMMS adoption. The UTAUT survey used to understand how behavioral intention correlates to the success of CMMS adoption influenced by performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance effectiveness (Busdicker, & Upendra, 2017; Ehrenfeld, 2017; Harris, Mills, Fawson, & Johnson, 2018; Venkatesh et al., 2003; Venkatesh et al., 2012). The practical implication from advancing research on the behavior influences of the adoption of CMMS by IT managers in the Healthcare industry will improve operational cybersecurity measures by reducing the risk of data breaches in HDO's (Ehrenfeld, 2017; Martin et al., 2018). There is a need to establish accepted industry security controls providing HDO's capabilities to assess security governance risks across vast technology landscapes, multi-platform environments, and medical devices (Angst, Block, D'Arcy, & Kelley, 2017; Sittig, Belmont, & Singh, 2018; van Staa, Goldacre, Buchan, & Smeeth, 2016). This study will provide awareness into the behavior influences and security governance requirements required to promote the adoption of CMMS and improve HDO's cybersecurity measures.

Research indicates that HDO cybersecurity threats are increasing; resulting in security breaches that interrupt patient services, impact patient safety, and theft of patient data, these cybersecurity threats should be the highest priority for HDO's. Continued research in this area is required to support HDO's abilities to manage medical system security and assess security risks across vast technology landscapes, multi-platform environments, and medical devices. By providing the perceived behavior influences of the adoption of CMMS, IT managers in the Healthcare industry can use this study to improve security controls lowering the risks of cybersecurity threats (Ehrenfeld, 2017).

The quantitative, nonexperimental, correlational research design explores behavioral characteristics influencing the adoption of CMMS. The research design will follow a quantitative methodology approach in line with post-positivist philosophical assumptions (Singhry, Rahman, & Imm, 2016). This design will use a survey as the primary strategy of the investigation. The survey administered to participants is in the form of close-ended questions and Likert scale (1=*Strongly Disagree*, 7=*Strongly Agree*) questions. The study will use statistical tests and procedures to answer the research problem, question, and hypotheses about the behavior influence of the adoption of CMMS by IT managers in Healthcare (Field, 2013). The nonexperimental research will consist of an exploratory statistical model to discover statistical relationships between the adoption of CMMS based on the behavior influence in the healthcare industry. The Venkatesh et al., (2003) survey instrument variables and UTAUT model of been validated in prior studies before being introduced in the survey (Harris et al., 2018; Rezaei & Ghofranfarid, 2018; Van Hoof et al., 2018; Venkatesh et al., 2003; Venkatesh et al., 2012)

Fuad and Hsu (2018) demonstrated the application of the UTAUT theoretical framework using the four core determinants of performance expectancy, effort expectancy, social influence,

and facilitating conditions. These studies demonstrate the straightforwardness of the unified model to conform to the research study. Fuad and Hsu (2018) explored the adoption of healthcare information and communication technologies in developing countries. The study implemented all four core determining factors, performance expectancy, effort expectancy, social influence, and facilitating conditions to intention and use. The study previously indicated that technology was not voluntary, the experience was similar, and age did not appear to be significant in the developing countries. As a result, the moderating variables, age, voluntariness, and experience where remove, leaving only the moderating effect of gender. The results reinforced the usage of the unified model to understand the adoption of information and communication technologies. It appears the unified model provided additional knowledge to the factors influencing intention and usage by including the moderators and four core determinants. Arias-Oliva, Pelegrín-Borondo, and Matías-Clavero (2019) applied the unified model with the principle determining factors of performance expectancy, effort expectancy, and social influence in the adoption of the use of cryptocurrency technologies. The study did not include the facilitating conditions based on supporting research where the existence of performance and effort expectancy deems the facilitating conditions non-significant in behavioral intention. With relation to the moderator variables, social influence appears to impact behavioral intentions, consequently reasoning the moderator variables affected social influence.

The population targeted for this study consists of IT managers working for HDO organizations with a minimum of 5 years' experience in the healthcare industry. Similar to the population and sampling method used by Niranjan, Spulick, and Savitskie (2018), the study will use Qualtrics survey panel to identify IT managers working for HDO organizations targeted for the questionnaire. The questionnaires sent to the pre-selected subset of the target population and

filtered via a valid sampling method per the website Qualtrics. A variety of global companies and numerous business schools in the United States have used Quatltrics (Niranjan et al., 2018). Researchers have been successful using the Qualtrics platform for data collection. For example, Niranjan et al. (2018) stated that using Qualtrics is an efficient way to collect data with a resulting survey completion rate of nearly 87% (Niranjan et al., 2018).

Significance of the Study

The practical implication from advancing research on the behavior influences and information security governance of the adoption of CMMS by IT managers in the Healthcare industry will improve operational cybersecurity measures by reducing the risk of data breaches in HDO's (Ehrenfeld, 2017; Martin et al., 2018; Olavsrud, 2017). Due to continuous medical solution expansion, and direct HDO cybersecurity threats increase there are principles to establish accepted industry security controls for effective cybersecurity to reduce the risk of data breaches (Angst et al., 2017; Sittig et al., 2018; van Staa et al., 2016). This study will provide awareness into the behavior influences, cybersecurity controls, regulatory requirements required to promote the adoption of CMMS and improve HDO's cybersecurity measures.

Research indicates that HDO cybersecurity threats are increasing; resulting in security breaches that interrupt patient services, impact patient safety, and theft of patient data, these cybersecurity threats should be the highest priority for HDO's. Continued research in this area is required to support HDO's abilities to manage medical system security and assess security risks across vast technology landscapes, multi-platform environments, and medical devices. By providing the perceived behavior influences of the adoption of CMMS, IT managers in the Healthcare industry may be able to use this study to improve security controls lowering the risks of cybersecurity threats (Ehrenfeld, 2017; Olavsrud, 2017).

Research Questions

This study investigates the extent of performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance effectiveness impact the adoption of computerized maintenance management systems by IT managers in the healthcare industry. There are six research questions included in this study.

RQ1: To what extent does Performance Expectancy (PE) correlate to the adoption of a Computerized Maintenance Management System?

RQ2: To what extent does Effort Expectancy (EE) correlate to the adoption of a Computerized Maintenance Management System?

RQ3: To what extent does Social Influence (SI) correlate to the adoption of a Computerized Maintenance Management System?

RQ4: To what extent does Facilitating Conditions (FC) correlate the adoption of a Computerized Maintenance Management System?

RQ5: To what extent does Technology Security Governance Effectiveness (TSGE) correlate to the adoption of a Computerized Maintenance Management System?

RQ6: How well does performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance predict the adoption of computerized maintenance management systems?

Definition of Terms

Within the field of information security, UTAUT is frequently incorporated in scientific research to understand user acceptance of and compliance with information security solutions (Cohen, 2014; Harris et al., 2018; Venkatesh et al., 2003; Venkatesh et al., 2012). The UTAUT framework will help to recognize how behavior influences origins that affect the adoption of

CMMS. The UTAUT model advances that these constructs' performance expectancy, effort expectancy, and social influence are direct determinants of behavioral intention in the adoption and use of technology (Venkatesh et al., 2003). The following definitions represent the constructs and their usage in this study.

Computerized Maintenance Management System (CMMS). A measurement of the consumer's determination to consciously adopt a technology database of information about enterprise maintenance operations (Rezaei & Ghofranfarid, 2018; Venkatesh et al., 2003). Behavioral intention is a predictor of intention to adopt a technology, supported by the validation of UTAUT and associated technology adoption models (Davis, 1989; Rezaei, & Ghofranfarid, 2018; Venkatesh et al., 2003). CMMS is an ordinal level of measurement with the possible values of 1-7 indicating a ranking order: 7 indicating strong disagreement with the statement and 1 indicating strong agreement with the statement.

Effort expectancy (EI). The degree to which a consumer feels that a product or technology is easy to use (Venkatesh et al., 2012). For this study, EE applies to the intention to adopt CMMS. EE is an ordinal level of measurement with the possible values of 1-7 indicating a ranking order: 7 indicating strong disagreement with the statement and 1 indicating strong agreement with the statement.

Facilitating conditions. The degree to which an individual believes that organizational and technical structures are present that will provide the use of the new technology or system (Venkatesh et al., 2012). FC is an ordinal level of measurement with the possible values of 1-7 indicating a ranking order: 7 indicating strong disagreement with the statement and 1 indicating strong agreement with the statement.

Performance Expectancy (PE). The consumer's belief that a technology or product will provide a benefit to them when using it to complete an activity (Harris et al., 2018; Rezaei, & Ghofranfarid, 2018; Venkatesh et al., 2003; Venkatesh et al., 2012). PE is an ordinal level of measurement with the possible values of 1-7 indicating a ranking order: 7 indicating strong disagreement with the statement and 1 indicating strong agreement with the statement.

Social Influence (SE). A measurement of the impact that other people who are essential to the consumer's life have on the decision to adopt a product or technology (Harris et al., 2018; Rezaei, & Ghofranfarid, 2018; Venkatesh et al., 2003; Venkatesh et al., 2012). SI is an ordinal level of measurement with the possible values of 1-7 indicating a ranking order: 7 indicating strong disagreement with the statement and 1 indicating strong agreement with the statement.

Technology security governance effectiveness (TSGE). The degree a user understands the standard tools, processes, and methodologies that enable an organization to align business strategy and goals with IT services, infrastructure, or the environment. (Harris et al., 2018; Rezaei, & Ghofranfarid, 2018). TSGE is an ordinal level of measurement with the possible values of 1-7 indicating a ranking order: 7 indicating strong disagreement with the statement and 1 indicating strong agreement with the statement.

Research Design

The quantitative, nonexperimental, correlational research design explores the behavioral relationship on the adoption of CMMS. The research design will follow a quantitative methodology approach in line with post-positivist philosophical assumptions (Dedeurwaerdere, 2018). This design will use a survey as the primary strategy of the investigation (Sabi et al., 2016). The survey administered to participants is in the form of close-ended questions and Likert scale (1=*Strongly Disagree*, 7 = *Strongly Agree*) questions. The study will use statistical tests

and procedures to answer the research problem, question, and hypotheses about the behavior influence of the adoption of CMMS by IT managers in the Healthcare industry (Field, 2013). The nonexperimental research will consist of an explanatory statistical model to discover statistical relationships between the adoption of CMMS resulting from the behavioral influence in the healthcare industry. Once the consent form agreed to, participants clicked on the link to complete the survey. The Venkatesh et al., (2003) survey instrument variables and UTAUT model of been validated in prior studies before being introduced in the survey (Harris et al., 2018; Rezaei & Ghofranfarid, 2018; Van Hoof et al., 2018; Venkatesh et al., 2003; Venkatesh et al., 2012).

This quantitative, nonexperimental, correlative study has multiple independent and one dependent variables; therefore, Spearman's rank correlation coefficient (rho) used to perform statistical analysis on the data. Spearman's assesses the strength of the relationship between two variables (Laerd Statistics, 2018). As a result of the survey instrument using a seven-point likert scale to capture responses, easily translated into ordinal data points used to calculate the Spearman rank correlation coefficient. The Qualtrics survey collection service contacted the target population to participate in the computerized maintenance management system study via the online platform. Once participants agreed to the consent form, the link to complete the survey provided. Once the survey finished, the data was downloaded and analyzed.

Assumptions and Limitations

Assumptions

This research study makes the following assumptions to guide the study in information security governance and the impact on the adoption of computerized maintenance management systems.

General methodological assumptions. This study uses inferential statistics and Spearman's correlation analysis, assuming that variables normally distributed and a linear relationship exists between dependent and independent variables without error, and data homodascity exists. The assumption made that respondents answer the survey questions truthfully and reflective of actual viewpoints that are randomly selected from the study populations removing sampling bias.

Theoretical assumptions. Theoretical assumptions are evidence that relationships exist between the unified theory of acceptance and usage of technology and CMMS. The assumptions made that the UTAUT variables are accurate to describe the adoption level of an organization

Topic-specific assumptions. There is an expectation that the participants are familiar with NIST SP 800-53 security controls and CMMS. Qualifying survey questions used to determine that the participant's work in both the field of information technology and healthcare industry. Another assumption was that the participants were responsible for, or involved in, the process of adopting information security frameworks and security controls within their organization. Qualifying survey questions used to determine the participant's involvement within their organization concerning the adoption of information security standards.

Assumptions about measures. This quantitative, nonexperimental, correlational study also includes the following assumptions: the survey instrument uses a large enough Likert scale; participants respond and view the measurements in a similar manner; and participants uniformly view measures.

Limitations

This research study has the following limitations guiding the study in information security governance and the impact on the adoption of computerized maintenance management systems.

Design limitations. This quantitative, nonexperimental, correlational study is limited to using the UTAUT characteristics influencing the adoption of computerized maintenance management systems and could be further expanded to include other theoretical frameworks such as the technology acceptance model developed by Davis (1989). The survey was explicitly limited to technology professionals in a management role. The management role was described by the individual's title in the organization and was not dependent on an explicitly defined supervisory role. The study was also explicitly limited to computer maintenance management systems and did not include other inventory technologies used in the healthcare industry.

Delimitations. The sample of IT managers is representative of IT managers in the United States healthcare industry, and the limitation is that this study is not representative of all geographies and regions. The randomness of the target sample is present since the Qualtrics survey panel identifies the respondents, and each participant had the opportunity to complete the survey. Fowler (2009) indicated that non-response is a potential source of bias in voluntary studies. For this study, non-response addressed by identifying the target sample size to the Qaultrics survey provider and obtaining the participants through the audience survey panel. Additionally, because all answers are confidential with personal identification information deleted, the assumption made that respondent's answers were truthful because there would be no fear of consequences.

Organization of the Remainder of the Study

Chapter 1 provides the background of the study and the benefits to the academic and professional fields. In addition, the research design assumptions and limitations provided. Chapter 2 includes a review of the scholarly literature related to information security governance, and the unified theory of acceptance and use of technology impact the adoption of computerized computer maintenance management systems. Chapter 3 describes the research methodology, research design, population, sample, and data collection techniques. Chapter 4 presents the analysis of the survey data and the findings of the extent that the effectiveness of technology security governance, performance expectancy, effort expectancy, social influence, and facilitating conditions impact on the adoption of Computerized Maintenance Management System. Chapter 5 summarizes the research results and provides recommendations and conclusions resulting from the data analysis.

CHAPTER 2. LITERATURE REVIEW

Current research indicates that cybersecurity threats against healthcare delivery organizations (HDO) are increasing, resulting in security breaches that interrupt patient services and cause the loss of patient data solutions (Au et al., 2017). This literature emphasizes that it is essential to learn from cybersecurity mistakes and incorporate those lessons learned into identifying cybersecurity framework gaps and make improvements (Knowles et al., 2015). Over the past decade, healthcare technology has continued to evolve and improve at an incredible rate. Healthcare medical devices, platforms, and the Internet of things (IoT) device cybersecurity preparedness is a relatively new field of study in the scholarly community compared to their standard technology industry driven counterparts (Knowles et al., 2015). Standard technology-driven industries such as finance, government, commercial, and manufacturing secure technologies through standard security controls such as the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), or International Electrotechnical Commission (IEC) (Au et al., 2017). Studies indicate that the complexity of healthcare environments is a reason why HDOs are not implementing information security governance supporting security programs and the proper cybersecurity control measures at a faster pace to protect against cyber threats (Chen et al., 2016).

Methods of Searching

Capella University's library is the primary source of information for the literature review, including academic search, ProQuest, and google scholar sources. Scholarly peer-reviewed articles are the base of data. The library search consisted of the terms information security governance, computerized maintenance management systems, and the unified theory of acceptance and use of technology. Results were further refined using the AND operator so that

results contained all of the defined terms used. Abstracts and references imported into RefWorks to summarize all articles in an annotated bibliography and remove duplicate sources.

Theoretical Orientation for the Study

The theoretical foundation used in this study is the UTAUT to examine the relationship between Technology security governance effectiveness, behavioral intention, social influence, effort expectancy, and performance expectancy on the impact of Computerized Maintenance Management System (CMMS) by IT managers in the Healthcare industry: A nonexperimental correlational design (Venkatesh et al., 2003). UTAUT is the most widely used model to recognize the acceptance of different types of information systems and technologies (Harris et al., 2018; Venkatesh et al., 2003; Venkatesh et al., 2012). Explicit to the field of information security, UTAUT has been used in scientific research to understand user acceptance of and compliance with Information Security solutions (Harris et al., 2018; Venkatesh et al., 2003; Venkatesh et al., 2012). The UTAUT framework will help to recognize how behavior influences origins that affect the adoption of Computerized Management Maintenance Systems (CMMS) based on Venkatesh et al., (2003).

The study will test to confirm the Theory of Acceptance and Use of Technology (UTAUT) (Harris et al., 2018; Venkatesh et al., 2003; Venkatesh et al., 2012) by contributing new information about its application of technology security governance effectiveness, social influence, effort expectancy, performance expectancy, and behavioral intention as it relates to the influence on the adoption of Computerized Management Maintenance Systems (CMMS) by IT managers in the Healthcare industry (Busdicker, & Upendra, 2017; Ehrenfeld, 2017; Harris et al., 2018; Venkatesh et al., 2003; Venkatesh et al., 2012). The theoretical implications should test to confirm the Unified Theory of Acceptance and Use of Technology (UTAUT) in the field of

information technology security and assurance by contributing new information about its association and effect of technology security governance effectiveness, social influence, effort expectancy, performance expectancy, and behavioral intention as it relates to the influence on the adoption of Computerized Management Maintenance Systems (CMMS) by IT managers in the Healthcare industry (Harris et al., 2018; Rezaei, & Ghofranfarid, 2018; Van Hoof et al., 2018; Venkatesh et al., 2003;Venkatesh et al., 2012)

Review of the Literature

Health Delivery Organizations Security

As the healthcare technology solutions of serving patient needs have increased in effectiveness and robustness, attackers are converging on these solutions, medical devices, platforms, and the Internet of things (IoT) devices to find new means to accomplish hacking objectives (Jamkhaneh et al., 2018). HDOs experienced a global cyber-attack by these attackers in the method of ransomware branded as WannaCry and Petya (Busdicker, & Upendra, 2017). The WannaCry and Petya attacks directed towards healthcare systems running on Microsoft Windows operating systems. The WannaCry crypto worm and Petya malware brought down more than 300,000 systems affecting HDOs in 150 countries by encrypting data and demanding ransom payments to decrypt the data (Busdicker, & Upendra, 2017). Following these attacks, the Ponemon Institute shared the results of a survey that showed only 15% of healthcare HDOs were taking significant steps to prevent cyber-attacks (Busdicker, & Upendra, 2017). Data sources and search reviews of current healthcare cyber threats by Coventry and Branley (2018) examines why healthcare is becoming a primary target for hackers. Within the last few years, the healthcare industry has experienced a historic increase in data breaches; these data breaches result in financial loss, loss of reputation, and impact on patient safety. The average cost to an

HDO for one pilfered healthcare record containing sensitive and confidential information, according to the Coventry and Branley (2018) study, is $380.

A recent review of literature conducted by Argaw, Bempong, Eshaya-Chauvin, and Flahault (2019) used a methodological framework following the preferred reporting items for systematic meta-analyses guidelines (PRISMA) to examine the state of research on cyber-attacks on HDOs and available best practice recommendations. This study showed that of the literature selected for review, 32% were published post-WannaCry and Petya attacks and 40% of the literature published before the previous three years (Argaw et al., 2019). The study revealed that the security of connected medical devices and equipment was a primary emphasis in the literature. Medical devices and solutions are separate systems from the HDO information technology (IT) infrastructure and support; it lacks the essential security protections that are critical to prevent cybersecurity attacks (Argaw et al., 2019). Among the recommendations found in this study is that HDO organizations need to assign more resources and funding to IT security to support medical devices and solutions. A significant limitation in the study was that only research available in English was used, which excluded numerous significant publications from countries with progressive cybersecurity practices (Argaw et al., 2019).

A study by McLeod and Dolezel (2018) examined the breach exposer, levels of security, and organization facts associated with healthcare security breaches. Using the NIST tactical security risk triangle of technology, business processes, and organizational influences, the study examined recognized industry security controls and the Department of Health and Human Services data breach data to determine the levels of risk exposure, security and organizational failures that lead to a security breach (McLeod & Dolezel, 2018). The results of the research showed that the complexities of large-scale organization, diversity of medical devices and

solutions, lack of funding, and low adherence to security standards are the contributing factors that lead to security breaches (McLeod & Dolezel, 2018). Legacy devices and solutions are pointed out as primary factors of risk; these are medical solutions that are at the end of life or end of support. Legacy devices and solutions have no security updates available they are primary threat targets. Asset management identified as a significant risk factor. The study references standardizing operational security controls on the International Electrotechnical Commission security controls IEC 80001 and the International Organization for Standardization (ISO) and NIST the National Institute of Standards and Technology cybersecurity framework to remove gaps in HDO medical device and solutions cybersecurity (McLeod & Dolezel, 2018).

Information Security Governance

The literature reviewed identifies laws, acts, and regulations that HDOs must comply with to protect patient information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and The Health Information Technology for Economic and Clinical Health Act (HITECH) are two frequently cited regulations (Kruse et al., 2017). The HIPAA privacy rule, in general, involves patient authorization for releasing personal health information (PHI). HIPAA promulgated, in part, to allow PHI use by researchers, investigators, and the commercial industry without patient authorization (Cohen, 2014). HITECH presented with new requirements addressing security, privacy concerns with electronic health (Sullivan, 2009). The HITECH Act specifies protocols, importance, and consequences for reporting data breaches (Kruse et al., 2017). A systematic review of 25 academic journals by Kruse et al. (2017) pursues to understand the security measures that healthcare organizations find most important when complying with HIPAA and HITECH. The study exposed that firewalls to protect the healthcare organizations' information technology systems, physical access controls limiting physical access to resources,

and administrative safeguards in the form of policies, practices, and procedures were the most commonly discussed within the academic journals.

The US Food and Drug Administration (FDA), through the 510k medical device certification process, controls the safety of medical devices and solutions. The United States Congress gave the FDA the authority to regulate medical devices by amending the Food, Drug, and Cosmetics Act in 1976, leading to the creation of the 510(k) review process (Owens, 2016). These devices can be on-body wearable, implantable systems, and large non-portable devices for diagnosis or treatment such as ultrasounds, infusion pumps, ventilators, and medical lasers located in HDO facilities. The FDA first implemented cybersecurity guidelines for medical devices (Owens, 2016). The guidelines based on the NIST critical infrastructure cybersecurity framework modified with appropriate recommendations for medical devices and solutions (Owens, 2016). The new guidelines Owens, (2016) emphasizes project to inspire device manufacturers to plan, monitor proactively, and respond to potential cybersecurity vulnerabilities in medical devices in the market. These guidelines did not require medical device manufacturers to build cybersecurity measures into the devices.

The recent security breaches of hospitals and health insurance organizations worldwide have brought forward from HDOs the call for stricter FDA cybersecurity regulations for medical devices and solutions (Yuan, Fernando, & Klonoff, 2018). New draft FDA cybersecurity guidelines were formed and released for comments (Yuan et al., 2018). The new draft FDA guidelines now focus on the manufacturer's integration of risk management in the product development lifecycle. Additionally, the guidelines recommend that manufacturers monitor for vulnerability throughout the product management lifecycle and update products to protect against known threats (Yuan et al., 2018). The FDA's new draft guidance documents, once

officially approved, will remain optional to manufacturers, i.e., will not be required by law (Yuan et al., 2018). The new guidelines are limited in scope, as Yuan et al. (2018) explain; the FDA will not be evaluating the risk assessment process implemented by manufacturers. Additionally, the guidelines do not require any security control standards for manufacturers to prevent cybersecurity threats (Yuan et al., 2018).

Computerized Maintenance Management Systems (CMMS)

A systematic, organizational prospective study of chief information officers, chief information security officers, and health care cybersecurity experts by Jalali and Kaiser (2018) also concluded that resources and funding of IT security to support medical devices are needed to advance HDO security initiatives. The Jalali and Kaiser (2018) study also indicated that resources are not the primary problem for HDOs; the focus should be on reducing endpoint complexities and cultivating internal stakeholder alignment to solve cybersecurity problems more effectively. Industry leaders, technology professionals, and HDO considerations, centered on endpoint complexities, are addressed in numerous articles after the global malware Wannacry event. The sheer numbers and diversity of medical devices and solutions that HDOs manage highlight the need for centralized solutions that maintain, monitor and implement required security updates (Argaw et al., 2019). Jamkhaneh et al. (2018) emphasize that a robust computerized maintained management system (CMMS) is necessary for HDO technology managers to be cost-effective and efficient in managing medical solutions. The essential functions of CMMS are asset management, preventive maintenance scheduling, including maintenance history, required for operations and standards compliance. An all-inclusive CMMS can provide HDO technology managers and professionals the analytical tools they need to advance cybersecurity measures to reduce risk and decrease costs (Jamkhaneh et al., 2018).

The necessary information in CMMS has the potential to provide support for cybersecurity measures and reduce risk when a vulnerability or threat advisory received for medical solutions, network system properties, software revisions, OS versions, and software patch levels (Copeland, 2018). A recent empirical research study by Jamkhaneh et al. (2018) to investigate the impacts of CMMS and appropriate supportive organizational influences on the efficiency of over-all productive maintenance established that organizations that utilize CMMS are decision-makers that are more effective across systems when identifying potential risks before a security event. Although the effectiveness of applying CMMS is considered essential to management standards providing strategic and operational benefits, the Copeland, (2018) study stresses that the adoption rate of CMMS is slow across many industries. The Jamkhaneh et al. (2018) study highlights the principles that CMMS used in industrialized multifaceted organizations increase strategic, operational effectiveness and decrease maintenance costs.

A comprehensive review of literature by Fraser, Hvolby, and Tseng (2015) set forth to determine and categorize the various maintenance management models, and to understand the availability of empirical evidence. The study intended to identify the primary maintenance management models in the current empirical literature to examine the practical examples and empirical evidence rates for maintenance-associated literature (Fraser et al., 2015). Within the considered literature, Fraser et al. (2015) identified 37 maintenance management models from these; three prominent models established to be prevalent: total productive maintenance (TPM), condition-based maintenance, and reliability-centered maintenance. The most recent literature also identified CMMS; in the study, Fraser et al. (2015) align TPM with CMMS as being similar models, noting CMMS is an electronic form of TPM. The study focused on 82 articles with empirical evidence, and of those, the automotive industry was the most prevalent studied. TPM

was the most widely studied model. The review of the literature concluded a steady decline in empirical studies from the nineties onwards and the introduction CMMS (Argaw et al., 2019). The use of maintenance management in healthcare identified in the modern industries of study. The outcome of this research Fraser et al. (2015) hopes to influence the current attitudes of future researchers by demonstrating two primary issues; first, the importance of maintenance management to new organizations, and second, the decline and absence of credible academic research of maintenance management practice.

Technology in the healthcare industry is going through radical changes due to the advancement and interoperability of electronic health record (EHR) systems, medical devices, and the services, platforms, provisioned and managed by third parties. The responsibility of management and maintenance of these systems and solutions falls on the healthcare delivery organizations (HDO). The fast pace of technology growth, a vast number of unique and complex networked solutions, the internet of things (IoT) category devices, and the absence of adequate maintenance has led to vulnerabilities resulting in significant HDO security breaches (Busdicker & Upendra, 2017). Industry leaders and current research point to the implementation of Computerized Maintenance Management Systems (CMMS) as a preeminent approach an HDO can implement to manage distributed complex environments. Resistance, confidence, ease of use, and competency can challenge the usage and adoption of CMMS technologies (Coventry & Branley, 2018). Several established theoretical technology acceptance models in use today can assist in identifying factors that influence the adoption and use of CMMS technologies. The examination of the theory of acceptance (TAM), the theory of reasoned (TRA), and the acceptance and use of technology (UTAUT) models in each section below explains the

constructs of each model and the effects of research studies applying the model's aptness in a study on adopting CMMS.

The theory of reasoned action defined by Fishbein and Ajzen (1975) consists of two primary elements related to an individual's intention to perform a behavior, attitude relating to the behavior, and subjective norm connecting to the behavior. The subject norm directly influenced by peer pressure or stimulus by a person who has perceived authority, known as social influencers (Fishbein & Ajzen, 1975). Both attitude and subjective norms determine behavior, the theory of reasoned action designates the performance of an action and behavior specified by the behavioral intention to perform the behavior and the norms connected to the specific behavior (Fishbein & Ajzen, 1975). Davis, Bagozzi, and Warshaw (1989) clarified attributes of this theory by integrating an individual's behavior is resolute by intent and is a function of the person's subjective norms towards the conditions that influence that action.

Fishbein & Ajzen, to postulate social behavior, established the theory of reasoned action (Davis, 1989). The foundational principles of the theory of reasoned actions are beliefs, attitudes, intentions, and behaviors (Davis, 1989). As a theoretical framework, Fishbein and Ajzen (1975) explain that a person's belief about a goal or activity forms the attitude towards that purpose. Consequently, the measurements of attitudes are beliefs (Davis, 1989). The positive or negative feelings toward a purpose represent a person's attitude. The intention is the choice of the person to perform or not perform the behavior. The Theory of Reasoned Action provides a conceptual model for investigating and measuring human behavior.

Two independent variables, attitude and subjective norm, extend the theory of reasoned action to behavioral intention (Fishbein & Ajzen, 1975). Further, outward variables that are implicit in influencing behavioral intention extend to the effects on attitudes or subjective norms.

The model used in research relies on theses outward variables as significant factors influencing attitude or subjective norms (Davis et al., 1989). The relevant influencing factors in this model are behavioral boundaries (Fishbein & Ajzen, 1975). Research behavior boundaries include volition or the power of choice; performance before the behavior, the intent remains the same (Fishbein & Ajzen, 1975). Various studies incorporated the Fishbein & Ajzen model, which specified an action, target, context time, and specificity for their research (Lai, 2017). The model aligns attitude and intention to the action, target, context, and timeframe (Mishra, Akman, & Mishra, 2014). The action refers to CMMS; target refers to CMMS in all healthcare delivery organizations, context refers to financial data; timeframe and specificity remain consistent across all healthcare organizations. The various studies reviewed illustrate the theory of reasoned action model strength for evaluating the performance of behavior and intentions.

The technology acceptance model derives from the Fishbein and Ajzen (1975) theory of reasoned action. As the research need for a technology proven model to determine user acceptance cultivated, Davis (1989) developed the technology acceptance model (TAM). Two research studies by Davis (1989) and Davis et al., (1989) presented the technology acceptance model, which Venkatesh et al. (2012) highlighted as cited more the 1000 times. The model follows the theory of reasoned action as the grounds to specify the fundamental connection between the two primary determining factors, perceived ease of use and perceived usefulness, to explain computer adoption behavior minus the subjective norm variable on the belief it has minimal impact on behavioral intention towards user acceptance (Davis et al., 1989).

The technology acceptance model consists of a minimum total of variables as causative factors to technology acceptance (Davis et al., (1989). The model employs constructs, perceived usefulness, and perceived ease of use has two independent variables. These two independent

variables are the primary determining factor of user acceptance. Perceived usefulness determined by the degree to which the user perceives the particular technology will enhance job performance (Davis et al., 1989). The user may sense that job performance has improved by technology. Perceived ease of use speaks to the amount the user perceives the particular technology to be effortless (Davis et al., 1989). The theory of reasoned action causative factor of the belief attitude variable is comparable to the technology acceptance model ease of use and usefulness variable. (Taherdoost, 2018). The technology acceptance model, as indicated by Venkatesh et al., (2012), is the perception of usefulness and the perceived ease of use that influences the user's intention to use technology that persuades the user's behavior to use the technology. The straightforwardness of the model explains the extensive usage of various technologies, acceptance, adoption, and decision-making research studies (Taherdoost, 2018; Venkatesh et al., 2012).

Information acceptance research has produced various contending models, each of which has different groups of acceptance determining factors (Venkatesh et al., 2003). In their research Venkatesh, et al. (2003) reviewed user acceptance works of eight prominent models and empirically compared them to formulate a unified model that adapted elements to develop the unified theory of acceptance and usage of technology. The eight prominent technology acceptance models are: (a) theory of reasoned action; (b) technology acceptance model; (c) motivational model; (d) theory of planned behavior; (e) the combined technology acceptance model and theory of planned behavior; (f) innovation diffusion theory; (g) the model of personal computer utilization; and (h) social cognitive theory. The technology acceptance model extends to the unified theory of acceptance and use of technology by adding the performance expectancy,

effort expectancy, and social influence constructs. These added constructs are influences of behavioral intent and technology usage (Venkatesh et al., 2003).

The unified theory of acceptance and use of technology comprises of these subsequent constructs: performance expectancy, effort expectancy, social influence, facilitating conditions, behavioral intention, and use behavior with the controlling variables of experience, voluntariness, gender, and age (Venkatesh et al., 2003). Performance expectancy, effort expectancy, and social influence are the three direct determining factors of intention, which is associated with the intention of use and facilitating conditions as the direct determining factor of usage (Venkatesh et al., 2003). The degree to which a user considers the technology supportive of achieving job performance connects to the construct of performance expectancy, which correlates to the technology acceptance model perceived usefulness. Performance expectancy refers to the perception of technology effectiveness, user's expectations for using, and impact on job performance by technology (Venkatesh et al., 2003).

The technology acceptance model perceived ease of use connects to effort expectancy: the degree of experience and technology ease of use. Social influence originates from the theory of reasoned actions and comparable to the subjective norms. The social influence construct refers to the user's impression of other people considering the technology as well as how technology measures into the social norms, feeling in reverences to if they should or should not use the technology, and the user perception of self-image (Venkatesh et al., 2003). The final determining factor relates to the facilitating conditions. Facilitating conditions is the degree a user believes there is backing for the technology mutually from the organization and technical infrastructure (Venkatesh et al., 2003). Facilitating conditions are inclusive with training and the resources required using the technology. The Venkatesh et al., 2003 unified theory of acceptance and use

of technology model design of moderators; age, gender, experience, and voluntariness moderate the effect of performance expectancy, effort expectancy, and social influence to remove weakness between their associations.

Several research studies conducted corroborated testing to validate the theory of reasoned action (Mceachan et al., 2016; Mishra et al., 2014; Mital, Chang, Choudhary, Papa, & Pani, 2018; Sher et al., 2017). Mceachan et al. (2016) conducted a meta-analysis to determine the efficiency of the TRA model. The examination provided robust evidence of the correlative effectiveness even though the majority studies expanded the above-stated boundary conditions. The theory of reasoned action model effectively predicts and expounds behavior across various domains (Davis et al., 1989; Dutot, Bhatiasevi, & Bellallahom, 2019; Lai, 2017).

Mishra et al. (2014) implemented the model to investigate the relationship between information technology specialists' behavior towards green information technology to examine the relationship between consciousness about renewable energy and beliefs about significant consequences of using renewable energy. The model expanded to include individual differences and situational constraints. The model considered appropriate in suggesting a relationship exists between the experience of respondents and the level of awareness making for the sample data. Sher et al. (2017) applied the theory of reasoned action to the area of perceived vulnerability and perceived severity (threat of EMR breaches) by expanding the model. The results indicate that the model adequately explains the information technology staff's fear-arousal concerning the threat of EMR breaches and significantly predicts the IT staff member's intention to comply with the stated privacy policy. Both studies did not expand the model for technology because it did not relate to the use of technology but the intention of using renewable energy and privacy policies.

There is an influence of the theory of reasoned action on research in technology. Liker and Sindi (1997) expanded the model to include technology aimed at determining the potential influence of expert systems. The model extended to include the impact of Expert Systems to the workplace affected by the challenges faced by management. Liker and Sindi (1997) extended variables comprised of the system characteristics: ease of use and user characteristics: age, education, and user involvement. The resulting extended measures focused on attitude toward the systems and intentions to use the system. Attitude toward the Expert Systems and intentions to use the Expert Systems were the outcome measures. The study indicated that the theory of reasoned actions behavioral constructs alone were not sufficient to recognize and determine the technology use characteristics and attitudes to establishing technology use.

Current empirical research in technology by Mital et al. 2018 proposed an exploratory study using the Structured Equation Model (SEM) method to examine the adoption of internet of things (IoT) from a multiple theory perspective, precisely, the theory of reasoned action, the theory of planned behavior and the technology acceptance model. This research objective was to test three contending models from the viewpoint of the adoption of IoT devices. Utilizing the primary constructs of each model, Mital et al., 2018 concluded based on the goodness to fit index that both theories of reasoned action and technology acceptance model assisted in predicting the intention to use IoT. Mital et al., 2018 conclude in some measure all three models on their own, lack adequate dimensions to explain the intention to use IoT based devices and that the theory of planned behavior cannot predict the intention to use IoT since the perceived behavior.

Venkatesh et al. (2012) emphasized that the technology acceptance model has been cited more the 1000 times, demonstrating widespread usage across various domains. Young, Park and Lim, (2018) compared the model in three different Korean country provinces by distributing a

survey to the teachers of three different universities on the adoption of integrated knowledge of teaching, content, and technology, called Technology Pedagogy and Content Knowledge (TPACK). The results indicated that the model might not predict the intention to use technology across different cultures with the results signifying cultural factors affecting the adoption and utilization of technology.

The volume of citations referring to Davis (1989) and Davis et al. (1989) along with the utilization of the model in various technologies Venkatesh et al., (2012) reached the conclusion that researchers in the information technology field refer to the model as their distinguishable theory and continue to extend the model's variables. Comparable to the research articles reviewed for the theory of reasoned action, the technology acceptance model similarly expands the variables in the research applying the model. Meta-analyses research by Tractinsky, (2018) discussed the model's usefulness suggestive of the continued extension of the variables extending to an organization and social factors routinely addressed in research to broaden its usage to include personal and social change aligned with various phases of technology implementation. Tractinsky (2018) suggested improvements in the canopies of measurements for the technology used as a relative indicator compared to the current measure referring to the variance in variables for usage. In the Hess, McNab, and Basoglu (2014) meta-analyses, researchers presented more than fifty external variables linking to perceived ease of use and perceived usefulness to provide a comprehensive understanding of variables influencing these principles. Wang and Goh (2017) and Fedorko, Bacik, and Gavurova (2018) research provided representations on expanding the technology acceptance model critical variables to identify determinants impacting perceived ease of use and perceived usefulness.

Fedorko et al., (2018) determined the aspects of selected users adopting e-commerce web site visiting technology, namely an e-business for social commerce that combines the commercial and social activities by deploying social technologies into e-commerce sites. The study indicated the model performed reasonably well in the context of e-business but required the modification of the original technology acceptance model with other constructs. Specifically, to address considerations for modern technologies such as social network and mobile applications that affect the use of e-commerce before implementing the technology. Wang and Goh's (2017) meta-analysis examined the perceived enjoyment of the usage behavior of video games. The model extended with perceived enjoyment, referring to the degree to which the activity of using the computer perceived to be enjoyable, affecting perceived usefulness and perceived ease of use (Wang & Goh, 2017). The results of the study indicated that game type significantly weakened the associations between perceptions and acceptance, influencing both perceived usefulness and perceived ease of use. Wang and Goh (2017) research concluded that the perceived enjoyment equally influenced the association between the perceived ease of use, perceived usefulness, and user acceptance.

Fuad and Hsu (2018) demonstrated the application of the UTAUT theoretical framework using the four core determinants of performance expectancy, effort expectancy, social influence, and facilitating conditions. These studies demonstrate the straightforwardness of the unified model to conform to the research study. Fuad and Hsu (2018) explored the adoption of healthcare information and communication technologies in developing countries. The study implemented all four core determining factors, performance expectancy, effort expectancy, social influence, and facilitating conditions to intention and use. The study previously indicated that technology was not voluntary, the experience was similar, and age did not appear to be

significant in the developing countries. As a result, the moderating variables, age, voluntariness, and experience where remove, leaving only the moderating effect of gender. The results reinforced the usage of the unified model to understand the adoption of information and communication technologies. It appears the unified model provided additional knowledge to the factors influencing intention and usage by including the moderators and four core determinants.

Arias-Oliva et al. (2019) applied the unified model with the principle determining factors of performance expectancy, effort expectancy, and social influence in the adoption of the use of cryptocurrency technologies. The study did not include the facilitating conditions based on supporting research where the existence of performance and effort expectancy deems the facilitating conditions non-significant in behavioral intention. The model modification presented by Arias-Oliva et al. (2019) predicts 53% of technology acceptance versus the 70% prediction of technology acceptance defined in the UTUAT model established by Venkatesh et al. (2003). With relation to the moderator variables, social influence appears to impact behavioral intentions consequently reasoning the moderator variables affected social influence.

The preceding sections examined the theory of reasoned action, technology acceptance model, and the unified theory of acceptance and use of technology acceptance models to determine the suitability of each for a study in the adoption of CMMS. The theory of reasoned action consists of two independent variables, which are limited to attitude and subjective norm, and relate to behavioral intention (Fishbein & Ajzen, 1975). Expanding the theory of reasoned action, Davis (1989) created the technology acceptance model with the two independent variables of perceived usefulness and perceived ease of use as the primary determinants of user acceptance. The unified theory of acceptance and use of technology-based on eight models, which encompasses the theory of reasoned action and technology acceptance model. The unified

model has four independent variables; performance expectancy, effort expectancy, social influence, facilitating conditions as the principal determining factors of behavioral intention, and user behavior. The moderating variables in the unified theory include; experience, voluntariness, gender, and age. After understanding the variables and analyzing the current usage of the models, and evaluation performed to qualify the utilization of each model for information security governance related to CMMS adoption,

The theory of reasoned action considered unsuitable due to the weakening viability when the model is used outside of its boundaries (Dutot et al., 2019; Lai, 2017). The study in adopting CMMS will require the model to expand outside of the boundaries to include security factors. The existing model requires an extension of the boundaries to take account of, not limited to, financial, security, legal, resources, demographic factors, and it does not include an obvious choice among alternatives, which weakens its viability. As determined by Per Lai (2017), the model is not appropriate when an individual cannot execute the action even when there are strong intentions. Relating to the adoption of CMMS, the person may have strong intentions to adopt CCMS, but there are limitations due to financial, security, or resource concerns. Based on previous research and recommendations, the theory of reasoned action deemed unsuitable for the study in adopting CMMS.

The technology acceptance model appears to be suitable for a study in adopting CMMS due to the meta-analysis studies of information technology researchers supporting the usage along with the straightforwardness of expanding the variables. Since the study of CMMS will involve several security variables as moderating variables, the association between the independent and dependent variables weakens influencing the reliability of the study (Wang & Goh, 2017). The unified theory of acceptance and use technology is also suitable in the adoption

of CMMS based on the notion of integrating various models and that addresses the limitations identified in the theory of reasoned actions and technology acceptance model. The unified theory of acceptance and use technology provides moderating variables influencing the principal determining factors contrasting the theory of reasoned action model that defines the relevant factors influencing attitude or subjective norms (Davis et al., 1989). By providing the moderating variables, the weakening of the association between the determining factors lessens. The Venkatesh et al. (2003) research makes a strong case for using the unified theory of acceptance and uses technology over the technology acceptance model by showing it as 40% to 50% more explanatory power regarding the end user's behaviors or behavioral intention to use.

Impacts of the Computerized Maintenance Management System

Jamkhaneh et al. (2018) perform a quantitative study on the impacts of computerized maintenance management systems (CMMS) and supportive organizational factors on total productivity. With the rapid evolution of technology, companies are focusing on implementing an automated system to increase workforce capabilities. The authors use quantitative survey-based research to conduct their investigation and receive 125 questionnaires from 60 Iran based manufacturing enterprises to validate and test the hypothesis along with theoretical framework (Jamkhaneh et al., 2018). Out of the 206 questionnaires distributed, 133 questionnaires received, and 125 deemed suitable for data analysis. The authors were able to test the construct validity of the questionnaires using confirmatory factor analysis. The study attempts to close the knowledge gap by identifying aspects of computerized maintenance management systems and relevant organization factors that promote productivity within the workplace. Alreemy, Chang, Walters, and Wills (2016) indicate that a short forecast for required IT resources' is the main problem found in technology security governance for enterprises surveyed. The findings of Jamkhaneh et

al. (2018) study reveals that CMMS positively relates to organization factors, including resource allocation, decision-making structure, employees' involvement, management support, and practical instruction. This result is in line with research performed by Rastegari and Mobin (2016) that indicate CMMS reduces project durations by assisting with planning management and offering real-time management schedules. The study concludes that the combination of CMMS and enterprise influences increase overall productivity and efficiencies within manufacturing companies located in Iran (Jamkhaneh et al., 2018).

Determinants of Master Data Management Adoption

An empirical study conducted by Haneem, Kama, Taskin, Pauleen, and Bakar (2019) examined the determinants of master data management (MDM) adoption. Data quality, governance, complexity, management support, technological competence, demand, relative advantage, security, and regulatory variables researched to evaluate if there is a relationship with the acceptance of MDM technology. The authors expand the technology-organization-environment (TOE) theoretical framework developed by Tornatzky, Fleischer, and Chakrabarti (1990) to conduct the study. The methodology of the study bases itself on structural equation modeling quantitative research techniques consisting of conceptual model construction, instrument development, data collection, and model validation (Hayes, Montoya, & Rockwood, 2017). To determine the extent of data quality, governance, complexity, management support, technological competence, demand, relative advantage, security, and regulatory factors affect MDM adoption, 465 surveys issued to the sample target population, and 224 valid responses received. The target population for the study is the local government organization in Malaysia, resulting in the authors distributing the survey to a sample set of participants working for the Malaysian government. Using the structural equation modeling partial least squares (SEM-PLS)

approach, developed by Sarstedt, Ringle, Smith, Reams, and Hair (2014), a two-phase analysis revealed the relationship between variables and MDM acceptance. The findings indicate that: data quality and governance are two determinants of MDM adoption; complexity, management support, technological competence, and demand have a significant effect on MDM acceptance; however relative advantage, security, and regulatory factors have a non-significant impact to MDM adoption specific to the context of the Malaysian local government (Haneem et al., 2019). The study focused on constructing and validating the TOE framework by applying it to master data management systems and results. In conclusion, an organization can benefit from Haneem, et al. (2019) research by identifying and addressing critical success in order to implement MDM systems successfully.

The Barriers and Facilitators to the Adoption of New Technologies

The qualitative study performed by Hadban, Yusof, and Hashim (2017) explored the barriers and facilitators to the adoption of new technologies in the public healthcare sector. The study investigated the opinion of healthcare professionals about the factors influencing the acceptance of technology using semi-structured interviews. Twenty-six themes emerged from the interviewee's responses that helped explore the phenomenon related to technology adoption in Iraqi public hospitals (Hadban et al., 2017). Information security governance, including standardization, management support, and compliance, are prominent factors influencing technology acceptance by healthcare professionals, and understanding the opinions of different healthcare professionals assisted with looking at the situation from different perspectives on the adoption of computerized maintenance management systems. Qualitative methods use purposeful sampling selection criteria for choosing participants (Etikan, Musa, & Alkassim, 2016). The study identified two hospitals located in Iraq to complete their study and identified

eight participants to take part in the one-on-one interviews. The study performed by Hadban et al. (2017) used the maximal variation sampling by selecting a small number of respondents that maximize diversity relevant to the adoption of maintenance systems by healthcare organizations. The healthcare staff voiced concerns about governance factors, including training, management support, data security, and privacy on the adoption of technology (Hadban et al., 2017; Wilkin, Couchman, Sohal, & Zutshi, 2016). Future research can involve several directions, including conducting quantitative studies that would incorporate the twenty-six themes highlighted in the study into technology adoption theories and retrieve responses on a large sample of participants to allow generalization of the findings.

Research Method Strengths and Weaknesses

Quantitative and qualitative research methods are not a hierarchy of excellence, as different techniques are appropriate for addressing different research questions. Qualitative methods focus primarily on exploratory research, and quantitative methods quantify the problem by generating numerical data and performing statistical analysis to test hypotheses (McCusker & Gunaydin, 2015). Quantitative methods measure the data and relationships, whereas qualitative methods aim to understand the experience and attitudes of participants. Accessing quantifiable data is relatively simple compared to qualitative research that requires considerable time and effort to allocate resources to a small participant sample. Theoretical framework constructs used to structure the data collection and analysis in quantitative research (Grant & Osanloo, 2014). Three studies about information security governance and CMMS evaluated based on the methodological strengths and weaknesses to determine which method is best suited for the proposed study. Each study presents its limitations along with future research suggestions on

how to address the knowledge gap and expand on theoretical frameworks in the information security and assurance discipline.

Impacts of the Computerized Maintenance Management System

Jamkhaneh et al. (2018) quantitative study on the impacts of computerized maintenance management systems (CMMS) and supportive organizational factors on total productivity uses a survey-based approach. The study aimed to enhance and develop a research model to test the impact of organizational factors on CMMS and productivity for manufacturing companies in Iran. Many researchers prefer quantitative research due to issues relating to time and financial considerations (McCusker & Gunaydin, 2015). A substantial advantage of the nonexperimental quantitative survey instrument is that it accommodates for working with a minimum number of researchers and funding. Tools such as questionnaires applied in multiple areas of study, allowing more inclusive findings and the potential of procuring large amounts of data within a short period (Awa, Uko, & Ukoha, 2017).

The weaknesses of the study performed by Jamkhaneh et al. (2018) are the focus on the medium and high tech manufacturing organizations in Iran, so it does not address multinational companies or low-tech industries. One disadvantage of the nonexperimental design is that it does not allow for data post-treatment, which can introduce new areas for researchers to consider (McCusker & Gunaydin, 2015). The quick nature of nonexperimental quantitative design does not deliver the same in-depth results as an experimental research design. As a result of the studies' weaknesses and limitations, future research can progress by applying CCMS and related organizational factors, including technology security governance, from growth to maturation (Jamkhaneh et al., 2018). The authors also suggest conducting studies on a multi-national level outside of Iran and include low-tech organizations within the target sample. Jamkhaneh et al.

(2018) take a quantitative approach, however, suggest future studies should explore the role of human resources and social capital as an enabler of computerized management maintenance systems using qualitative research methods.

Determinants of Master Data Management Adoption

An empirical study conducted by Haneem et al. (2019) examined the technological, organizational, and environmental determinants of technology adoption by governments in Malaysia. A quantitative survey approach tailored to the context of this study allowed the authors to capture relevant information regarding the research constructs. Having custom questions is a strength in that it enables one to focus the respondents on a specific topic; however, proper validity and reliability tests along with the performance of a pilot study. The new questions developed and not re-used from previous studies tested to demonstrate no bias or misleading terms introduced and measurements modified to suit the context of the study (Haneem et al., 2019). Structural equation modeling, partial least squares (SEM-PLS) statistical analysis, used to test the relationship among variables, and established hypotheses (Haneem et al., 2019). The strength of SEM-PLS is that it is versatile and provides an excellent capability of modeling data to establish correlative models (McIntosh, Edwards, & Antonakis, 2014). An advantage of the quantitative research method used in the study allows for data collection from a variety of participants within a short period.

The study restricted to the local governments in Malaysia that are different from other public organizations and state governments. Similar to the geographical limitation and weakness found in research performed by Jamkhaneh et al. (2018), the current study focuses on Malaysian governments and is not generalized internationally. Future research on maintenance management systems adoption is required for public corporations since results may differ compared to

governments located in Malaysia. Out of 465 surveys issued, 224 valid responses received representing a response rate of 48%. One of the most significant weaknesses of conducting surveys is that over the past decade, there is a consistent pattern of decrease survey response rate (Guo, Kopec, Cibere, Li, & Goldsmith, 2016). To overcome the challenge of low response rate, the authors issued a cover letter explaining the study along with including a stamped return envelope and following up via telephone with the selected target participants who received the survey.

Research Method Implications for Information Security Governance

The security factors influencing the adoption of computerized management maintenance systems (CMMS) by IT managers in the healthcare industry evaluated in the proposed study (Busdicker, & Upendra, 2017; Ehrenfeld, 2017; Harris et al., 2018; Venkatesh et al., 2003; Venkatesh et al., 2012;). The practical implication from advancing research on the behavior influences of the adoption of CMMS by IT managers in the Healthcare industry will improve operational cybersecurity measures by reducing the risk of data breaches in HDO's (Ehrenfeld, 2017; Martin et al., 2018). There is a need to establish accepted industry security controls for effective cybersecurity to reduce the risk of data breaches, and to provide HDO's the capabilities to assess security governance risks across vast technology landscapes, multi-platform environments, and medical devices (Angst et al., 2017; Sittig et al., 2018; van Staa et al., 2016). This study will provide awareness into the behavior influences and security governance requirements required to promote the adoption of CMMS and improve HDO's cybersecurity measures.

Research indicates that HDO cybersecurity threats are increasing, resulting in security breaches that interrupt patient services, impact patient safety, and theft of patient data, these

cybersecurity threats should be the highest priority for HDO's. Continued research in this area is required to support HDO's abilities to manage medical system security and assess security risks across vast technology landscapes, multi-platform environments, and medical devices. By providing the perceived behavior influences of the adoption of CMMS, IT managers in the Healthcare industry can use this study to improve security controls lowering the risks of cybersecurity threats (Ehrenfeld, 2017).

Synthesis of Research Findings

Advances in technology are producing revolutionary medical devices and interventions in healthcare. Health technology, like medical research, generally uses a range of processes that embraces researchers, investigators, stakeholders, and other relevant parties to assess the medical, social, economic, and ethical issues in new health technologies (Vydiswaran, Zhai, Roth, & Pirolli, 2015). There is no standard for research in this area. The literature reviewed focuses on three characteristics: performance, safety, and economic issues, and frequently limit the valuation of ethical and social issues or overlook them completely (García, Rodriguez, & Fdez, 2015).

Over the past decades, Roumen (2015) explains that corporations have become integrally involved with the research on their products. Corporate participation includes sponsorship, study design, analysis, writing content, content endorsement, and setting the timing and format of the published results (Roumen, 2015). These corporate-sponsored studies designed with the intent to produce positive results. Sponsored medical research examples can appear in drug tests that compare results with placebos avoiding existing drugs only to point a non-comparison result (Roumen, 2015). Further examples identify that dosages of the tested drug are lowered to minimize the side effect outcomes (Roumen, 2015). The publishing of results can also be skewed

by not including relevant data and parsing the data to enhance a favorable outcome by softening the evidence of potentially severe adverse side effects.

A review of studies by Bero (2013) using the Cochrane methodology examines the relationship of pharmaceutical, medical device industry-sponsored studies, and the differences of risks and partiality compared with non-industry-sponsored studies. A selection of forty-eight drug and medical device studies revealing that favorable results were 24% higher in industry-sponsored research compared to non-sponsored research (Bero, 2013). Additionally, the results show that industry-sponsored studies have an increased likelihood of ill-treatment in the way that the industry-sponsored studies presented less indication of harm caused by the drug or medical device (Bero, 2013). The Bero (2013) study supports the need for access to the raw data and transparency on how the research is conducted to understand the effects of bias in industry-sponsored studies better. Recommendations from this study plea with government agencies to implement an ethics validation requirement for company-sponsored research and experimental evidence supporting drug and device regulatory use approval (Bero, 2013).

A conflict of interest as defined by Roumen (2015) as a set of conditions in which primary professional importance is excessively influenced by an entity's secondary interest, which comes into conflict with ethical responsibilities concerning patients, health professionals, and the industry. To establish transparency and integrity for published industry-sponsored studies, in 2008, the pharmaceutical industry and the International Society for Medical Publication Professionals established the Medical Publishing Insights and Practices (ISMPP) initiative (Roumen, 2015). The literature review of medical research-supported and published by accredited medical associations indicates that ethics in research is a priority. Both conflicts of interest and sponsorship stated in these research publications. The technology research reviewed

does not provide any conflict of interest statements. Further research on the relationship between technology industry sponsorship and research outcomes would contribute to the current literature by examining the ethical considerations and credibility of sponsored technology research concerning the purposes for advancing scientific, medical, and technology knowledge.

Healthcare and cybersecurity ethics

The review of literature on the adoption of Computerized Maintenance Management Systems (CMMS) exposes cybersecurity threats directed toward Healthcare Deliver Organizations (HDO) are increasing and that these threats are targeting vulnerable medical devices and medical solution platforms. HDOs are vulnerable because of the progressive interoperability of technology that provides care to patients and the numerous ways medical devices are connected. Medical solutions are inherently accessible, which increases the probability that attackers will breach them (Coventry & Branley, 2018). The complexity of healthcare environments is a reason why HDOs are not implementing information security governance supporting security programs and the proper cybersecurity control measures at a faster pace to protect against cyber threats (Chen et al., 2016). Within this literature, there is no mention of the moral or ethical implications related to cybersecurity preparedness.

A search for empirical research on healthcare and cybersecurity ethics showed that little research conducted on the subject. Li, No, and Wang (2018) emphasize that cybersecurity ethics and compliance exists today within established government standards policies and regulations. Within healthcare, The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and The Health Information Technology for Economic and Clinical Health Act (HITECH) guide securing infrastructures, data and protected personal health information (PHI) (Kafali, Jones, Petruso, Williams, & Singh, 2017). The United States Food and Drug Administration (FDA),

through the 510k medical device certification process, controls the security and safety of medical devices and solutions. Conventional technologies secured through standard security controls such as the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), or International Electrotechnical Commission (IEC). With substantive guidance through cybersecurity regulations and standards, it is essential to understand how cybersecurity ethics influence the adoption of robust information security governance.

A review of empirical research by Finnemore (2018) investigates the current circumstances of cybersecurity ethics that are prevalent with users of the internet. Finnemore (2018) explains that cybersecurity ethics is the study of the ethics that are important to computer environments, which is made up of user's behavior and its effects on individuals and society. The objective of the Finnemore (2018) study is to understand whether users are familiar with the term cybersecurity ethics, what the participant uses fundamental cybersecurity ethics, and to analyze the cybersecurity ethics behavior patterns of users. The Finnemore (2018) qualitative research was assembled through semi-structured interviews and exposes that while some users believe that regulation is essential to enforce security adequately, others believe that commercial and private industry does not equally share in that responsibility. Secondly, industries need to take responsibility for attaining the essential technical and knowledge resources to address deficiencies in cyber defense and ethical behavior. Further research on the relationship between cybersecurity ethics and information security governance would contribute to the current literature by examining the ethical considerations and security readiness research about the purposes for advancing scientific, medical, and technology knowledge.

Critique of Previous Research Methods

Dutot et al. (2019) confirmed the TRA model fittingness when used within its boundaries. The theory is appropriate when predicting straightforward behaviors aligned with volitional constraints. Outside of the model's boundaries, both Dutot et al. (2019) and Lai (2017) point out the model's fittingness diminishes. Dutot et al. (2019) meta-analyses concluded that the theory of reasoned action is an appropriate model alongside behaviors aligned with the person's volitional control and prediction of objectives or activities with an obvious choice. The prediction is only proficient by expounding on the specific substitutions to allow the study participant to provide specific answers, which in turn delivers distinctive and consistent predictions.

Initial research indicated that the model was appropriate for studying the influences of computer usage behavior (Davis et al., 1989). Research indicates that the model may not be the most suitable instrument to determine the behavior factors influencing the adoption of CMMS (Dutot et al., 2019; Mital et al., 2018; Sher et al., 2017). The existing model involves an extension of the boundaries to take account of, not limited to, financial, security, legal, resources, demographic factors, and it does not include an obvious choice among alternatives, which weakens its viability. Per Lai, 2017, the model is not appropriate when an individual cannot execute the action even when there are strong intentions. Relating to the adoption of CMMS, the person may have strong intentions to adopt CCMS, but there are limitations due to financial, security, or resource concerns. Based on previous research and recommendations, the theory of reasoned action considered unsuitable for the study in adopting CMMS.

The review of research indicates that the technology acceptance model is a useful model used in various studies to explain the behavior of technology usage (Fedorko et al., 2018; Wang

& Goh, 2017). Venkatesh et al. (2012) emphasized through a recommendation of using the model's original constructs in reliable predictions of user acceptance. In the current empirical research reviewed, it is evident that the model requires additional variables to explain the association between the perceived ease of use, perceived usefulness, and user acceptance in contemporary technology. TAM is suitable for the adoption of CMMS due to various meta-analysis studies concluding the technology acceptance model is useful and employed across diverse domains, the sustenance of the model by information technology researchers, and the ability to expand the variables. The proposed adoption of CMMS research will require expansion and moderating variables to include security variables; this may influence the reliability or weaken the association between the independent and dependent variables.

The unified theory of acceptance and use of technology model addresses some of the limitations delineated with the technology acceptance model previously reviewed. Arias-Oliva et al. (2019) applied the unified model with the principal determining factors of performance expectancy, effort expectancy, and social influence in the adoption of the use of cryptocurrency technologies. Ricardo, Moriguchi, and Andrade (2016) implemented the unified model in Brazil to determine the factors influencing the adoption of mobile payment technology. The study predicts the factor of social influence influencing the adoption, while Young et al. (2018) could only suggest cultural factors in adopting technology Pedagogy and Content Knowledge (TPACK). There appear to be difficulties in extending variables in using the technology acceptance model, Ricardo de Sena Abrahão et al. (2016) research indicated the effectiveness of adopting the unified model with additional determinants and moderators. The research did not introduce weakness among the four key determinants, as in the Arias-Oliva et al. (2019) study.

Summary

A review of the literature shows that cybersecurity threats directed toward HDO's are increasing and that these threats are targeting vulnerable medical devices and medical solution platforms. Hackers motivated by the prospect of financial or political gain (Coventry & Branley (2018). HDOs are vulnerable because of the progressive interoperability of technology that provides care to patients and the numerous ways medical devices are connected. Medical solutions are inherently accessible, which increases the probability that attackers will find them (Coventry & Branley, 2018). A single medical device can make available the possible entry point to further extensive HDO networks. The complexity of healthcare environments is a reason why HDOs are not implementing information security governance supporting security programs and the proper cybersecurity control measures at a faster pace to protect against cyber threats (Chen et al., 2016). Legacy medical devices solutions and asset management are pointed out as primary factors of risks. Regulatory guidance is only present to inspire manufacturers to plan, monitor proactively, and respond to potential cybersecurity vulnerabilities in medical devices in the market, and these remain optional to manufactures. Resources, adherence to security standards, and legacy medical devices are pointed out as primary factors of cybersecurity risks for HDOs (McLeod & Dolezel, 2018).

The review of literature additionally shows that CMMS can be implemented to manage and reduce resources, enable compliance with security standards, enable decision-making for legacy medical devices, and to track medical device cybersecurity measures reducing risks for HDOs (Jalali, & Kaiser, 2018; Jamkhaneh et al., 2018). The studies seem to be in direct conflict on the adoption of CMMS; some studies indicate that the adoption rate of CMMS is slow across many industries while other studies stating that the adoption of CMMS is increasing. Empirical

research on maintenance management models indicating that recent substantive studies on practice and adoption are sparse and in decline (Fraser et al., 2015). The review of literature further indicates that research on the adoption of CMMS and the behavioral characteristics of HDOs influence, acceptance, and perceived usefulness of CMMS would add to the overall body of knowledge.

CHAPTER 3. METHODOLOGY

The purpose of this study is to help healthcare IT managers understand if performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance effectiveness influence the adoption of computerized maintenance management systems. The simple definition of CMMS is when enterprise maintenance operations data is stored is a centralized location accessed by end users (Rastegari & Mobin, 2016). The data helps maintenance workers perform their jobs effectively by providing them the ability to determine which systems require maintenance and locate spare parts. Additionally the centralized information allows management to make informed decisions about preventive versus reactive repair activities resulting in better allocation of resources (Fortin et al., 2018). Gaining an understanding of the type of IT managers that adopts the emerging technology is key for successful CMMS implementations. Chapter 3 provides a summary of the purpose of the study and research questions with hypothesis. The research design, target population, and sampling procedure elaborated on along with a description of the data analysis and statistical tests performed. This chapter also includes the ethical elements taken into considerations when conducting the study to ensure the privacy and confidentiality of survey participants.

Purpose of the Study

The purpose of this quantitative nonexperimental correlational research addresses the research gap about the relationship between technology security governance's impact on the adoption of Computerized Management Maintenance Systems (CMMS) by IT managers (Benham-Hutchins, Staggers, Mackert, Johnson, & DeBronkart, 2017). This study will use the survey instrument created by Venkatesh et al. (2003) that measures facilitating conditions, social influence, effort expectancy, performance expectancy factors affecting the adoption of CMMS in

HDO's based on the Theory of Acceptance and Use of Technology (UTAUT) (Benham-Hutchins et al., 2017; Harris et al., 2018; Rezaei, & Ghofranfarid, 2018). This study will integrate Venkatesh et al. (2012) adapted the UTUAT survey instrument to understand technology security governance factors influencing technology managers in healthcare acceptance of CMMS.

Research Questions and Hypotheses

This study intended to help organizations understand what factors may influence the adoption of CMMS systems and security governance controls within their organization. Understanding these factors may allow organizations to focus on specific obstacles and develop strategies to ensure the adoption of the governance standards successfully implemented for computerized management maintenance systems. By examining data collected by a survey, answers to the following six research questions and hypothesis were determined:

RQ1: To what extent does Performance Expectancy (PE) correlate to the adoption of a Computerized Maintenance Management System?

$H1_0$ - There is no statistically significant correlative relationship between PE and adoption of Computerized Maintenance Management System (CMMS)

$H1_A$ - There is a statistically significant correlative relationship between PE and adoption of Computerized Maintenance Management System (CMMS)

RQ2: To what extent does Effort Expectancy (EE) correlate to the adoption of a Computerized Maintenance Management System?

$H2_0$ - There is no statistically significant correlative relationship between EE and adoption of Computerized Maintenance Management System (CMMS)

$H2_A$ - There is a statistically significant correlative relationship between EE and adoption of Computerized Maintenance Management System (CMMS)

RQ3: To what extent does Social Influence (SI) correlate to the adoption of a Computerized Maintenance Management System?

$H3_0$ - There is no statistically significant correlative relationship between SI and adoption of Computerized Maintenance Management System (CMMS)

$H3_A$ - There is a statistically significant correlative relationship between SI and adoption of Computerized Maintenance Management System (CMMS)

RQ4: To what extent does Facilitating Conditions (FC) correlative the adoption of a Computerized Maintenance Management System?

$H4_0$ - There is no statistically significant correlative relationship between FC and adoption of Computerized Maintenance Management System (CMMS)

$H4_A$ - There is a statistically significant correlative relationship between FC and adoption of Computerized Maintenance Management System (CMMS)

RQ5: To what extent does Technology Security Governance Effectiveness (TSGE) correlate to the adoption of a Computerized Maintenance Management System?

$H5_0$ - There is no statistically significant correlative relationship between TSGE and adoption of Computerized Maintenance Management System (CMMS)

$H5_A$ - There is a statistically significant correlative relationship TSGE impact and adoption of Computerized Maintenance Management System (CMMS)

RQ6: How well does performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance predict the adoption of computerized maintenance management systems?

$H6_0$ - there will be no statistically significant prediction of CMMS adoption by performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance.

$H6_a$ - there will be a statistically significant prediction of CMMS adoption by performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance.

Research Design

Quantitative, nonexperimental correlational research used in this study to explore the effects of information security governance factors on CMMS implementation. A survey instrument will measure information security governance effectiveness, behavioral intention, social influence, effort expectancy, performance expectancy factors, and adoption of CMMS (Benham-Hutchins et al., 2017). The Qualtrics survey management system is an accessible online survey available to collect information from the target population in the technology industry. Benham-Hutchins et al. (2017) used the Qualtrics survey management system in their research to collect survey results to evaluate the inpatient hospitalization influences of patient self-management of chronic disease across care transition that verified Qualtrics to be useful. The survey will measure the constructs of information security governance behavioral factors as they relate to the adoption of CMMS.

Quantitative and qualitative research methodologies, used to investigate information security governance as it relates to the adoption of computerized maintenance management

systems, are prominent techniques used within the academic studies. Research explores organizational factors including information systems management, performance management; accountability; communication; governance; and capability development to evaluate technology adoption within organizations (Tang & Zhang, 2016). Information security governance provides a framework and structure to ensure the adequate mitigation of risk, while management ensures that controls implemented promote the successful enterprise-wide adoption of new technologies. Computerized maintenance management systems (CMMS) are emerging technology that permits decision analysis capability based on the system containing master data on organizations' maintenance operations (Rastegari & Mobin, 2016). The application of automated systems is expanding rapidly in different industries, and CMMS plays an essential role in the automation of production systems (Jamkhaneh et al., 2018). CMMS technologies have grown in the past 50 years with web-based connectivity and assist firms with enterprise resource planning that provides seamless information about the flow for main business processes and decision-making data (Wan et al., 2017). Three studies evaluated to understand the purpose, research method, findings, and conclusion that provides a scholarly foundation for information security governance influencing the adoption of CMMS. Qualitative studies focus on exploring research problems via interviews and investigative techniques, whereas quantitative research measures the problem by generating numerical data and performing statistical analysis. Jamkhaneh et al. (2018) and Haneem et al., (2019) perform quantitative research in the field of information security and assurance, whereas Hadban et al., (2017) perform qualitative interview research to explore the challenges and facilitators for technology adoption.

The proposed study research design is a nonexperimental correlational study to explore the behavior influence effects of the adoption of CMMS by IT managers in Healthcare. The

research design will follow a quantitative methodology approach in line with post-positivist philosophical assumptions (Singhry et al., 2016). This design will use a survey as the primary strategy of the investigation. A survey is a nonexperimental, correlational instrument that used to determine if there is a statistically significant relationship between behavior influence effects and the adoption of CMMS. (Sabi et al., 2016). The survey administered to participants is in the form of close-ended questions and Likert scale (7=*Strongly Agree*, 1=*Strongly Disagree*) questions. The study will use statistical tests and procedures to answer the research problem, question, and hypotheses about the behavior influence of the adoption of CMMS by IT managers in Healthcare (Field, 2013). The nonexperimental research will consist of an exploratory statistical model to discover statistical relationships between the adoption of CMMS based on the behavior influence in the healthcare industry. The Venkatesh et al., (2003) survey instrument variables and UTAUT model of been validated in prior studies before being introduced in the survey (Harris et al., 2018; Rezaei & Ghofranfarid, 2018; Venkatesh et al., 2003; Venkatesh et al., 2012)

The proposed research presents minimal risk to participants since no more than the risk encountered in daily life introduced in the target population. The research population does not include personal data or information that is not publically available. There is minimal risk to contributors since the degree of risk presented by the research is no more than the risk encountered in daily life (Van Hoof et al., 2018).

Target Population and Sample

The primary research question addressed is to what extent performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance effectiveness correlate to the adoption of a CMMS. The focus of this quantitative, nonexperimental, correlative study centered on U.S. healthcare organizations targeting IT

professionals due to their understanding of CMMS. The remainder of this section describes the population, sample size, and power analysis.

Population

The population targeted for this study consists of IT managers working for HDO organizations with a minimum of 5 years' experience in the healthcare industry. Similar to the population and sampling method used by Niranjan et al. (2018), the study will use Qualtrics survey panel to identify IT managers working for HDO organizations targeted for the questionnaire. The questionnaires sent to the pre-selected subset of the target population and filtered via a valid sampling method per the website Qualtrics. Per their website, Qualtrics (www.qualtrics.com) survey used by a variety of global companies and numerous business schools in the United States (Niranjan et al., 2018). Researchers have been successful using the Qualtrics platform for data collection. For example, Niranjan et al., 2018 stated that using Qualtrics is an efficient way to collect data with a resulting survey completion rate of nearly 87% (Niranjan et al., 2018). The target population for this research is healthcare IT managers in the United States that can be of any gender, over age of 18, and with various professional backgrounds. The Bureau of Labor Statistics (2016) indicates there are 352,200 medical and health IT managers located in the United States. The sample set consists of United States IT managers in the healthcare industry from a database maintained by Qualtrics of potential participants. Based on this sample frame, Qualtrics performed random sampling to produce the participants for this study.

Sample

The study will use a probability sampling method for examining facilitating conditions that affect CMMS adoption in the healthcare industry. The unique characteristic of non-probability sampling is that subjective judgment plays a role in sample selection, indicates which unit of the population is included in the sample. In contrast, probability sampling involves a random selection (Creswell, 2009). Quota sampling and response rate have the same proportions of respondents as the entire population regarding this study of IT healthcare managers with over two years of work experience. The sampling using Qualtrics survey platform to collect data for the healthcare IT manager probability sampling will use individuals that have been recruited in advance and agreed to complete the surveys (Field, 2013). The quota sampling selection is due to obtaining a specific number of IT healthcare managers, along with having a predefined number of survey respondents. This technique selected ensures that an adequate number of respondents will answer the survey concerning the adoption of CMMS. The sample inclusion criteria include the following: healthcare information technology managers; over 5 years experience in the healthcare technology field; and employed at a healthcare organization. The exclusion criteria consist of participants whose organizations have not implemented CMMS (Niranjan et al., 2018). Survey results from participants who do not meet this criterion are discarded.

Power Analysis

The sample size is determined using the tool G*Power3 analytics to perform the statistical tests used to substantiate the hypothesis of CMMS acceptance and relationship with facilitating conditions effects (Field, 2013; Niranjan et al., 2018). Tests using a priori analysis is completed in the sample selection to determine the necessary size required for the appropriate significance level (Cohen, 2014). Using the G*Power 3.1.9.2 sample calculator with a population

of 352,200, an exact test family for correlation bivariate, normal model, a priori compute required sample size , $\alpha = .05$, $\beta = .80$, and correlation p H1 = 0.3 the final sample size calculation arrived at 67 respondents (Field, 2013). By determining the appropriate population and sample size, the results of the study apply to generalized IT managers working for the HDO population (Field, 2013).

Procedures

This research study completed using quantitative methodology implies that the variables not manipulated and an online Qualtrics survey instrument used to collect data from participants. Qualtrics, an online survey distribution tool, used to reach potential participants since the platform has a large database of IT managers in the healthcare industry. The Qualtrics platform has a panel of participants that fit the inclusion criteria for this research study and the survey sent to participants without influence or preference indicating simple random sampling method used to choose the contributors for the study. The remainder of this section includes details regarding participant selection, protection of participants, data collection and data analysis processes.

Participant Selection

The procedure used for data collection is the deployment Qualtrics survey panel electronic questionnaire (Qualtrics, 2019). Qualtrics survey panel audience panel is the primary method to poll participants and provide them access to the online survey. The web-based survey will require participants to agree to the consent form to participate. The confidentiality of participants is protected by coding the response from each respondent with a unique identification number. The sample inclusion criteria include the following: (a) Healthcare information technology managers (b) five years' experience in the healthcare technology field, (c) employed at a healthcare organization. The exclusion criteria consist of participants whose

organizations have not implemented CMMS (Niranjan et al., 2018). Survey results from participants who do not meet this criterion are discarded. Survey results are downloaded from the Qualtrics website and stored on an encrypted external storage device. The external storage device is stored safely at a secure location. The survey and research data destroyed after 7 years (Niranjan et al., 2018).

Protection of Participants

The privacy, confidentiality, and anonymity of research participants are protected. The confidentiality of participants is protected by coding the response from each respondent with a unique identification number. To prevent any ethical issues, participants provided informed consent forms, and the research survey reviewed and approved by the Institutional Review Board (IRB). Survey results downloaded from the Qualtrics survey panel website and stored on an encrypted external storage device. The external storage device safely stored at a secure location, and after 7 years, the survey and research data destroyed (Van Hoof et al., 2018).

Data Collection

The survey conducted over a 45-day time frame. Surveys used to answer multiple-choice questions, which are also known as closed-end questions (Schindler, 2006). These types of questions are useful because they force participants to choose between preselected answers. The Likert scale responses determine how much the participant agrees or disagrees with the survey question and measured as an ordinal variable (Creswell, 2009).

This survey conducted using a self-administered online questionnaire. Participants were prompted with a choice to agree to informed consent or disagree. If they disagree, the questionnaire page thanks the participant for their time and are not considered any longer for the survey. If the participant agrees, then they are taken to the login hosted on the online Qualtrics

survey distribution tool. The participants complete the survey and submit the data transmitted by the Qualtrics online survey distribution tool. Data is stored on a flash drive for 7 years after completion of the study and no personal information or organizational information stored. After the completion of all online surveys, the survey and results removed from the online survey distribution tool. After 7 years, data permanently removed from the hard drive by formatting the flash drive.

Data Analysis

Data collected via an online survey distribution tool. Data is collected online and then downloaded. The downloaded data will not hold any personal or identifiable information to protect privacy. Only the answers to the survey questions are collected. The surveys managed through an online survey provider. The data downloaded to a flash drive, encrypted, and saved in a password-protected file. Data screened for missing data and outliers using IBM's SPSS statistics software. Outliers identified eliminated from the statistical analysis since they represent data points that differ significantly from other observations (Sarstedt et al., 2014). Qualtrics Survey tool collects the data, and IBM SPSS software version 24 used for the statistical analysis. This study will take account of the ensuing assumptions: (a) measures will use a sufficient Likert scale; (b) participants will respond and view the measure similar or the same; and (c) the measures are constant and viewed similarly by participants (Venkatesh et al., 2003; Venkatesh et al., 2012). Questions are measuring performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance effectiveness as it relates to computerized maintenance management systems evaluated to answer the studies' research questions and hypothesis. IBM SPSS statistics software used to conduct Spearman's correlation

analyses among the independent and dependent variables and outline relationships between the data points.

Descriptive Statistics. Descriptive data collected for the survey includes three demographic questions. The participants' age, job title, and organizational size inputted to understand additional information about the participants and potentially contribute to future research. Coding is required to measure each survey response correctly, and Table 1 through 3 represents the coding of demographic data. The demographic information used to group participants, and no additional statistical analysis performed. The Likert scale used for the questions went in steps where 1 = *Strongly Disagree*, 2 = *Disagree*, 3 = *Slightly Disagree*, 4 = *Neither Agree or Disagree*, 5 = *Slightly Agree*, 6 = *Agree*, and 7 = *Strongly Agree.* No coding of the Likert scale required.

Table 1: Coding for Age Demographic Information

Value	Age
1	18 - 24 years old
2	25 - 34 years old
3	35 - 44 years old
4	45 - 54 years old
5	55 - 64 years old

Table 2: Coding for Job Title Demographic Information

Value	Job Title
1	Chief Information Officer
2	IT Analyst
3	IT Manager
4	Senior IT Analyst
5	Senior IT Administrator
6	IT Administrator
7	Technology Architect
8	Technology Professional
9	VP/Director IT

Table 3: Coding for Organization Size Demographic Information

Value	Organizational Size
1	1 to 4 employees
2	5 to 9 employees
3	10 to 19 employees
4	20 to 49 employees
5	50 to 99 employees
6	100 to 499 employees
7	500 or more employees

Note. Demographic information age, job title, organizational size for respondents with 100% completion rate.

Hypothesis Testing. The hypothesis 1 to 5 tested using Spearman's rank correlation coefficient on the variable to determine if there is a statistically significant correlation between the independent and dependent variables. The statistical significance investigated for each variable and analyzed as it relates to the five specific research questions. Spearman's correlation has three assumptions to be tested, the first two relate to the study design, and the third relates to the nature of the data (Field, 2013). These three assumptions consist of: two continuous or ordinal variables, the variables represent paired observations, and a monotonic relationship exists between the two variables (Laerd Statistics, 2018). Hypothesis 6 tested using PLS methods on the variables to determine statistical significance. Structural path coefficients and statistical significance between the independent and dependent variables investigated, and predictive analysis conducted on the variables to understand how UTAUT factors predict CMMS adoption. Prior to running partial least squares analysis multicollinearity between the independent variables, linearity, and outliers assumptions are confirmed to validate the dataset (Laerd Statistics, 2018), Qualtrics obtained seventy-seven participants to respond to the survey. The Qualtrics survey service verified that all participants were IT managers from healthcare organizations within the United States, with over five years of work experience. There are three outliers identified in the study, and those responses discarded from the statistical analysis

conducted. The 74 survey responses used for the study had no missing data, and all questions were responded to by the participants. The dataset analysis conducted on the variables identified whether a correlation existed between the independent variable of performance expectancy, effort expectancy, social influence, facilitating conditions, technology security governance effectiveness as it relates to the adoption of a computerized maintenance management system.

Instruments

To investigate the variables, PE, EE, SI, FC, and TSGE, the Venkatesh, et al., (2003), Unified Theory of Acceptance and Use of Technology (UTAUT) instrument is used. The copyright belongs to the Management Information Systems Research Center (MISRC) of the University of Minnesota. Permission to use and adapt the instrument was obtained from the MIS quarterly publication. Partial least squares, conducted in the study performed by Venkatesh et al. (2003) , examine the reliability and validity of the measures presented in the UTAUT framework. All internal consistency reliabilities were more significant than .70 and are deemed acceptable for the constructs PE, EE, SI, and FC. This design will use a survey as the primary research method of inquiry and poll participants, providing them access to the online survey using the Qualtrics audience panel. The data types for each research question presented in Table 4. PE, EE, SI, FC, and TSGE and CMMS represent ordinal measurement levels with the possible values of 1 -7, resulting in ranking order. The ordinal scale shows the order but not the distances between the rankings resulting in the ordinal scale, also classified as a ranked scale (Sabi et al., 2016). The Computerized Maintenance Management Systems Survey used for this study coded as follows: *Strongly Agree* (7); *Agree* (6); *Slightly Agree* (5); *Neither Agree nor Disagree* (4); *Slightly Disagree* (3); *Disagree* (2), and *Strongly Disagree* (1).

Table 4: Research Question Data Types

RQ	Variables	Independent /Dependent Variable	Data Type
1	PE	IV	Ordinal
	Computerized Maintenance Management System (CMMS)	DV	Ordinal
2	EE	IV	Ordinal
	Computerized Maintenance Management System (CMMS)	DV	Ordinal
3	SI	IV	Ordinal
	Computerized Maintenance Management System (CMMS)	DV	Ordinal
4	FC	IV	Ordinal
	Computerized Maintenance Management System (CMMS)	DV	Ordinal
5	TSGE	IV	Ordinal
	Computerized Maintenance Management System (CMMS)	DV	Ordinal

Note. Data types for PE, EE, SI, FC, TSGE, and CMMS

The quantitative study uses Spearman's rank-order correlation coefficient to determine if there is a relationship between the independent and dependent variables. Spearman is appropriate for statistical analysis since the measurement data types are ordinal scales (Mertler & Reinhart, 2016). Spearman's rank correlation coefficient assesses the statistical strength of the relationship between the independent and dependant variables.

Factors Impacting the Adoption of CMMS

Validity. Venkatesh et al. (2003) produced a questionnaire to extend upon the constructs of eight prior technology acceptance models by developing a seven-point Likert scale (i.e., one at the negative end of the scale and seven at the positive end). Partial Least Square (PLS) regression calculate to examine the reliability and validity of the measures gathered from the questionnaires (Venkatesh et al., 2003). Factors including internal consistency reliability, mean, standard deviation, and the square root of the shared variance between constructs and their measures evaluated (Venkatesh et al., 2003). All internal consistency reliability scores are higher than .70, indicating convergent and discriminant validity of the survey instrument (Venkatesh et al., 2003).

Reliability. There are multiple research studies in the literature as to the validity and reliability of the Venkatesh et al. (2003) UTAUT survey tool. According to Venkatesh et al. (2003), research studies have reported a Cronbach's alpha score to be between .88 and .94, which indicates a high degree of trust and reliability in the UTAUT survey instrument.

Ethical Considerations

The proposed research presents minimal risk to participants. The research population does not include personal data or information that is not publicly available. There is minimal risk to contributors since the degree information collected and presented will not include the participant names, or identifying characteristics, in order to protect the confidentiality and anonymity of participants (Van Hoof et al., 2018). To prevent any ethical issues, participants provided informed consent forms, and the research survey is reviewed and approved by the Capella University Institutional Review Board (IRB). Survey results are downloaded from the Qualtrics survey panel website and stored on an encrypted external storage device. The external storage device stored safely at a secure location. Survey and research data is destroyed after 7 years (Van Hoof et al., 2018).

Summary

Quantitative and qualitative methodologies, used to investigate information security governance as it relates to the adoption of computerized maintenance management systems, are prominent techniques used in research studies. Research explores organizational factors including information systems management, performance management; accountability; communication; governance; and capability development to evaluate technology adoption within organizations (Tang & Zhang, 2016). Jamkhaneh et al. (2018) and Haneem et al. (2019) perform quantitative research in the field of information security and assurance. In contrast, Hadban et al.

(2017) perform qualitative interview research to explore the challenges and facilitators for maintenance management systems adoption. Based on data presented, the authors indicate that future research can be done in the area of information security governance as it relates to computerized maintenance management systems. Performing research in regions outside or Iran and Malaysia, and expanding factors of the UTAUT theoretical framework will help close the knowledge gap presented in current literature.

CHAPTER 4. RESULTS

Background

The purpose of this quantitative study evaluates the relationship between the UTAUT variables (Venkatesh et al., 2003): performance expectancy, effort expectancy, social influence, facilitating conditions, technology security governance effectiveness, and the dependent variable of the adoption of computerized maintenance management systems (CMMS) among technology managers in the United States. The management-level question addressed relative to CMMS is, what are the factors of the UTAUT variables upon the acceptance and usage of CMMS by information technology managers.

Description of the Sample

Seventy-seven technology managers completed the survey examining how health-care IT managers in the United States understand the benefits of CMMS. The study uses the IBM SPSS statistics software package to conduct the testing and analysis. The demographic composition of the participants was as follows: 23 (29.87%) were information technology managers; 12 (15.58%) were chief information officers; 11 (14.29%) were VP's of information technology; 8 (10.39%) were technology administrators; 7 (9.09%) were information technology analyst; 7 (9.09%) were technology professionals; 4 (5.19%) were technology architects; 3 (3.90%) were senior technology analysts, and 2 (2.60%) were senior technology analysts. All participants work in the healthcare industry as information technology professionals, and all 77 samples were valid with no missing data identified, as indicated in Table 5. There was a wide age range of participants, and the demographic data included in tables 6, 7, 8, and 9.

Table 5: Missing Data

		Industry	Organization Type	Age	Gender	Organization Size	Job Title
N	Valid	77	77	77	77	77	77
	Missing	0	0	0	0	0	0

Note. Sample size check for validity and missing data, *N=77*

Table 6: Participants' Familiarity with Computerized Maintenance Management Systems

		Frequency	%	Valid %	Cumulative %
Valid	< 1 year	12	15.6	15.6	15.6
	> 5 years	8	10.4	10.4	26.0
	1 - 2 years	11	14.3	14.3	40.3
	2 - 3 years	16	20.8	20.8	61.0
	3 - 4 years	9	11.7	11.7	72.7
	4 - 5 years	21	27.3	27.3	100.0
	Total	77	100.0	100.0	

Note. *N* = 77. These responses are for the question: How much experience do you have using Computerized Maintenance Management Systems?

Table 7: Age

		Frequency	%	Valid %	Cumulative %
Valid	18 - 24 years old	5	6.5	6.5	6.5
	25 - 34 years old	22	28.6	28.6	35.1
	35 - 44 years old	33	42.9	42.9	77.9
	45 - 54 years old	13	16.9	16.9	94.8
	55 - 64 years old	4	5.2	5.2	100.0
	Total	77	100.0	100.0	

Note. *N* = 77. These responses are for the question: What is your current age?

Table 8: Job Title

		Frequency	%	Valid %	Cumulative %
Valid	Chief Information Officer	12	15.6	15.6	15.6
	IT Analyst	7	9.1	9.1	24.7
	IT Manager	23	29.9	29.9	54.5
	Senior IT Analyst	3	3.9	3.9	58.4
	Senior IT Administrator	2	2.6	2.6	61.0
	IT Administrator	8	10.4	10.4	71.4
	Technology Architect	4	5.2	5.2	76.6
	Technology Professional	7	9.1	9.1	85.7
	VP/Director IT	11	14.3	14.3	100.0
	Total	77	100.0	100.0	

Note. $N = 77$. These responses are for the question: What is your job title?

Table 9: Organization Size

		Frequency	%	Valid %	Cumulative %
Valid	10 to 19 employees	2	2.6	2.6	2.6
	100 to 499 employees	19	24.7	24.7	27.3
	20 to 49 employees	5	6.5	6.5	33.8
	5 to 9 employees	1	1.3	1.3	35.1
	50 to 99 employees	7	9.1	9.1	44.2
	500 or more employees	43	55.8	55.8	100.0
	Total	77	100.0	100.0	

Note. $N = 77$. These responses are for the question: How many employees work at your organization?

Hypothesis Testing

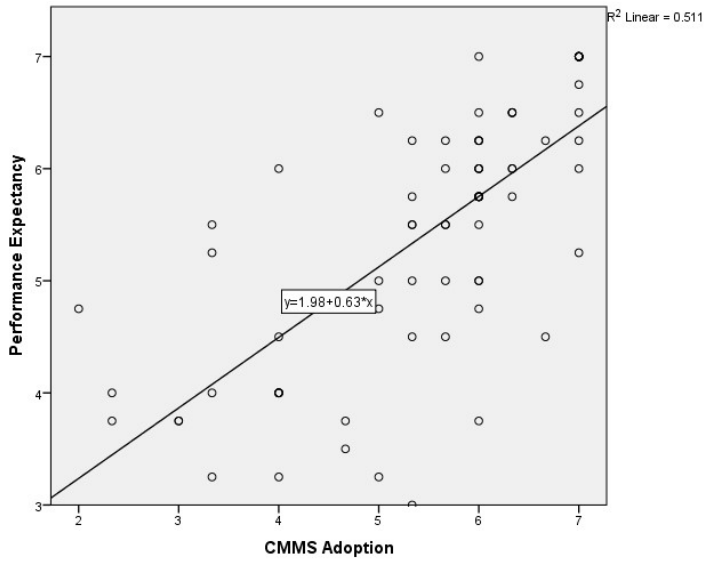
The Computerized Maintenance Management Systems Survey used for this study coded as follows: *Strongly Agree* (7); *Agree* (6); *Slightly Agree* (5); *Neither Agree nor Disagree* (4); *Slightly Disagree* (3); *Disagree* (2), and *Strongly Disagree* (1). The management-level question to address relative to CMMS is: To what extent do the UTAUT variables correlate to the acceptance and usage of CMMS by healthcare IT managers? The omnibus research question contains variables for testing and evaluation, including Performance Expectancy (PE), Effort Expectancy (EE), Social Influence (SI), Facilitating Conditions (FC), Technology Security Governance Effectiveness (TSGE) with regards to the adoption CMMS.

The quantitative study uses Spearman's rank-order correlation coefficient to determine if there is a relationship between the independent and dependent variables. The null hypothesis is rejected when the coefficient is less than or equal to the .05 level of significance using a two-tail significance measure. The null hypothesis being rejected means that there is a statistically significant relationship between the independent and dependant variables. When the calculation is higher than the .05 level of significance, the study fails to reject the null hypothesis. The study fails to reject the null hypothesis means that there is no statistically significant relationship between the independent and dependant variables. The following research questions and hypotheses guide the study to determine the extent of Performance Expectancy (PE), Effort Expectancy (EE), Social Influence (SI), Facilitating Conditions (FC), and Technology Security Governance Effectiveness (TSGE) correlate to the adoption CMMS.

Partial Least Squares testing used to determine how well performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance predict the adoption of computerized maintenance management systems. The null hypothesis is rejected when the significance level is less than or equal to the.05 level of significance (Laerd Statistics, 2018). The study fails to reject the null hypothesis means that there is no statistically significant prediction of CMMS adoption by performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance. Prior to running partial least squares analysis multicollinearity between the independent variables, linearity, and outliers' assumptions are confirmed to validate the dataset

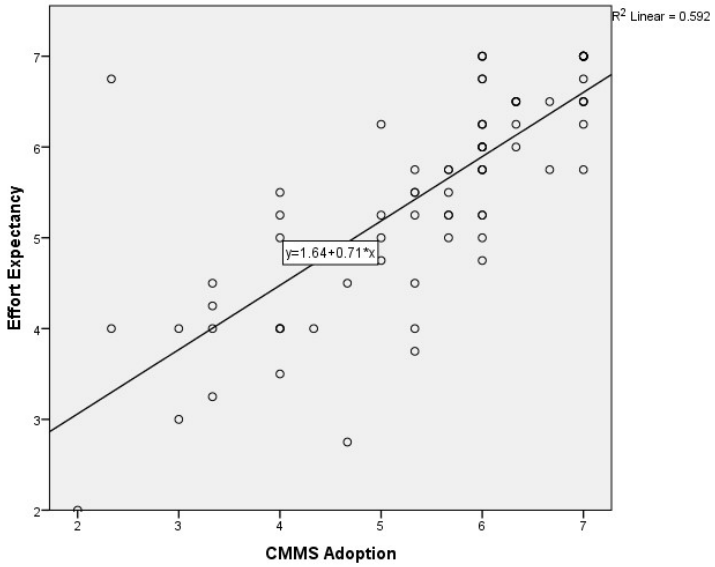
The Spearman's correlation has three assumptions, the first two relate to the study design, and the third relates to the nature of the data (Field, 2013). These three assumptions consist of: two continuous or ordinal variables, the variables represent paired observations, and a monotonic

relationship exists between the two variables (Laerd Statistics, 2018). The data assumption involves using SPSS Statistics to determine whether there is a monotonic relationship between the independent and dependent variables. A monotonic relationship exists if the value of one variable increases as the other variable increases or the value of one variable increases and the other variable decreases (Laerd Statistics, 2018). In order to proceed with Spearman's correlation, all three assumptions met, including having ordinal variables, the variables representing paired observations, and a monotonic relationship existing between two variables. As a result of the independent and dependent variables being ordinal in measurement and the variables represent paired observations the assumptions regarding the study design met. To identify if a monotonic relationship exists, a scatterplot diagram created for the study variables. The scatterplots are a visual depiction of the relationships between performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance effectiveness represented in figure 1 to 5. From visual inspection of the scatterplot diagrams, there is a monotonic, but non-linear, relationships that exist between the independent and dependent variables. The relationship between variables is positive since variable Y increases as X increases. Since a monotonic relationship exists between variables, Spearman's correlation analysis conducted on the data.



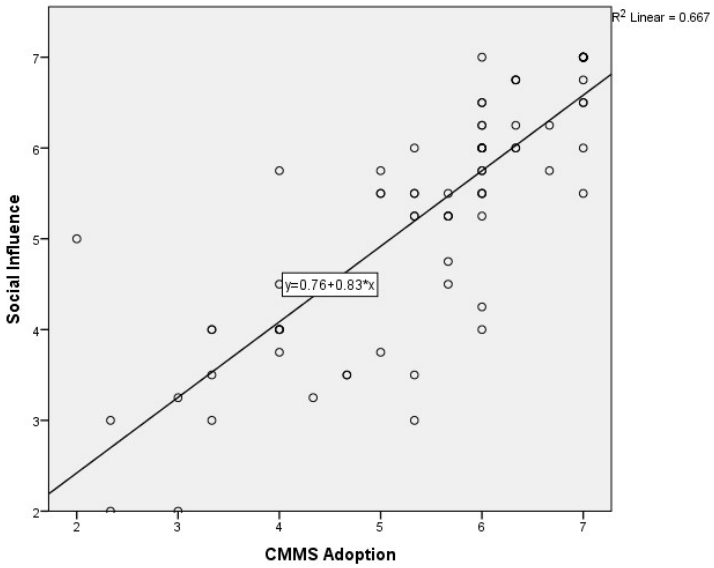
Note. Performance Expectancy and CMMS adoption scatterplot

Figure 1: Scatterplot diagram performance expectancy



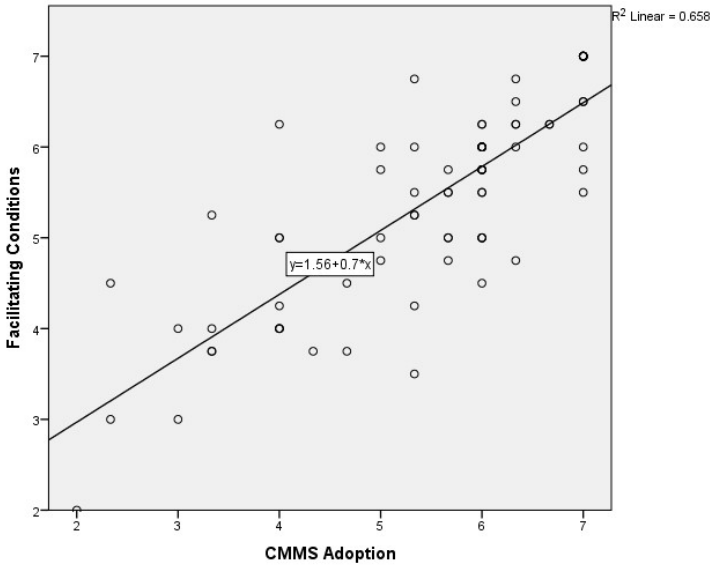
Note. Effort Expectancy and CMMS adoption scatterplot

Figure 2: Scatterplot diagram effort expectancy



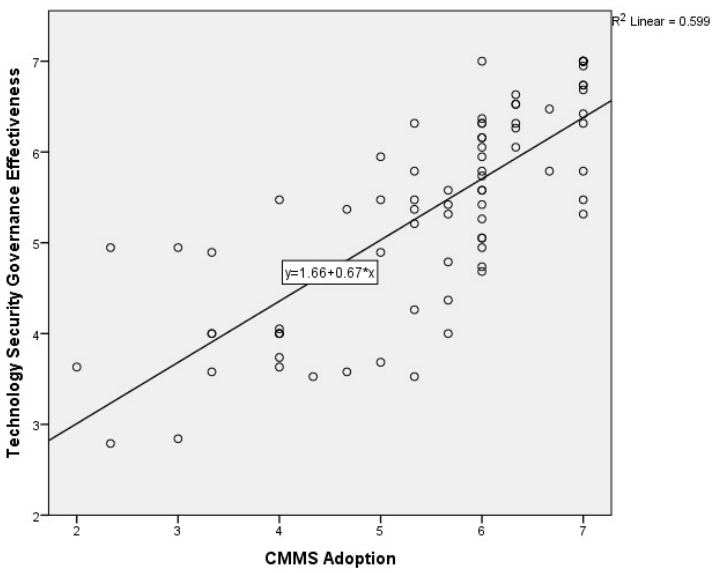
Note. Social Influence and CMMS adoption scatterplot

Figure 3: Scatterplot diagram social influence



Note. Facilitating Conditions and CMMS adoption scatterplot

Figure 4: Scatterplot diagram facilitating conditions



Note. Technlology Security Governance Effectivness and CMMS adoption scatterplot

Figure 5: Scatterplot diagram technology security governance effectiveness

When performing hypothesis testing is important to determine if any outliers exist within the dataset. Mahalanobis distance evaluated as a chi-square (χ^2) statistic with degrees of freedom equal to the number of variables in the analysis (Mertler & Reinhart, 2016). The accepted criterion for outliers is a value for Mahalanobis distance that is significant beyond $p < .001$, determined by comparing the obtained value for Mahalanobis distance to the chi-square critical value. Degrees of Freedom = 6 and p =.001 has a Chi-square value of 16.81 (Mertler & Reinhart, 2016, p.357). Based on the Mahalanobis distance, three respondents' information classified as outliers since their mahalanobis distance greater than 16.81. The three cases presented in Table 10 eliminated from future analysis.

Table 10: Extreme Values

			Case Number	Value
Mahalanobis Distance	Highest	1	30	29.24681
		2	60	20.26771
		3	1	18.44082
		4	74	16.73952
		5	32	13.57826
	Lowest	1	52	.19157
		2	45	.29542
		3	68	.36895
		4	56	.51413
		5	62	.66957

Note. Mahalanobis Distance (χ^2=16.81, p<.001, df=6)

RQ1: To what extent does Performance Expectancy (PE) correlate to the adoption of a Computerized Maintenance Management System?

$H1_0$ - There is no statistically significant correlative relationship between PE and adoption of Computerized Maintenance Management System (CMMS)

$H1_A$ - There is a statistically significant correlative relationship between PE and adoption of Computerized Maintenance Management System (CMMS)

The Spearman's rank-order correlation coefficient determined that the UTAUT variable, PE, has a statistically significant relationship to the adoption of CMMS by IT managers in the healthcare industry. The variable, PE, had a mean score of 5.46 with a standard deviation of 1.139, and the dependent variable, CMMS, had a mean score of 5.59 with a standard deviation of 1.186 among healthcare IT managers use of CMMS. At the 0.050 level of significance, the calculated Spearman's rank-order correlation coefficient, the analysis yielded a correlation coefficient of 0.760 with a two-tail significance of 0.000. Because the calculated two-tail

significance is less than the level of significance, the null hypothesis rejected, meaning that there is a statistically significant relationship between the independent and dependent variables. Therefore, IT managers in the healthcare industry relate the UTAUT variable, PE, to the adoption of CMMS. Table 11 presents the descriptive statistics, and Table 12 presents Spearman's rank-order correlation coefficient results for $H1_A$.

Table 11: Descriptive Statistics Performance Expectancy

	N	Minimum	Maximum	Mean	Std. Deviation
Performance Expectancy	74	3	7	5.46	1.139
CMMS Adoption	74	2	7	5.59	1.186
Valid N (listwise)	74				

Note. Descriptive statistics for performance expectancy where N=74

Table 12: Correlations Performance Expectancy

			Performance Expectancy	CMMS Adoption
Spearman's rho	Performance Expectancy	Correlation Coefficient	1.000	.760
		Sig. (2-tailed)	.	.000
		N	74	74
	CMMS Adoption	Correlation Coefficient	.760	1.000
		Sig. (2-tailed)	.000	.
		N	74	74

Note. Correlation is significant at the 0.01 level (2-tailed)

RQ2: To what extent does Effort Expectancy (EE) correlate to the adoption of a Computerized Maintenance Management System?

$H2_0$ - There is no statistically significant correlative relationship between EE and adoption of Computerized Maintenance Management System (CMMS)

$H2_A$ - There is a statistically significant correlative relationship between EE and adoption of Computerized Maintenance Management System (CMMS)

The Spearman's rank-order correlation coefficient determined that the UTAUT variable, EE, has a statistically significant relationship to the adoption of CMMS by IT managers in the healthcare industry. The variable, EE, had a mean score of 5.63 with a standard deviation of 1.090, and the dependent variable, CMMS, had a mean score of 5.59 with a standard deviation of 1.186 among healthcare IT managers use of CMMS. At the 0.050 level of significance, the calculated Spearman's rank-order correlation coefficient, the analysis yielded a correlation coefficient of 0.783 with a two-tail significance of 0.000. Because the calculated two-tail significance is less than the level of significance, the null hypothesis rejected, meaning that there is a statistically significant relationship between the independent and dependent variables. Therefore, IT managers in the healthcare industry relate the UTAUT variable, EE, to the adoption of CMMS. Table 13 presents the descriptive statistics, and Table 14 presents Spearman's rank-order correlation coefficient results for $H2_A$.

Table 13: Descriptive Statistics Effort Expectancy

	N	Minimum	Maximum	Mean	Std. Deviation
CMMS Adoption	74	2	7	5.59	1.186
Effort Expectancy	74	3	7	5.63	1.090
Valid N (listwise)	74				

Note. *Descriptive statistics for effort expectancy where* N=*74*

Table 14: Correlations Effort Expectancy

			CMMS Adoption	Effort Expectancy
Spearman's rho	CMMS Adoption	Correlation Coefficient	1.000	.783
		Sig. (2-tailed)	.	.000
		N	74	74
	Effort Expectancy	Correlation Coefficient	.783	1.000
		Sig. (2-tailed)	.000	.
		N	74	74

Note. Correlation is significant at the 0.01 level (2-tailed)

RQ3: To what extent does Social Influence (SI) correlate to the adoption of a Computerized Maintenance Management System?

$H3_0$ - There is no statistically significant correlative relationship between SI and adoption of Computerized Maintenance Management System (CMMS)

$H3_A$ - There is a statistically significant correlative relationship between SI and adoption of Computerized Maintenance Management System (CMMS)

The Spearman's rank-order correlation coefficient determined that the UTAUT variable, SI, has a statistically significant relationship to the adoption of CMMS by IT managers in the healthcare industry. The variable, SI, had a mean score of 5.40 with a standard deviation of 1.263, and the dependent variable, CMMS, had a mean score of 5.59 with a standard deviation of 1.186 among healthcare IT managers use of CMMS. At the 0.050 level of significance, the calculated Spearman's rank-order correlation coefficient, the analysis yielded a correlation coefficient of 0.847 with a two-tail significance of 0.000. Because the calculated two-tail significance is less than the level of significance, the null hypothesis rejected, meaning that there is a statistically significant relationship between the independent and dependent variables. Therefore, IT managers in the healthcare industry relate the UTAUT variable, SI, to the adoption of CMMS. Table 15 presents the descriptive statistics, and Table 16 presents Spearman's rank-order correlation coefficient results for $H3_A$.

Table 15: Descriptive Statistics Social Influence

	N	Minimum	Maximum	Mean	Std. Deviation
CMMS Adoption	74	2	7	5.59	1.186
Social Influence	74	2	7	5.40	1.263
Valid N (listwise)	74				

Note. Descriptive statistics for social influence where N=74

Table 16: Correlations Social Influence

			CMMS Adoption	Social Influence
Spearman's rho	CMMS Adoption	Correlation Coefficient	1.000	.847
		Sig. (2-tailed)	.	.000
		N	74	74
	Social Influence	Correlation Coefficient	.847	1.000
		Sig. (2-tailed)	.000	.
		N	74	74

Note. Correlation is significant at the 0.01 level (2-tailed)

RQ4: To what extent does Facilitating Conditions (FC) correlative the adoption of a Computerized Maintenance Management System?

$H4_0$ - There is no statistically significant correlative relationship between FC and adoption of Computerized Maintenance Management System (CMMS)

$H4_A$ - There is a statistically significant correlative relationship between FC and adoption of Computerized Maintenance Management System (CMMS)

The Spearman's rank-order correlation coefficient determined that the UTAUT variable, FC, has a statistically significant relationship to the adoption of CMMS by IT managers in the healthcare industry. The variable, FC, had a mean score of 5.50 with a standard deviation of 1.028, and the dependent variable, CMMS, had a mean score of 5.59 with a standard deviation of 1.186 among healthcare IT managers use of CMMS. At the 0.050 level of significance, the calculated Spearman's rank-order correlation coefficient, the analysis yielded a correlation coefficient of 0.781 with a two-tail significance of 0.000. Because the calculated two-tail significance is less than the level of significance, the null hypothesis rejected, meaning that there is a statistically significant relationship between the independent and dependent variables. Therefore, IT managers in the healthcare industry relate the UTAUT variable, FC, to the

adoption of CMMS. Table 17 presents the descriptive statistics, and Table 18 presents Spearman's rank-order correlation coefficient results for $H4_A$.

Table 17: Descriptive Statistics Facilitating Conditions

	N	Minimum	Maximum	Mean	Std. Deviation
CMMS Adoption	74	2	7	5.59	1.186
Facilitating Conditions	74	3	7	5.50	1.028
Valid N (listwise)	74				

Note. *Descriptive statistics for facilitating conditions where* N=*74*

Table 18: Correlations Facilitating Conditions

			CMMS Adoption	Facilitating Conditions
Spearman's rho	CMMS Adoption	Correlation Coefficient	1.000	.781
		Sig. (2-tailed)	.	.000
		N	74	74
	Facilitating Conditions	Correlation Coefficient	.781	1.000
		Sig. (2-tailed)	.000	.
		N	74	74

Note. Correlation is significant at the 0.01 level (2-tailed)

RQ5: To what extent does Technology Security Governance Effectiveness (TSGE) correlate to the adoption of a Computerized Maintenance Management System?

$H5_0$ - There is no statistically significant correlative relationship between TSGE and adoption of Computerized Maintenance Management System (CMMS)

$H5_A$ - There is a statistically significant correlative relationship TSGE impact and adoption of Computerized Maintenance Management System (CMMS)

The Spearman's rank-order correlation coefficient determined that the variable, TSGE, has a statistically significant relationship to the adoption of CMMS by IT managers in the healthcare industry. The variable, TSGE, had a mean score of 5.41 with a standard deviation of

1.116, and the dependent variable, CMMS, had a mean score of 5.59 with a standard deviation of 1.186 among healthcare IT managers use of CMMS. At the 0.050 level of significance, the calculated Spearman's rank-order correlation coefficient, the analysis yielded a correlation coefficient of 0.790 with a two-tail significance of 0.000. Because the calculated two-tail significance is less than the level of significance, the null hypothesis rejected, meaning that there is a statistically significant relationship between the independent and dependent variables. Therefore, IT managers in the healthcare industry relate the variable, TSGE, to the adoption of CMMS. Table 19 presents the descriptive statistics, and Table 20 presents Spearman's rank-order correlation coefficient results for $H5_A$.

Table 19: Descriptive Statistics Technology Security Governance Effectiveness

	N	Minimum	Maximum	Mean	Std. Deviation
CMMS Adoption	74	2	7	5.59	1.186
Technology Security Governance Effectiveness	74	3	7	5.41	1.116
Valid N (listwise)	74				

Note. Descriptive statistics for technology security governance effectiveness where *N*=74

Table 20: Correlations Technology Security Governance Effectiveness

			CMMS Adoption	Technology Security Governance Effectiveness
Spearman's rho	CMMS Adoption	Correlation Coefficient	1.000	.790
		Sig. (2-tailed)	.	.000
		N	74	74
	Technology Security Governance Effectiveness	Correlation Coefficient	.790	1.000
		Sig. (2-tailed)	.000	.
		N	74	74

Note. Correlation is significant at the 0.01 level (2-tailed)

RQ6: How well does performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance predict the adoption of computerized maintenance management systems?

$H6_0$ - there will be no statistically significant prediction of CMMS adoption by performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance.

$H6_a$ - there will be a statistically significant prediction of CMMS adoption by performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance.

An assessment of the measurement model performed using the partial least squares (PLS) regression technique to reduce the factors to a group of components that related to the measurement variable. Figure 6 contains the Partial Least Squares model generated by SmartPLS, and shows the indicators that kept in the final model based on having a value of above .70. Most measurement variables remained in the study since all outer loadings were in the .70 required range, except FC3 and TSGE15 since their value is 0.533 and 0.453. The PLS regression model examines multiple independent and dependent variables and is not dependent on normalized data distribution. Additionally, a large sample size is not required for PLS analysis (Hair, Hult, Ringle, & Sarstedt, 2017).

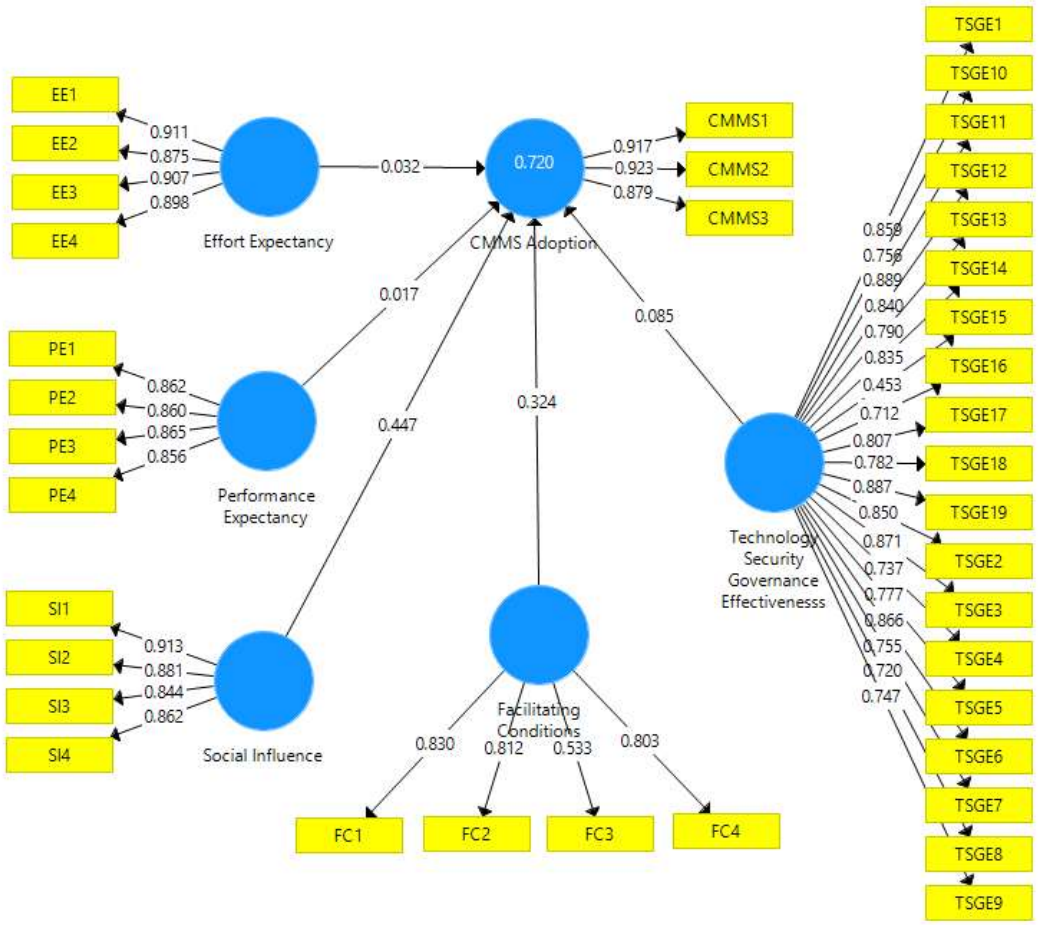


Figure 6: Partial least squares path model

Performance Expectancy measured by four questions on the survey related to CMMS adoption. The outer loading value for the four items were .862, .86, .865 and .856, included in Table 21. All outer loadings greater than .70 indicting that there was a high contribution of the questions assigned to the studies construct.

Table 21. Outer Loadings for PE

Item	Question Number	Variable	Outer Loading Value
PE1	Q8	Performance Expectancy	0.862
PE2	Q9	Performance Expectancy	0.86
PE3	Q10	Performance Expectancy	0.865
PE4	Q11	Performance Expectancy	0.856

Note. Outer loadings > .70 demonstrate a high contribution to the assigned construct

Effort Expectancy measured by four questions on the survey related to CMMS adoption. The outer loading value for the four items were .911, .875, .907 and .898, included in Table 22. All outer loadings greater than .70 indicting that there was a high contribution of the questions assigned to the studies construct.

Table 22. *Outer Loadings for EE*

Item	Question Number	Variable	Outer Loading Value
EE1	Q12	Effort Expectancy	0.911
EE2	Q13	Effort Expectancy	0.875
EE3	Q14	Effort Expectancy	0.907
EE4	Q15	Effort Expectancy	0.898

Note. Outer loadings > .70 demonstrate a high contribution to the assigned construct

Social Influence measured by four questions on the survey related to CMMS adoption. The outer loading value for the four items were .913, .881, .844 and .862, included in Table 23. All outer loadings greater than .70 indicting that there was a high contribution of the questions assigned to the studies construct.

Table 23. *Outer Loadings for SI*

Item	Question Number	Variable	Outer Loading Value
SI1	Q16	Social Influence	0.913
SI2	Q17	Social Influence	0.881
SI3	Q18	Social Influence	0.844
SI4	Q19	Social Influence	0.862

Note. Outer loadings > .70 demonstrate a high contribution to the assigned construct

Facilitating Conditions measured by four questions on the survey related to CMMS adoption. The outer loading value for the four items were .83, .812, .533 and .803, included in Table 24, three of the four items are greater than .70 indicting that there was a high contribution of the questions assigned to the studies construct. Question 22 had an outer loading value of .533 indicating a non-significant contribution to the construct. Question 22 removed from the analysis.

Table 24. *Outer Loadings for FC*

Item	Question Number	Variable	Outer Loading Value
FC1	Q20	Facilitating Conditions	0.83
FC2	Q21	Facilitating Conditions	0.812
FC3	Q22	Facilitating Conditions	0.533
FC4	Q23	Facilitating Conditions	0.803

Note. Outer loadings > .70 demonstrate a high contribution to the assigned construct

Technology Security Governance Effectiveness measured by nineteen questions on the survey related to CMMS adoption. The outer loading value for the four items were 0.859, 0.85, 0.871, 0.737, 0.777, 0.866, 0.755, 0.72, 0.747, 0.756, 0.889, 0.84, 0.79, 0.835, 0.453, 0.712, 0.807, 0.782, 0.887, included in Table 25, eighteen or the nineteen items are greater than .70 indicting that there was a high contribution of the questions assigned to the studies construct. Question 38 had an outer loading value of .453 indicating a non-significant contribution to the construct. Question 38 removed from the analysis.

Table 25. *Outer Loadings for TSGE*

Item	Question Number	Variable	Outer Loading Value
TSGE1	Q24	Technology Security Governance Effectiveness	0.859
TSGE2	Q25	Technology Security Governance Effectiveness	0.85
TSGE3	Q26	Technology Security Governance Effectiveness	0.871
TSGE4	Q27	Technology Security Governance Effectiveness	0.737
TSGE5	Q28	Technology Security Governance Effectiveness	0.777
TSGE6	Q29	Technology Security Governance Effectiveness	0.866
TSGE7	Q30	Technology Security Governance Effectiveness	0.755
TSGE8	Q31	Technology Security Governance Effectiveness	0.72
TSGE9	Q32	Technology Security Governance Effectiveness	0.747
TSGE10	Q33	Technology Security Governance Effectiveness	0.756
TSGE11	Q34	Technology Security Governance Effectiveness	0.889
TSGE12	Q35	Technology Security Governance Effectiveness	0.84
TSGE13	Q36	Technology Security Governance Effectiveness	0.79
TSGE14	Q37	Technology Security Governance Effectiveness	0.835
TSGE15	Q38	Technology Security Governance Effectiveness	0.453
TSGE16	Q39	Technology Security Governance Effectiveness	0.712
TSGE17	Q40	Technology Security Governance Effectiveness	0.807
TSGE18	Q41	Technology Security Governance Effectiveness	0.782
TSGE19	Q42	Technology Security Governance Effectiveness	0.887

Note. Outer loadings > .70 demonstrate a high contribution to the assigned construct

Computerized Maintenance Management System Adoption measured by three questions on the survey related to CMMS adoption. The outer loading value for the four items were .917, .923, and .879, included in Table 26, all greater than .70 indicting that there was a high contribution of the questions assigned to the studies construct.

Table 26. Outer Loadings for CMMS

Item	Question Number	Variable	Outer Loading Value
CMMS1	Q43	Computerized Maintenance Management System Adoption	0.917
CMMS2	Q44	Computerized Maintenance Management System Adoption	0.923
CMMS3	Q45	Computerized Maintenance Management System Adoption	0.879

Note. Outer loadings > .70 demonstrate a high contribution to the assigned construct

The mean correlation coefficients, p-values and t-statistic values associated with each relationship in the model displayed in Table 27. Only facilitating conditions has a statistically significant influence over behavioral intention for CMMS adoption. Effort expectancy, performance expectancy, social influence and technology security governance effectiveness *p* values >.05 indicating that they do not have a statistically significant predictive relationship over behavioral intention for CMMS adoption. Facilitating conditions is defined as the degree to which an individual believes that organizational and technical structures are present that will provide the use of the new technology or system (Venkatesh et al., 2012). While the UTAUT theory suggests that four key constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions are direct determinants of intent to adopt and use technology (Venkatesh et al., 2003), the current study only finds a statistically significant relationship between FC and the adoption of CMMS.

Table 27. Bootstrap Statistical Output

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
EE -> CMMS	0.032	0.06	0.191	0.166	0.868
FC -> CMMS	0.325	0.334	0.146	2.226	0.026
PE -> CMMS	0.017	0.016	0.166	0.102	0.919
SI-> CMMS	0.443	0.396	0.246	1.8	0.072
TSGE-> CMMS	0.087	0.104	0.159	0.549	0.583

Note. $p < 0.05$; EE = effort expectancy; FC = facilitating conditions; PE = performance expectancy; SI = social influence; TSGE = technology security governance effectiveness; CMMS = computerized maintenance management system adoption

The *r* square of CMMS adoption calculated in Table 28 reveals that .739 of the variance of CMMS adoption is explained by the model. The total adjusted *R2* was 0.72 for CMMS adoption. Therefore, the model explains 72% of the variance of CMMS adoption. The null

hypothesis rejected since there is a statistically significant prediction of CMMS adoption by the independent variable facilitating conditions with $p = .026 < .05$.

Table 28. R square of CMMS adoption

	R Square	R Square Adjusted
CMMS Adoption	0.739	0.72

Note. R square for CMMS adoption 0.739

Summary

A total of 77 IT managers completed the survey examining how healthcare personnel In the United States, understand the benefits of CMMS. Three of the participants' data are outliers and excluded from the hypothesis testing resulting in the final sample used of 74 participants. The study used Spearman's rank-order correlation coefficient to determine the relational analysis for this quantitative study. The results of the analysis indicated that IT managers relate UTAUT variables, PE, EE, SI, FC, and TSGE to the adoption of CMMS. The strength of the statistically significant relationship between independent and dependent variables in order of magnitude is: SI (0.847); TSGE (0.790); EE (0.783); FC (0.781); and PE (0.760). All six null hypotheses rejected resulting from the statistical analysis.

CHAPTER 5. DISCUSSION, IMPLICATIONS, RECOMMENDATIONS

Chapter 5 includes the summary of results produced from the Qualtrics survey instrument and interpretation of the findings. The summary of results are compared to previous research studies and conclusions and limitations discussed in further detail. Following the studies limitations, the theoretical and practical implications along with recommendations for future research described within the section.

Summary of the Results

The purpose of this quantitative research study is to assess the relationship among the UTAUT (Unified Theory of Acceptance and Use of Technology) variables: PE, EE, SI, FC, and TSGE and the outcome variable of the adoption of computerized maintenance management systems (CMMS) by IT managers in the healthcare industry. The studies six research questions and hypothesis summarized in this section.

Discussion for Research Hypothesis 1

RQ1: To what extent does Performance Expectancy (PE) correlate to the adoption of a Computerized Maintenance Management System?

$H1_0$ - There is no statistically significant correlative relationship between PE and adoption of Computerized Maintenance Management System (CMMS)

$H1_A$ - There is a statistically significant correlative relationship between PE and adoption of Computerized Maintenance Management System (CMMS)

After analyzing the findings of the research study, the first research question null hypotheses, the UTUAT variable PE, is rejected since PE has a statistically significant relationship to the adoption of CMMS by IT managers in the healthcare industry. Performance Expectancy (PE) defined as the consumer's belief that a technology or product will provide a

benefit to them when using it to complete an activity. (Harris et al., 2018; Rezaei, & Ghofranfarid, 2018; Venkatesh et al., 2003; Venkatesh et al., 2012). Performance expectancy refers to the perception of technology effectiveness, user's expectations for use, and impact on job performance by technology (Venkatesh et al., 2003). The variable, PE, had a mean score of 5.46 with a standard deviation of 1.139, and the dependent variable, CMMS adoption, had a mean score of 5.59 with a standard deviation of 1.186. At the .050 level of significance, the Spearman's rank-order correlation coefficient is .760, with a two-tail significant of .000. Therefore, according to the results for Hypothesis 1, the UTAUT variable, PE, is related to the adoption of CMMS for healthcare IT managers.

Discussion for Research Hypothesis 2

RQ2: To what extent does Effort Expectancy (EE) correlate to the adoption of a Computerized Maintenance Management System?

$H2_0$ - There is no statistically significant correlative relationship between EE and adoption of Computerized Maintenance Management System (CMMS)

$H2_A$ - There is a statistically significant correlative relationship between EE and adoption of Computerized Maintenance Management System (CMMS)

After analyzing the findings of the research study, the second research question null hypotheses, the UTUAT variable EE, is rejected since EE has a statistically significant relationship to the adoption of CMMS by IT managers in the healthcare industry. Effort Expectancy (EE) defined as the degree to which a consumer feels that a product or technology is easy to use (Venkatesh et al., 2012). The variable, EE, had a mean score of 5.63 with a standard deviation of 1.090, and the dependent variable, CMMS adoption, had a mean score of 5.59 with a standard deviation of 1.186. At the .050 level of significance, the Spearman's rank-order

correlation coefficient is .783, with a two-tail significant of .000. Therefore, according to the results for Hypothesis 2, the UTAUT variable, EE, is related to the adoption of CMMS for healthcare IT managers.

Discussion for Research Hypothesis 3

RQ3: To what extent does Social Influence (SI) correlate to the adoption of a Computerized Maintenance Management System?

$H3_0$ - There is no statistically significant correlative relationship between SI and adoption of Computerized Maintenance Management System (CMMS)

$H3_A$ - There is a statistically significant correlative relationship between SI and adoption of Computerized Maintenance Management System (CMMS)

After analyzing the findings of the research study, the third research question null hypotheses, the UTUAT variable SI, is rejected since SI has a statistically significant relationship to the adoption of CMMS by IT managers in the healthcare industry. Social Influence (SI) is defined the A measurement of the impact that other people who are essential to the consumer's life have on the decision to adopt a product or technology (Harris et al., 2018; Rezaei, & Ghofranfarid, 2018; Venkatesh et al., 2003; Venkatesh et al., 2012). Social influence originates from the theory of reasoned actions and comparable to the subjective norms. The social influence construct refers to the user's impression of other people considering the technology as well as how technology measures into the social norms, feeling in reverences to if they should or should not use the technology, and the user perception of self-image (Venkatesh et al., 2003). The variable, SI, had a mean score of 5.40 with a standard deviation of 1.263, and the dependent variable, CMMS, had a mean score of 5.59 with a standard deviation of 1.186 among healthcare IT managers use of CMMS. At the 0.050 level of significance, the calculated Spearman's rank-

order correlation coefficient, the analysis yielded a correlation coefficient of 0.847 with a two-tail significance of 0.000. Because the calculated two-tail significance is less than the level of significance, the null hypothesis rejected, meaning that there is a statistically significant relationship between the independent and dependent variables. Therefore, IT managers in the healthcare industry relate the UTAUT variable, SI, to the adoption of CMMS.

Discussion for Research Hypothesis 4

RQ4: To what extent does Facilitating Conditions (FC) correlative the adoption of a Computerized Maintenance Management System?

$H4_0$ - There is no statistically significant correlative relationship between FC and adoption of Computerized Maintenance Management System (CMMS)

$H4_A$ - There is a statistically significant correlative relationship between FC and adoption of Computerized Maintenance Management System (CMMS)

After analyzing the findings of the research study, the fourth research question null hypotheses, the UTUAT variable FC, is rejected since FC has a statistically significant relationship to the adoption of CMMS by IT managers in the healthcare industry. Facilitating conditions is defined as the degree to which an individual believes that organizational and technical structures are present that will provide the use of the new technology or system (Venkatesh et al., 2012). Facilitating conditions is the degree a user believes there is backing for the technology mutually from the organization and technical infrastructure (Venkatesh et al., 2003). Facilitating conditions are inclusive with training and the resources required using the technology. The variable, FC, had a mean score of 5.50 with a standard deviation of 1.028, and the dependent variable, CMMS, had a mean score of 5.59 with a standard deviation of 1.186 among healthcare IT managers use of CMMS. At the 0.050 level of significance, the calculated

Spearman's rank-order correlation coefficient, the analysis yielded a correlation coefficient of 0.781 with a two-tail significance of 0.000. Because the calculated two-tail significance is less than the level of significance, the null hypothesis rejected, meaning that there is a statistically significant relationship between the independent and dependent variables. Therefore, IT managers in the healthcare industry relate the UTAUT variable, FC, to the adoption of CMMS.

Discussion for Research Hypothesis 5

RQ5: To what extent does Technology Security Governance Effectiveness (TSGE) correlate to the adoption of a Computerized Maintenance Management System?

$H5_0$ - There is no statistically significant correlative relationship between TSGE and adoption of Computerized Maintenance Management System (CMMS)

$H5_A$ - There is a statistically significant correlative relationship TSGE impact and adoption of Computerized Maintenance Management System (CMMS)

After analyzing the findings of the research study, the fifth research question null hypotheses, the UTUAT variable TSGE, is rejected since TSGE has a statistically significant relationship to the adoption of CMMS by IT managers in the healthcare industry. Technology Security Governance Effectiveness (TSGE) defined as the standard tools, processes, and methodologies that enable an organization to align business strategy and goals with IT services, infrastructure, or the environment. (Harris et al., 2018; Rezaei, & Ghofranfarid, 2018). The variable, TSGE, had a mean score of 5.41 with a standard deviation of 1.116, and the dependent variable, CMMS, had a mean score of 5.59 with a standard deviation of 1.186 among healthcare IT managers use of CMMS. At the 0.050 level of significance, the calculated Spearman's rank-order correlation coefficient, the analysis yielded a correlation coefficient of 0.790 with a two-tail significance of 0.000. Because the calculated two-tail significance is less than the level of

significance, the null hypothesis rejected, meaning that there is a statistically significant relationship between the independent and dependent variables. Therefore, IT managers in the healthcare industry relate the variable, TSGE, to the adoption of CMMS.

Discussion for Research Hypothesis 6

RQ6: How well does performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance predict the adoption of computerized maintenance management systems?

$H6_0$ - there will be no statistically significant prediction of CMMS adoption by performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance.

$H6_a$ - there will be a statistically significant prediction of CMMS adoption by performance expectancy, effort expectancy, social influence, facilitating conditions, and technology security governance.

The *r* square of CMMS adoption reveals that .739 of the variance of CMMS adoption is explained by the model. The total adjusted R2 was 0.72 for CMMS adoption. Therefore, the model explains 72% of the variance of CMMS adoption. The null hypothesis rejected since there is a statistically significant prediction of CMMS adoption by the independent variable facilitating conditions with $p = .026 < .05$.

Discussion of the Results

The evolution of technology creates a demand for more efficient and faster system maintenance management activities. Improved infrastructure results in organizations moving from manual to automated preventive repairs to help IT managers perform their jobs more effectively. Investing in CMMS technologies is a significant undertaking, and management

needs to outweigh the benefits of implementing the new technology, including staff training on its use, with the implementation and ongoing support costs. CMMS systems facilitate healthcare operation by saving time, streamlining operations, resulting in enhanced efficiencies and patient experience (Cohen, 2014). An instrument to assist in determining the potential barriers to the adoption of CMMS systems by IT managers is beneficial to decision-makers tasked with implementing this infrastructure within the healthcare industry. The UTUAT framework guided the study for the testing procedures, and a review of the literature of healthcare information technology software included in the research. The review of the literature demonstrates that CMMS implemented to manage and reduce resources, enable compliance with security standards, enable decision-making for legacy medical devices, and to track medical device cybersecurity measures reducing risks for health delivery organizations (Jalali, & Kaiser, 2018; Jamkhaneh et al., 2018). The literature review also revealed that research on the adoption of CMMS and the behavioral characteristics of health delivery organizations influence, acceptance, and perceived usefulness of CMMS would add to the overall body of knowledge on information technology security and assurance.

Demographic information included in this study contains participant age range, technology job classification, organization size, and years of experience using CMMS, which provides insight into the familiarity of the technology. If the UTAUT results from this study reveal a correlation with the adoption of CMMS and the familiarity of the technology, to ease the transition of implementing CMMS within the healthcare industry, decision-makers could potentially focus on IT managers that have a higher level of experience with this specific type of system.

Conclusions Based on the Results

Comparison of the Findings with the Theoretical Framework and Previous Literature

This study related the UTAUT framework to the adoption of computerized maintenance management systems. Similar to previous research, this study expanded the theoretical framework to encompass technology security governance effectiveness influencing the adoption of a CMMS by IT managers in the healthcare industry (Jamkhaneh et al., 2018). Previous studies demonstrate that factors including performance expectancy, effort expectancy, social influence, facilitating conditions, technology security governance effectiveness influences the adoption rate of new technologies within enterprises. The current research examines factors and the correlation to the adoption of a CMMS. While previous studies demonstrate that all UTAUT variables predict new system adoption and usage (Jamkhaneh et al., 2018), the current study focuses on the impact on the adoption of the specific CMMS technology.

Interpretation of the Findings

The results of the analysis indicated that IT managers relate UTAUT variables, PE, EE, SI, FC, and TSGE to the adoption of CMMS. The strength of the statistically significant relationship between independent and dependent variables in order of magnitude is: SI (0.847); TSGE (0.790); EE (0.783); FC (0.781); and PE (0.760). All six null hypotheses rejected as a result of the analysis using IBM SPSS software. The data collected is reliable and valid as per the partial least squares conducted indicating most variable remained in the study resulting from the outer loadings being above the .70 required range. All five independent variables PE, EE, SI, FC, TSGE has a positive correlation on the adoption of a CMMS for IT manager working in the healthcare industry.

Limitations

This study included organizations located in the United States, and cultures could respond differently to the survey questions in addition to a different type of method used other than an online quantitative questionnaire regarding the adoption of computerized maintenance management systems. Healthcare technology managers' targeted for the study, and other industrial samples and professions selected to determine if the results are similar across other sectors. Survey participants' role defined by the organization title; all respondents selected are IT professionals limited the studies perception of IT security governance, and UTAUT factors influencing the decision to adopt computerized maintenance management systems.

The study assumes that the US bureau of labor statistics is representative of the entire set of IT managers in the healthcare industry in the United States. The study used the UTAUT methodology developed by Venkatesh et al. (2003) as the most suitable framework for this study's purpose and research questions. There are study limitations that need acknowledgment, including time and financial constraints. The small sample size was selected as compared to the population, and a larger sample would make the results more generalizable. This research study focused on six aspects of IT managers' demographics and the adoption of computerized maintenance management systems. Demographics consist of respondent's data on industry, organization type, age, gender, organization size, and job title. While consumer demographic information was collected, no statistical analysis conducted.

Implications for Practice

Although this study aimed to use the UTAUT survey instrument to determine the factors that affect healthcare IT managers and the adoption of computerized maintenance management systems, the results are beneficial on a much larger scale. The results of this research can have a

positive influence on the delivery of healthcare computer systems. The results of the study indicate the potential for the UTAUT model to be highly useful when introducing or implementing CMMS on a large scale within organizations and the importance of technology security governance effectiveness. CMMS helps to manage data on the maintenance workforce, inventories, repair schedule, and equipment history. Workload maintenance and management performed via CMMS technologies and are vital for coordination related to productivity, availability, and maintainability of the systems. CMMS improves maintenance performance by recording, planning, and conducting maintenance actions designed to provide data for the decision-making process healthcare IT managers (Jokela, Siponen, Hirasawa, & Earthy, 2006). The greatest weakness related to CMMS used to be a standalone system. The end-user could not access more than one system at a time and had to use different computers to access different data. The integrated CMMS solution allows systems to communicate with each other, transfers data and interacts between applications.

This study for practitioners and scholars implies that non-technical variables influence the decision-making IT managers responsible for the adoption of computerized maintenance management systems. The results of the research indicate that CMMS vendors need to address the UTAUT factors of PE, EE, FC, SI, and TSGE identified in this research to promote the widespread adoption of the technology within healthcare organizations. The decision on whether or not to adopt CMMS depends on whether the technology supports the organizations' needs and strategies, is cost-effective, is reliable, and employs effective technology security governance mechanisms. The market for CMMS systems requires a more complex collaboration between potential customers and vendors rather than merely providing a catalog and price chart. Addressing the healthcare IT managers' needs can include supplying data about CMMS

reliability, security, and how the technology can satisfy organizational needs in terms of performance and effort expectancy required to learn how to operate the systems. User adoption is a critical factor when it comes to organizations maximizing the return on investment in CMMS (Sharma & Tewari, 2019). Involving all stakeholders at the onset of requirements gathering and needs, assessment along with a presentation of the benefits of CMMS will promote users to approve the new technology change. Additionally, making the software easy to use, removing complex processes or functions will promote CMMS adoption.

CMMS adoption in organizations is challenging because of the economic, social, and infrastructural limitations. A CMMS adoption model proposed to explore the critical factors influencing the decision of adoption of CMMS by IT managers in healthcare organizations in the United States. Fraser et al. (2015) argue that every organization should establish guiding principles to lay the foundation on which a CMMS will thrive. While every company is different and might establish a different set of principles, companies should create a culture that supports the implementation of CMMS technologies.

Recommendations for Further Research

Implementing computerized maintenance management systems has a significant impact on IT managers' ability to manage asset inventory and maintenance across global organizations with multiple stakeholders. The return on investment of CMMS results from decreased asset downtime, efficiency gains, optimized performance, inventory management, and an increase in asset lifespan. To get different perspectives on how CMMS could be a benefit or a hindrance, further research could include physicians, healthcare professions, as well as executives such as the chief financial officers and chief executive officers. Future research should include a longitudinal study to identify and measure if there are any attitude changes by healthcare role

and their intention to adopt CMMS. On-premise, cloud, or hybrid environments used to deploy CMMS and investigated whether the type of deployment influences CMMS adoption. The organizations typically manage On-premise own IT department, cloud-based hosted at vendor access via the internet, and hybrid is a combination of both models. A recommendation for future research on UTAUT's survey instrument as it applies to IT managers in the healthcare industry would be to focus on the qualitative or case study approach. Conducting research such as a case study or going onsite and speak to the healthcare IT managers in person. Future studies can conduct case studies on companies that adopted CMMS successfully and evaluate the decision making process and operational benefits.

The demographic data collected in this study more closely examined to determine if the relationship among those variables and CMMS adoption. Participant age range, technology job classification, organization size, and years of experience using CMMS descriptive variables measured in the study to determine technology acceptance within organizations and methods used to attract and retain end-users. In future studies, the population more varied since the individuals in this study represented a healthcare organization in the United States. The results from this study may not represent factors affecting technology security governance effectiveness and the adoption of computerized maintenance management systems among diverse sectors found outside the United States. Researchers can extend the geographic boundary of the study by gaining insight into multiple regions and a more diversified population with a bigger sample size to understand the differences between adoption cultures. Implementing standardized CMMS systems for medical devices in the healthcare industry has several challenges. Companies have benefited from technology, but feedback from the field is limited. This study provides quantitative information related to the UTAUT variable and TSGE factors influencing the

adoption of CMMS using the Qualtrics online questionnaire. Future research can include other framework variables such as technology, organizational, and environmental (T-O-E) variables that influence the adoption of new technology.

There is little research done on the impact of implementing CMMS, and future studies could provide additional data focusing on the industry-specific impact of the technology. Baseline information such as inventory and asset management, as well as organization-specific metrics documented and monitored for sustainment through CMMS. The healthcare industry should create a standard for CMMS over the upcoming years and obtain global concurrence to promote organizations working together for the implementation of standardized systems to enhance medical device safety and reduction errors. Studies could examine the regulatory influence and set of standardized procedures influence technology adoption. Research indicates that HDO cybersecurity threats are increasing resulting in security breaches that interrupt patient services, impact patient safety, and theft of patient data, these cybersecurity threats should be the highest priority for HDO's (Ehrenfeld, 2017). Continued research in this area is required to support HDO's abilities to manage medical system security and assess security risks across vast technology landscapes, multi-platform environments, and medical devices. By providing the perceived behavior influences of the adoption of CMMS, IT managers in the Healthcare industry may be able to use this study to improve security controls lowering the risks of cybersecurity threats. Future research can identify the impact of top management support influencing the adoption of CMMS within organizations of different sizes. Researchers of future studies could include business size, including measurements about start-up, medium, and large size organizations.

Conclusion

This study shows a statistically significant correlative relationship between information security governance effectiveness, facilitating conditions, social influence, effort expectancy, performance expectancy factors and adoption of CMMS (Harris et al., 2018; Rezaei, & Ghofranfarid, 2018; Venkatesh et al., 2003; Venkatesh et al., 2012). The primary reason for this study is to investigate factors influencing the adoption of CMMS by IT managers in the healthcare industry located in the United States. Adoption of a comprehensive system to capture asset management data is the best option organizations have to track and manage assets along with maintenance activities preventing system failures and outages. Understanding acceptance factors influencing CMMS information security governance effectiveness will help organizations better prepare for the adoption of the application technology. The research conducted using an online questionnaire measuring factors influencing the intention to adopt and use CMMS within IT organizations identified a variance of use behavior explained by the UTAUT variables.

The research highlights key factors influencing the intent to adopt CMMS and the need for future research to address gaps in existing studies. Companies must focus on successfully implementing comprehensive technology security governance effectiveness in order to protect information assets digitalized within computerized maintenance management systems. The business decision of whether to adopt CMMS relies heavily on the unified theory of acceptance and use of technology is a technology acceptance model variables. Five factors examined had statistically significant relationships and determined to be significant factors affecting IT managers' decision to adopt CMMS in the United States healthcare industry. Between the five factors, social influence and technology security governance effectiveness determined to be the most significant factors influencing IT managers' intent to implement CMMS. The study's

findings might help IT decision-makers, and CMMS providers understand how decisions made and what influencing factors need consideration when deploying the new technology. Existing research indicates that normative pressure and social influence exhibit the most substantial effects on an organization's intends to adopt CMMS applications (Yoon & Kim, 2013).

Nevertheless, other researches argue that external pressure does not influence the attitude towards technology adoption (Gholami, Sulaiman, Ramayah, & Molla, 2013). The empirical research contributes to the limited research on the adoption of computerized maintenance management systems offering a broad investigation of the correlative variables through the assessment of the UTAUT aspects of the framework. This study conducted using a quantitative online survey methodology with correlational design, and future studies could extend this research by using other technology adoption theories and qualitative methodologies to explore additional factors influencing CMMS adoption. Although addressing technical concerns of CMMS technology is essential, it is just critical to evaluate how adopting and implementing advanced maintenance management systems fits in with the organizations' structure, culture, objectives, and goals.

REFERENCES

Alreemy, Z., Chang, V., Walters, R., & Wills, G. (2016). Critical success factors (CSFs) for information technology governance (ITG). *International Journal of Information Management, 36*, 907-916. doi:10.1016/j.ijinfomgt.2016.05.017

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly, 41*, 893-914. doi:10.25300/MISQ/2017/41.3.10

Argaw, S. T., Bempong, N., Eshaya-Chauvin, B., & Flahault, A. (2019). The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review. *BMC Medical Informatics & Decision Making, 19*, 10-21. doi:10.1186/s12911-018-0724-5

Arias-Oliva, M., Pelegrín-Borondo, J., & Matías-Clavero, G. (2019). Variables influencing cryptocurrency use: A technology acceptance model in Spain. *Frontiers in Psychology, 10*, 475-488. doi:10.3389/fpsyg.2019.00475

Au, M. H., Yuen, T. H., Liu, J. K., Susilo, W., Huang, X., Xiang, Y., & Jiang, Z. L. (2017). A general framework for secure sharing of personal health records in cloud system. *Journal of Computer and System Sciences, 90*, 46-62. doi:10.1016/j.jcss.2017.03.002

Awa, H. O., Uko, J. P., & Ukoha, O. (2017). An empirical study of some critical adoption factors of ERP software. *International Journal of Human–Computer Interaction, 33*, 609-622. doi:10.1080/10447318.2016.1265828

Benham-Hutchins, M., Staggers, N., Mackert, M., Johnson, A. H., & DeBronkart, D. (2017). "I want to know everything": a qualitative study of perspectives from patients with chronic diseases on sharing health information during hospitalization. *BMC health services research*, *17*, 529-543. doi:10.1186/s12913-017-2487-6

Bero, L. (2013). Industry sponsorship and research outcome: A cochrane review. *JAMA Internal Medicine, 173*, 580-581. doi:10.1001/jamainternmed.2013.4190

The Bureau of Labor Statistics (2016). *Medical and health services managers*. Retrieved from https://www.bls.gov/ooh/management/medical-and-health-services-managers.htm

Busdicker, M., & Upendra, P. (2017). The role of healthcare technology management in facilitating medical device cybersecurity. *Biomedical Instrumentation & Technology, 51*, 19-25. doi:10.2345/0899-8205-51.s6.19

Chen, K. F., Hwang, H., Sher, M., & Lin, E. H. (2016). An empirical study of concern for privacy on providing health information in the EMR context. *Door, 12*, 677-688.

Cohen, T. (2014). The Basics of CMMS. *Biomedical Instrumentation & Technology*, *48*, 117-121. doi:10.2345/0899-8205-48.2.117

Copeland, S. (2018). Gathering basic information in support of medical network risk management. *Biomedical Instrumentation & Technology, 52*, 112-119. doi:10.1108/BIJ-05-2016-0072

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas, 113*, 48-52. doi:10.1016/j.maturitas.2018.04.008

Creswell, J. W. (2009). *Research design qualitative, quantitative, and mixed method approaches* (3rd ed.). Thousand Oaks, CA: Sage.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*, 319-340. doi:10.2307/249008

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*, 982-1003. doi:10.1287/mnsc.35.8.982

Dedeurwaerdere, T. (2018). From ecological psychology to four varieties of post-positivism in transdisciplinary science. *Environment Systems and Decisions*, *38*, 79-83. doi: 10.1007/s10669-017-9663-4

Dutot, V., Bhatiasevi, V., & Bellallahom, N. (2019). Applying the technology acceptance model in a three-countries study of smartwatch adoption. *The Journal of High Technology Management Research, 20*(1), 1-14. doi:10.1016/j.hitech.2019.02.001

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

Ehrenfeld, J. M. (2017). WannaCry, cybersecurity and health information technology: A time to act. *Journal of Medical Systems, 41*, 41-104. doi:10.1007/s10916-017-0752-1

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

Fedorko, I., Bacik, R., & Gavurova, B. (2018). Technology acceptance model in e-commerce segment. *Management & Marketing, 13*, 1242-1256. doi:10.2478/mmcks-2018-0034

Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th ed.). Thousand Oaks, CA: Sage.

Finnemore, M. (2018). Ethical dilemmas in cyberspace. *Ethics & International Affairs, 32*, 457-462. doi:10.1017/S0892679418000576 pmid:

Fishbein, M., & Ajzen, I. (1975). In Addison-Wesley (Ed.), *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Fortin, J., Bloomfield, P., Mahaz, J., & Alfaqih, L. (2018). Guidebook for advanced computerized maintenance management system integration at airports. *Science Engineering Medicine, 155, 66-151.* doi: 10.17226/25053

Fowler, F. (2009). *Survey research methods*. Thousand Oaks, CA: Sage.

Fraser, K., Hvolby, H., & Tseng, T. (2015). Maintenance management models: A study of the published literature to identify empirical evidence. *The International Journal of Quality & Reliability Management, 32*, 635-664. doi:10.1108/IJQRM-11-2013-0185

Fuad, A., & Hsu, C. (2018). UTAUT for HSS: Initial framework to study health IT adoption in the developing countries. *F1000research, 7*, 101-107. doi:10.12688/f1000research.13798.1

García, J., Rodriguez, R., & Fdez, J. (2015). Bias and effort in peer review. *Journal of the Association for Information Science & Technology, 66*, 2020-2030. doi:10.1002/asi.23307

Garner, R. L. (2017). Evaluating solutions to cyber attack breaches of health data: How enacting a private right of action for breach victims would lower costs. *Ind.Health L.Rev., 14*, 127-266.

Gholami, R., Sulaiman, A. B., Ramayah, T., & Molla, A. (2013). Senior managers' perception on green information systems (IS) adoption and environmental performance: Results from a field survey. *Information & Management, 50*, 431-438. doi:10.1016/j.im.2013.01.004

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

Griebel, L., Prokosch, H., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., … Sedlmayr, M. (2015). A scoping review of cloud computing in healthcare. *BMC Medical Informatics and Decision Making, 15*, 17-20.

Groves, P., Kayyali, B., Knott, D., & Kuiken, S. V. (2016). The 'big data' revolution in healthcare: Accelerating value and innovation. *The McKinsey Quarterly, 2,* 3-7.

Guo, Y., Kopec, J. A., Cibere, J., Li, L. C., & Goldsmith, C. H. (2016). Population survey features and response rates: A randomized experiment. *American Journal of Public Health, 106*, 1422-1426. doi:10.2105/AJPH.2016.303198

Hadban, W., Yusof, S., & Hashim, K. (2017). The barriers and facilitators to the adoption of new technologies in public healthcare sector: A qualitative investigation. *International Journal of Business and Management, 12*, 159-168. doi:10.5539/ijbm.v12n1p159

Hair, J. F., Hult, T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling* (*PLS-SEM*). Thousand Oaks, CA: Sage

Haneem, F., Kama, N., Taskin, N., Pauleen, D., & Bakar, N. A. A. (2019). Determinants of master data management adoption by local government organizations: An empirical study. *International Journal of Information Management, 45*, 25-43. doi:10.1016/j.ijinfomgt.2018.10.007

Harris, M. E., Mills, R. J., Fawson, C., & Johnson, J. J. (2018). Examining the impact of training in the unified theory of acceptance and use of technology. *Journal of Computer Information Systems, 58*, 221-233. doi:10.1080/08874417.2016.1230725

Hayes, A. F., Montoya, A. K., & Rockwood, N. J. (2017). The analysis of mechanisms and their contingencies: PROCESS versus structural equation modeling. *Australasian Marketing Journal (AMJ), 25*, 76-81. doi:10.1016/j.ausmj.2017.02.001

Hess, T. J., McNab, A. L., & Basoglu, K. A. (2014). Reliability generalization of perceived ease of use, perceived usefulness, and behavioral intentions. *M IS Quarterly, 38*(1), 1-29. doi:10.25300/MISQ/2014/38.1.01

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research, 20*, 1439-1456. doi:10.2196/10059

Jamkhaneh, H., Pool, J., Khaksar, M., Arabzad, M., & Kazemi, R. (2018). Impacts of computerized maintenance management system and relevant supportive organizational factors on total productive maintenance. *Benchmarking: An International Journal, 25*, 2230-2247. doi:10.1108/BIJ-05-2016-0072

Jokela, T., Siponen, M., Hirasawa, N., & Earthy, J. (2006). A survey of usability capability maturity models: implications for practice and research. *Behaviour & Information Technology*, *25*, 263-282. doi: 10.1080/0144929050016807

Kafali, Ö., Jones, J., Petruso, M., Williams, L., & Singh, M. P. (2017). How good is a security policy against real breaches?: A HIPAA case study. Paper presented at the *Proceedings of the 39th International Conference on Software Engineering,* 530-540.

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection, 9*, 52-80. doi:10.1016/j.ijcip.2015.02.002

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of Medical Systems, 41*(8), 1-9. doi:10.1007/s10916-017-0778-4

Laerd Statistics (2018). *Multiple regression using SPSS statistics*. Retrieved February 13, 2020, from Laerd Statistics: https://statistics.laerd.com/premium/spss/mr/multiple-regression-in-spss.php

Lai, P. C. (2017). The literature review of technology adoption models and theories for the novelty technology. *Journal of Information Systems and Technology Management : JISTEM, 14*, 21-38. doi:10.4301/S1807-17752017000100002

Lee, B. S., Walker, J., Delbanco, T., & Elmore, J. G. (2016). Transparent electronic health records and lagging LawsTransparent electronic health records. *Annals of Internal Medicine, 165*, 219-220.

Lemberg, A. (2017). Hackers made me lose my job: Health data privacy and its potentially devastating effect on the LGBTQ population. *Golden Gate UL Rev., 47*, 175.

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems, 30*, 40-55. doi:10.1016/j.accinf.2018.06.003

Liker, J. K., & Sindi, A. A. (1997). User acceptance of expert systems: A test of the theory of reasoned action. *Journal of Engineering and Technology Management, 14*, 147-173. doi:10.1016/S0923-4748(97)00008-8

Malhotra, V. (2018). CTO foresees future of CMMS-enabled 'true interoperability'. *Biomedical Instrumentation & Technology, 52*, 60-62. doi:10.2345/0899-8205-52.1.60

Martin, G., Ghafur, S., Kinross, J., Hankin, C., & Darzi, A. (2018). WannaCry-a year on. *BMJ (Clinical Research Ed.), 361*, 2381-2383. doi:10.1136/bmj.k2381

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

Mceachan, R., Taylor, N., Harrison, R., Lawton, R., Gardner, P., & Conner, M. (2016). Meta-analysis of the reasoned action approach (RAA) to understanding health behaviors. *Annals of Behavioral Medicine, 50*, 592-612. doi:10.1007/s12160-016-9798-4

McIntosh, C. N., Edwards, J. R., & Antonakis, J. (2014). Reflections on partial least squares path modeling. *Organizational Research Methods, 17*, 210-251. doi:10.1177/1094428114529165

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems, 108*, 57-68. doi:10.1016/j.dss.2018.02.007

Mertler, C. A., & Reinhart, R. V. (2016). *Advanced and multivariate statistical methods: Practical application and interpretation* (6th ed.). Los Angeles, CA: Routledge.

Mishra, D., Akman, I., & Mishra, A. (2014). Theory of reasoned action application for green information technology acceptance. *Computers in Human Behavior, 36*, 29-40. doi:10.1016/j.chb.2014.03.030

Mital, M., Chang, V., Choudhary, P., Papa, A., & Pani, A. K. (2018). Adoption of internet of things in india: A test of competing models using a structured equation modeling approach. *Technological Forecasting and Social Change, 36*, 339-346. doi:10.1016/j.techfore.2017.03.001

Niranjan, S., Spulick, S. R., & Savitskie, K. (2018). Mediating and moderating influencers of firm performance: Supply chain managers perspective. *Journal of Enterprise Information Management, 31*, 38-63. doi:10.1108/JEIM-08-2016-0141

Olavsrud, T. (2017, August 31). *How to measure cybersecurity effectiveness before it's too late*. Computerworld Hong Kong. Retrieved from https://www.cio.com/article/3221426/how-to-measure-cybersecurity-effectiveness-before-it-s-too-late.html

Ostherr, K., Borodina, S., Bracken, R. C., Lotterman, C., Storer, E., & Williams, B. (2017). Trust and privacy in the context of user-generated health data. *Big Data & Society, 4*(1), 2053951717704673.

Owens, B. (2016). Stronger rules needed for medical device cybersecurity. *The Lancet, 387*, 1364-1370. doi:10.1016/S0140-6736(16)30120-9

Qualtrics. (2019). Factors impacting the adoption of CMMS. Retrieved from https://www.qualtrics.com

Rantos, K., Fysarakis, K., & Manifavas, C. (2012). How effective is your security awareness rogram? an evaluation methodology. *Information Security Journal: A Global Perspective, 21*, 328-345.

Rastegari, A., & Mobin, M. (2016). Maintenance decision making, supported by computerized maintenance management system. *Reliability and Maintainability, 19*(1), 1-8. doi:10.1109/RAMS.2016.7448086

Rezaei, R., & Ghofranfarid, M. (2018). Rural households' renewable energy usage intention in iran: Extending the unified theory of acceptance and use of technology. *Renewable Energy, 122*, 382-391. doi:10.1016/j.renene.2018.02.011

Ricardo, A., Moriguchi, S. N., & Andrade, D. F. (2016). Intention of adoption of mobile payment: An analysis in the light of the unified theory of acceptance and use of technology (utaut). *Rai, 13*, 221-230. doi:10.1016/j.rai.2016.06.003

Roumen, F. J. (2015). Industry-sponsored research: How to eliminate bias? *European Journal of Contraception & Reproductive Health Care, 20*, 155-157. doi:10.3109/13625187.2015.1046254

Sabi, H. M., Uzoka, F. E., Langmia, K., & Njeh, F. N. (2016). Conceptualizing a model for adoption of cloud computing in education. *International Journal of Information Management, 36*, 183-191. doi:10.1016/j.ijinfomgt.2015.11.010

Sarstedt, M., Ringle, C. M., Smith, D., Reams, R., & Hair, J. F. (2014). Partial least squares structural equation modeling (PLS-SEM): A useful tool for family business researchers. *Journal of Family Business Strategy, 5*, 105-115. doi:doi.org/10.1016/j.jfbs.2014.01.002

Schindler, C. P. (2006). Discussion Report. *European Business Organization Law Review*, *7*, 131-134. doi:10.1017/s1566752906001315

Sharma, S. B., & Tewari, P. C. (2019). A general framework of computerized maintenance management system for an automobile industry. *International Research Journal of Engineering and Technology, 6*, 2087-2092.

Sher, M., Talley, P. C., Yang, C., & Kuo, K. (2017). Compliance with electronic medical records privacy policy: An empirical investigation of hospital information technology staff. *The Journal of Health Care Organization, Provision, and Financing, 54*(12), 1-11. doi:10.1177/0046958017711759

Singhry, H. B., Rahman, A. A., & Imm, N. S. (2016). Effect of advanced manufacturing technology, concurrent engineering of product design, and supply chain performance of manufacturing companies. *The International Journal of Advanced Manufacturing Technology, 86*, 663-669. doi:10.1007/s00170-015-8219-3

Sittig, D. F., Belmont, E., & Singh, H. (2018). Improving the safety of health information technology requires shared responsibility: It is time we all step up. *Healthcare, 6*, 7-12. doi:10.1016/j.hjdsi.2017.06.004

Sullivan, K. M. (2009). But doctor, I still have both feet! remedial problems faced by victims of medical identity theft. *American Journal of Law & Medicine, 35*, 651-685. doi: 10.1177/009885880903500406

Taherdoost, H. (2018). A review of technology acceptance and adoption models and theories. *Procedia Manufacturing, 22*, 960-967. doi:10.1016/j.promfg.2018.03.137

Tang, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: A case study. *Information Technology and Management, 17*, 179-186. doi:10.1007/s10799-015-0252-2

Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. (1990). *The processes of technological innovation. issues in organization and management series*. Lexington, MA*: Lexington Books*.

Tractinsky, N. (2018). The usability construct: A dead end? *Human–Computer Interaction, 33*, 131-177. doi:10.1080/07370024.2017.1298038

Van Hoof, W., Meesters, K., Dossche, L., Christiaens, D., De Bruyne, P., & Walle, J. V. (2018). Ethical considerations of researchers conducting pediatric clinical drug trials: A qualitative survey in two belgian university children's hospitals. *European Journal of Pediatrics, 177*, 1003-1008. doi:10.1007/s00431-018-3151-9

van Staa, T., Goldacre, B., Buchan, I., & Smeeth, L. (2016). Big health data: The need to earn public trust. *BMJ: British Medical Journal (Online), 354*, 3636-3639. doi:10.1136/bmj.i3636

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*, 425–478. doi:10.2307/30036540

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly, 36*, 157-178. doi:10.2307/41410412

Vydiswaran, V. G. V., Zhai, C., Roth, D., & Pirolli, P. (2015). Overcoming bias to learn about controversial topics. *Journal of the Association for Information Science & Technology, 66*, 1655-1672. doi:10.1002/asi.23274

Wan, S., Li, D., Gao, J., Roy, R., & Tong, Y. (2017). Process and knowledge management in a collaborative maintenance planning system for high value machine tools. *Computers in Industry, 84*, 14-24. doi:10.1016/j.compind.2016.11.002

Wang, X., & Goh, D. H. (2017). Video game acceptance: A meta-analysis of the extended technology acceptance model. *Cyberpsychology, Behavior, and Social Networking, 20*, 662-671. doi:10.1089/cyber.2017.0086

Wilkin, C. L., Couchman, P. K., Sohal, A., & Zutshi, A. (2016). Exploring differences between smaller and large organizations' corporate governance of information technology. *International Journal of Accounting Information Systems, 22*, 6-25. doi:10.1016/j.accinf.2016.07.002

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Medical Devices (Auckland, N.Z.), 8*, 305-400. doi:10.2147/MDER.S50048

Yang, R., Qu, D., Qian, Y., Dai, Y., & Zhu, S. (2019). An online log template extraction method based on hierarchical clustering. EURASIP Journal on Wireless Communications and Networking, *19*(1), 1-12. doi: 10.5220/0006941001690181

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. *Information Technology & People, 26*, 401–419. doi: 10.1108/ITP-12-2012-0147

Young, J., Park, S., & Lim, E. (2018). Factors influencing preservice teachers' intention to use technology: TPACK, teacher self-efficacy, and technology acceptance model. *Journal of Educational Technology & Society, 21*, 48-59. Retrieved from https://www.jstor.org/stable/26458506

Yuan, S., Fernando, A., & Klonoff, D. C. (2018). Standards for medical device cybersecurity in 2018. *Journal of Diabetes Science and Technology, 12*, 743-746. doi:10.1177/1932296818763634