

8-3-2021

Information Security Maturity Model for Healthcare Organizations in the United States

Bridget Joan Barnes Page
Portland State University

Follow this and additional works at: https://pdxscholar.library.pdx.edu/open_access_etds



Part of the [Information Security Commons](#)

Let us know how access to this document benefits you.

Recommended Citation

Barnes Page, Bridget Joan, "Information Security Maturity Model for Healthcare Organizations in the United States" (2021). *Dissertations and Theses*. Paper 5758.
<https://doi.org/10.15760/etd.7629>

This Dissertation is brought to you for free and open access. It has been accepted for inclusion in Dissertations and Theses by an authorized administrator of PDXScholar. Please contact us if we can make this document more accessible: pdxscholar@pdx.edu.

Information Security Maturity Model for Healthcare Organizations in the United
States

by

Bridget Joan Barnes Page

A dissertation submitted in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy
in
Technology Management

Dissertation Committee:
Tugrul Daim, Chair
Timothy Anderson
William Hersh
Andrew Tolmach

Portland State University
2021

© 2021 Bridget Joan Barnes Page



This work is licensed under a Creative Commons Attribution-Non Commercial 4.0

International License

ABSTRACT

This research provides a maturity model for information security for healthcare organizations in the United States. Healthcare organizations are faced with increasing threats to the security of their information systems. The maturity model identifies specific performance metrics, with relative importance measures, that can be used to enhance information security at healthcare organizations allowing them to focus scarce resources on mitigating the most important information security threat vectors. This generalizable, hierarchical decision model uses both qualitative and quantitative metrics based on objective goals. This model may be used as a baseline by which to measure individual organizational performance, to measure performance against other organizations, or to monitor changes in the information security environment over time.

Information security incidents cause significant harm, both financial and reputational, to individuals and organizations across the globe. The cybersecurity threat is pervasive and continues to grow at an alarming rate. This harm is heightened in healthcare organizations because human lives may also be at risk in the event of an information security incident. Healthcare organizations have also become a popular target with cybercriminals due to the rich trove of personal information entrusted to them. Existing information system security frameworks are complicated, difficult and time intensive to administer and monitor, and rarely provide relative importance of key performance metrics. Understanding the most important levers in

improving information security by introducing a generalizable model can help close a gap in the existing literature.

Using a comprehensive literature review, objectives, goals, and outputs were identified and linked together in a four-level hierarchical decision model (HDM). At level 1, the purpose of the HDM is to determine the degree to which the organization meets the mission of providing a secure information security environment by evaluating a broad set of metrics. Level 2 specifies five objectives, based on industry- and domain-relevant research, for the promotion of a secure information security environment. Level 3 identifies twenty-two goals with associated measurable outputs, characterized by desirability functions, to create level 4. A structured model is developed using these linked concepts with the help of subject matter experts to validate the content and construct of the model. The model is further tested by measuring for inconsistency and disagreement.

Using case studies, actual industry data are used to demonstrate how the model calculates a score to create a performance measure for each case study organization. Results are discussed to illustrate how the case study sites might increase their performance in future assessments against the model.

This research project contributes to the field by introducing a generalizable model and measurement system that compares information security performance in healthcare organization to an ideal state. Healthcare organizations provide critical resources to millions every day and must remain operational despite information

security threats. Understanding where healthcare organizations can best direct their limited resources to support stability of their information systems is essential to leaders of these organizations.

DEDICATION

I would like to dedicate this work to my family:

To Scott, who encourages and supports me toward being my best;

To my daughters Kyle, Kelly and Adrienne were consistently supportive through the very long process to complete this work.

ACKNOWLEDGMENTS

I would like to begin by acknowledging my PhD advisor and committee chair Dr. Tugrul Daim. Without Dr. Daim's steady hand, and persistent nudging, this work would not have been completed. His consistent guidance and support encouraged me and provided the confidence I needed to find my way through to execution of work that taught me much and that I hope will be of value to others. His dedication to the field and to his students is unwavering and I am grateful for having had the privilege of working with him.

I also want to express gratitude for the support of my committee members, Dr. Timothy Anderson, Dr. William Hersh, and Dr. Andrew Tolmach. Each one shared their valuable time and insights through the completion of my dissertation and I am thankful for their sharing and sacrifice.

This research would not have been possible without the contribution of time, knowledge and insight of industry experts. I appreciate the community of support that has been developed by the College of Healthcare Information Management Executives (CHIME) as well as my colleagues in the Healthcare Information and Management Systems Society. Members of these two professional organizations willingly shared critical support and information which informed this research.

I'd like to acknowledge and thank the Engineering and Technology Management (ETM) department and students. This group has always felt like a family

to me. Welcoming, encouraging, providing un-paralleled support. I am grateful to have known so many helpful and nurturing souls during my time with ETM.

Finally, I'd like to acknowledge the unwavering support of my family. My husband Scott and my three daughters Kyle, Kelly and Adrienne. They have been patient and supportive beyond measure and I am honored to be their "Dr. Mama".

TABLE OF CONTENTS

ABSTRACT	<i>i</i>
DEDICATION	<i>iv</i>
ACKNOWLEDGMENTS	<i>v</i>
LIST OF TABLES	<i>xv</i>
LIST OF FIGURES	<i>xvi</i>
CHAPTER 1: INTRODUCTION	<i>1</i>
CHAPTER 2: LITERATURE REVIEW	<i>6</i>
2.1 Information Security Incidents and Breaches	<i>7</i>
2.2 Information Security Environment and Compliance	<i>11</i>
2.2.1 Technical Controls	<i>12</i>
2.2.2 Management process controls.....	<i>13</i>
2.2.3 Training	<i>17</i>
2.2.4 Governance.....	<i>21</i>
2.3 Assessing Information Security Environment in Healthcare	<i>23</i>
2.4 Information security models and metrics	<i>26</i>
2.5 Maturity Models in Healthcare and the Benefits of Certification	<i>39</i>
2.6 Findings, Recommendations and Gaps in Literature	<i>42</i>
CHAPTER 3: RESEARCH APPROACH	<i>44</i>

3.1	Research Problem	44
3.2	Research Scope and Objectives	45
3.3	Multi Criteria Decision Problem	47
3.4	Expert Judgement	60
3.4.1	Validation	61
3.4.2	Selecting Experts	62
3.4.3	Inconsistency in Expert Judgements	64
3.4.4	Disagreement Among Experts.....	68
3.5	Research Approach	71
3.5.1	HDM as a framework.....	72
3.5.2	Delphi	75
3.5.3	Desirability Curves.....	76
3.5.4	Sensitivity Analysis	76
3.5.5	Challenges and Mitigation Strategy	77
3.5.6	Limitations of Hierarchical Decision Model (HDM) with Delphi	77
3.5.7	Identification of Information Security Experts for Panels.....	79
3.5.8	Data collection and analysis approach	85
CHAPTER 4: HDM DEVELOPMENT		88
4.1	Objectives	88
4.1.1	Organizational support for information security	89
4.1.2	Information security policies and standards.....	89
4.1.3	Information security awareness and training	90
4.1.4	Information security technical hygiene.....	90

4.1.5	Mitigation of external threats	91
4.2	Goals and Outputs	91
4.2.1	Organization Support - Governance.....	92
4.2.2	Organization Support - Leadership and management	92
4.2.3	Organizational Support - Resource availability	93
4.2.4	Organizational Support - Risk assessment, risk management, disaster recovery and incidence response.....	94
4.2.5	Policies and Standards - Policy documentation and awareness	95
4.2.6	Policies and Standards - Procedure documentation and awareness.....	95
4.2.7	Policies and Standards - Technical standard documentation and awareness.....	96
4.2.8	Policies and Standards - Sanction documentation and awareness	97
4.2.9	Awareness and Training - Communications.....	97
4.2.10	Awareness and Training - Awareness events	98
4.2.11	Awareness and Training - Information portal.....	98
4.2.12	Awareness and Training - Training	99
4.2.13	Awareness and Training - Behavioral and real-time teaching.....	100
4.2.14	Technical Hygiene - Physical controls	100
4.2.15	Technical Hygiene - Asset management.....	101
4.2.16	Technical Hygiene - Routine security updates.....	101
4.2.17	Technical Hygiene - Protection of stored information and information in transit	102
4.2.18	Technical Hygiene - Identity, authentication, access management and monitoring.	102
4.2.19	External Threats - Data loss prevention	103
4.2.20	External Threats - Anti-spam and malware protection	103

4.2.21	External Threats - Intrusion detection and prevention	104
4.2.22	External Threats - Protection of network	105
4.3	Metrics	105
4.4	Desirability Curve Development	106
4.4.1	Desirability Curves Associated with Governance	108
4.4.2	Desirability Curves Associated with Leadership and Management Support	108
4.4.3	Desirability Curves Associated with Resource Availability	109
4.4.4	Desirability Curves Associated with Risk Assessment, Risk Management, Disaster Recovery and Incidence Response	110
4.4.5	Desirability Curves Associated with Policy Documentation and Awareness	111
4.4.6	Desirability Curves Associated with Procedure Documentation and Awareness	112
4.4.7	Desirability Curves Associated with Technical Standards Documentation and Awareness	113
4.4.8	Desirability Curves Associated with Sanction Documentation and Awareness ...	114
4.4.9	Desirability Curves Associated with Communications	115
4.4.10	Desirability Curves Associated with Awareness Events	116
4.4.11	Desirability Curves Associated with Information Portal	116
4.4.12	Desirability Curves Associated with Training	117
4.4.13	Desirability Curves Associated with Behavioral Testing and Real-time Teaching	118
4.4.14	Desirability Curves Associated with Physical Controls	118
4.4.15	Desirability Curves Associated with Asset Management	119
4.4.16	Desirability Curves Associated with Routine Security Updates	120
4.4.17	Desirability Curves Associated with Protection of Stored Information and Information in Transit	121

4.4.18	Desirability Curves Associated with Identity, Authentication, and Access Management and Monitoring	122
4.4.19	Desirability Curves Associated with Data Loss Prevention.....	123
4.4.20	Desirability Curves Associated with Anti-spam and Malware Protection.....	123
4.4.21	Desirability Curves Associated with Intrusion Detection and Prevention.....	124
4.4.22	Desirability Curves Associated with Protection of Network.....	125
CHAPTER 5: FINALIZING THE MODEL.....		126
5.1	Model Validation	126
5.2	Quantification of model	127
5.3	Inconsistency.....	127
5.4	Disagreement Analysis	129
5.5	Finalized HDM	129
CHAPTER 6: CASE STUDIES.....		131
6.1	Healthcare organization selection.....	132
6.1.1	Critical Access Hospital (CAH)	134
6.1.2	Stand-alone community hospital	134
6.1.3	Integrated Delivery Network (IDN)	134
6.1.4	Large health system	135
6.1.5	Academic medical center	135
6.2	Illustration case: Stand-alone community hospital (SACH).....	135
6.2.1	Maturity assessment score	136
6.2.1	Strengths and Opportunities for Improvement	137

6.3	Comparative Analysis Across All Case Study Sites.....	140
6.4	Sensitivity Analysis.....	143
CHAPTER 7: DISCUSSION		147
7.1	Research and Practical Implications.....	148
7.1.1	Top Rated Criteria – Intrusion Detection and Prevention	149
7.1.2	Top Rated Criteria – Protection of Network	150
7.1.3	Top Rated Criteria – Identity, Authentication, and Access Management and Monitoring.....	150
7.1.4	Top Rated Criteria – Anti-spam and Malware Protection.....	151
7.1.5	Top Rated Criteria – Behavioral Testing and Real-time Teaching.....	152
7.2	Generalizability.....	153
7.3	Feedback from Experts and Other Considerations	155
CHAPTER 8: CONCLUSIONS		158
8.1	Conclusions and Contributions	158
8.2	Risks and Limitations	162
8.3	Future Research.....	164
REFERENCES		167
APPENDICES		205
Appendix A: Research Instruments		205
	Appendix A-1: Invitation Letter	205

Appendix A-2: Consent Form	206
Appendix A-3: Example of web based validation instrument	209
Appendix A-4: Web based judgment quantification instrument	210
Appendix A-5: Table of research instruments	211
Appendix B: Expert Panels.....	212
Appendix B-1: Expert Panel Configuration	212
Appendix B-2: Expert Background	213
Appendix B-3: Expert Panel Assignments	214
Appendix C: Validation Data.....	215
Appendix C-1: Validation Data at Level 2 (Objective).....	215
Appendix C-2: Validation Data for Level 3 (Goals)	216
Appendix D: Quantification Data Collection Instrument and Data	220
Appendix D-1: Quantification of Level 2 (Objectives)*	220
Appendix D-2: Quantification of Level 3 (Goals) *	221
Appendix D-2-1: Organizational Support Goal *	221
Appendix D-2-2: Policies & Standards Goal *	222
Appendix D-2-3: Training & Awareness Goal *	223
Appendix D-2-4: Technical Hygiene Goal *	224
Appendix D-2-5: Mitigation of External Threats Goal*	225
Appendix D-3: Quantification Data Entry and Analysis Tool	226
Appendix E: Desirability Curves Data Collection Tool & Data	227
Appendix E-1: Desirability Curve Data Collection Instrument (limited sample for technical hygiene)	227
Appendix E-2: Desirability Curve Definition and Values.....	230

Appendix F: Case Study Data	241
Appendix G: Sensitivity Scenario Data	251
Appendix H: Acronyms.....	254

LIST OF TABLES

Table 1: Comparison of Information Security Standards	31
Table 2. Comparison of Maturity Model Levels	32
Table 3: Information Security Models Identified in Literature Outside of Standard Models	34
Table 4: SMART Metrics	38
Table 5: Advantages and Limitations of Predominant MCDA Methods	55
Table 6: Summary of Expert Panel Application to Model	61
Table 7: Summary of Key Demographics for Case Study Sites	134
Table 8: Maturity Assessment Score for Stand-alone Community Hospital	137
Table 9: Strengths and Opportunities for Stand-alone Community Hospital.....	138
Table 10: Maturity Scores for Case Study Sites.....	141
Table 11: Key Maturity Scores for Case Study Sites.....	142
Table 12: Reallocated Model Weights for Scenario Analysis	145
Table 13: Summary Results of Scenario Analysis for Stand-alone Community Hospital.....	146
Table 14: Model Elements by Weight	149
Table 15: Addressing Research Gaps	161
Table 16: Addressing Research Questions.....	162

LIST OF FIGURES

Figure 1: Literature Review Areas	7
Figure 2: Total reported losses by year in U.S. dollars as reported to U.S. Federal Bureau of Investigation’s Internet Crime Complaint Center	8
Figure 3: Healthcare Data Breaches of 500 or More Records.....	23
Figure 4: Average total cost of a data breach by industry for 2020 in US\$ millions..	24
Figure 5: Standard Risk Assessment Process	33
Figure 6: Standard Risk Assessment Process	35
Figure 7: HIMSS Analytics US EMR Adoption Model	40
Figure 8 : Research Gaps, Goals, Questions.....	46
Figure 9: Idealized Multi Criteria Decision Analysis Process.....	48
Figure 10: Structured Research Process.....	71
Figure 11: Generalized Hierarchical Decision Model	74
Figure 12: Expert Functions	85
Figure 13: Desirability Curve for Governance Goal.....	108
Figure 14: Desirability Curve for Leadership and Management Support Goal	109
Figure 15: Desirability Curve for Resource Availability Goal.....	110
Figure 16: Desirability Curve for Risk Assessment, Risk Management, Disaster Recovery and Incidence Response Goal	111
Figure 17: Desirability Curve for Policy Documentation and Awareness Goal	112
Figure 18: Desirability Curve for Procedure Documentation and Awareness Goal	113
Figure 19: Desirability Curve for Technical Standards Documentation and Awareness Goal.....	114
Figure 20: Desirability Curve for Sanction Documentation and Awareness Goal .	115
Figure 21: Desirability Curve for Communication Goal.....	115
Figure 22: Desirability Curve for Awareness Events Goal.....	116
Figure 23: Desirability Curve for Information Portal Goal.....	117
Figure 24: Desirability Curve for Training Goal	117
Figure 25: Desirability Curve for Behavioral Testing and Real-time Teaching	118
Figure 26: Desirability Curve for Physical Controls Goal.....	119

Figure 27: Desirability Curve for Asset Management Goal	119
Figure 28: Desirability Curve for Routine Security Updates Goal	120
Figure 29: Desirability Curve for Protection of Stored Information and Information in Transit Goal.....	121
Figure 30: Desirability Curve for Identity, Authentication, and Access Management and Monitoring Goal.....	122
Figure 31: Desirability Curve for Data Loss Prevention Goal.....	123
Figure 32: Desirability Curve for Anti-spam and Malware Protection Goal	124
Figure 33: Desirability Curve for Intrusion Detection and Prevention Goal.....	125
Figure 34: Desirability Curve for Protection of Network Goal	125
Figure 35: Validated HDM	127
Figure 36: Inconsistent expert data.....	128
Figure 37: Generalizable model for healthcare information security maturity	130

CHAPTER 1: INTRODUCTION

The healthcare sector has increased implementation of information systems dramatically since the advent of the American Recovery and Reinvestment Act (ARRA) of 2009. Formerly a laggard in the utilization of technology to support enhanced efficiencies and improved business operations [1], ARRA [2] enabled the Centers for Medicare and Medicaid Services (CMS) to provide financial incentives for the effective use of health information technology (HIT), and beginning in 2015, financial penalties for not implementing HIT that demonstrated “meaningful use” [3]. Largely as a result of this law, HIT has become ubiquitous in the United States.

The proliferation of HIT has also created a new and significant risk to health organizations; protecting the privacy and integrity of large caches of protected health information (PHI). The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires healthcare organizations, known as “covered entities,” to ensure the protection of individual identifiable information [4][5]. The Department of Health and Human Services’ Office for Civil Rights (OCR) serves to monitor compliance of covered entities with the provisions of HIPAA. In recent years the OCR has dramatically increased their compliance monitoring and auditing of covered entities. This increased monitoring and auditing has led to a significant increase in both the

number and cost of fines to covered entities. The U.S. Department of HHS OCR web site reporting breach activity [6] has become known as the “wall of shame.”

Settlement fees paid to the OCR totaling nearly \$20 million for PHI violations were reported in 2016 alone [7]. These settlement fees are a small portion of the expense associated with ensuring security of protected health information. Organizations can easily invest millions more in securing their information systems and, of course, there can be significant reputational harm incurred when a breach of protected health information occurs. For example, Oregon Health & Science University paid a one-time settlement fee of \$2.7M in 2016 for a breach that occurred in 2013[8]. As a result of their resolution agreement and three-year corrective action plan with the OCR they invested an additional \$8M per year in information security initiatives for the duration of the corrective action plan. This same level of investment was required to maintain security operations after the corrective action plan was resolved.

As a result of the increased risk factor for information security in a world with large collections of protected health information being created, stored, and transmitted, many healthcare organizations are making additional efforts to improve their information security risk profile. Healthcare organizations, especially those of smaller size, struggle to understand the best use of their limited resources to address this issue. There are many well established cybersecurity frameworks to draw upon

for guidance - NIST, HITRUST, CIS Critical Security Controls to name a few [9]. These frameworks can be unwieldy and most fail to provide guidance on which cybersecurity strategies provide the most value. While there is increasing literature examining the problem of the cybersecurity threat in healthcare, there are few examples of program evaluation through quantitative methods based on elements identified in traditional cybersecurity frameworks or qualitative case-based methods.

This study examines the literature to explore the current state of the information security environment at healthcare organizations. It provides value by creating a measurement system that incorporates both qualitative and quantitative metrics. A generalizable model is created and validated by subject matter experts which produces a score to evaluate overall performance in cybersecurity for healthcare organization. Through a criterion-based validation process, experts agree the model may also be used to understand the relative importance of individual metrics to aid organizations in understanding which cybersecurity strategies may provide the most value in increasing overall performance. Subject matter experts agree that the model accurately reflects performance results and case studies confirm this assessment.

Including this introduction, the paper is organized into 8 chapters. Chapter 2 reviews the academic literature on information security in healthcare organizations. Cybersecurity breach and incident types and rates are discussed. Cybersecurity

mitigation strategies are identified, as are cybersecurity frameworks. Research gaps are noted, highlighting the need for a maturity evaluation model.

Chapter 3 further clarifies the problem and provides information about the approach that is taken to provide structure to model development. Many multi-criteria decision-making methods are reviewed and the decision to utilize the Hierarchical Decision Model (HDM) is discussed. Due to the reliance on subject matter experts for validation of the model, important elements of working with experts such as formation of research instrument and identification of experts are discussed.

Chapter 4 describes how the hierarchical decision model was developed. Initiated by a literature review, and then modified through a validation process involving subject matter experts. The validated four-level model links objectives, goals and outputs. At level 1, the purpose of the HDM is identified as development of a healthcare information security maturity model. Level 2 specifies five objectives: organizational support, policies and standards, awareness and training, information security technical hygiene, and mitigation of external threats. Twenty-two goals populate level 3 with measurable outputs characterized by desirability curves to fill level 4 of the model.

Chapter 5 discusses how the generalizable model was finalized. Subject matter experts first quantified the criteria through a series of pairwise comparisons, resulting in a weighting of each criterion within the model. Key analysis was

performed to check for individual expert inconsistency followed by an assessment for disagreement among experts. The finalized generalizable model is presented.

Chapter 6 describes how the model is used to demonstrate information security maturity within healthcare organizations. The results are validated by subject matter experts. The model is used to calculate performance in case studies at a variety of healthcare organization types. Scores and metric values are analyzed to provide recommendations to a select case study site.

Chapter 7 reviews the results of the model development as related to the problem statement are discussed as well as practical implications of findings. In addition, the generalizability of the model is analyzed. Expert feedback responses during the model validation process support concerns identified in literature regarding severity of threat and need for prioritization of cybersecurity strategies given limited resources. Subject matter experts were in agreement of the validity of the model.

Chapter 8 summarizes and concludes the discussion, notes contributions to the field as well as limitations of the study. Future research opportunities are also noted.

CHAPTER 2: LITERATURE REVIEW

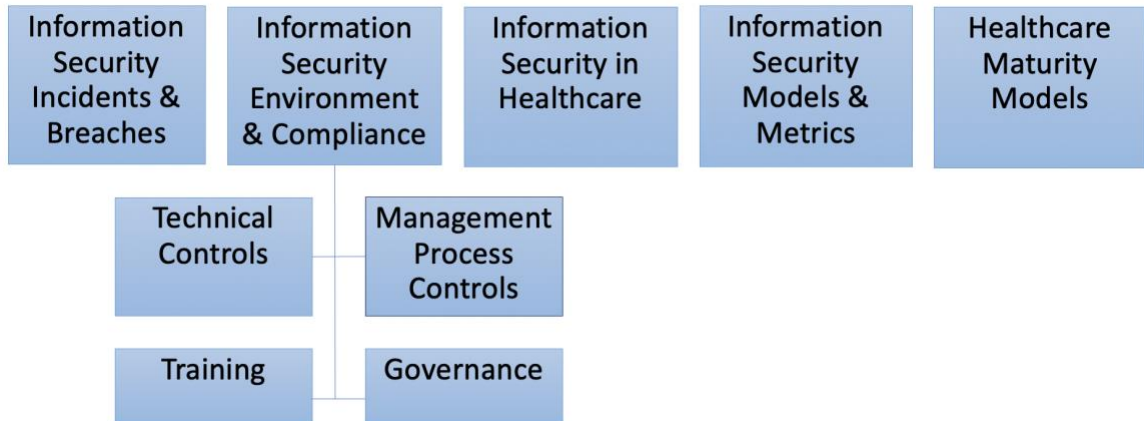
A comprehensive review of information security within healthcare organizations was conducted. The body of literature reviewed was selected through a variety of methods. First, literature searches using EBSCO, PubMed/Medline, Elsevier, and Science Direct were conducted using key words Information Security, Data Breach, Healthcare, PHI, Training, and Organization Culture. These searches were joined in several instances to narrow the results as a means of identifying the most relevant literature. When an article cited a particularly significant prior work, that referenced article was also studied. Search was primarily conducted on articles from 2007 to present, but several articles dating as far as 2000 were utilized as relevant as well as one article from 1982. Over 200 relevant articles are cited.

The rest of this chapter contains six sections. Section 2.1 identifies information security incidents and breaches, highlighting the impact of unsecured information. Section 2.2 reviews information security environments and practices, noting the practices generally employed to improve the security of information; taking a deeper dive into governance, training, management process controls and technical controls utilized to improve information security. Section 2.3 delves into the information security environment in healthcare organizations specifically. Section 2.4 focuses on existing information security models, frameworks and metrics. Section 2.5 focuses on maturity models in healthcare and the benefits of certification.

Finally, Section 2.6 concludes the discussion by summarizing the findings and presenting the research gaps.

Figure 1 provides a visual representation of the areas considered in this literature review.

Figure 1: Literature Review Areas



2.1 Information Security Incidents and Breaches

Information security incidents and breaches have grown exponentially in recent years and have made headlines across the globe. These threats affect all types of organizations large and small, across all industries and across geographic boundaries. During the 2013 Christmas shopping season, a cyberattack on Target Corporation’s retail store netted millions of customer’s credit card information [10]. In the United Kingdom, a government-sponsored survey found that 87% of small businesses had detected and reported cyberattacks [11]. In June of 2015, The United States Office of Personnel Management discovered that the background records for current, former and prospective Federal employees had been stolen, including the

records of over 21 million individuals [12]. In June of 2021 FBI Director Christopher Wray compared ransomware challenge to 9/11 [13]. This is a mere sampling of the incidents that have hit the press in recent years. This sample serves to illustrate the significant risk and vulnerability posed by cybercriminals. Of further note, healthcare is persistently ranked as the number one target of cybercriminals, followed by education, government, retail, financial sectors in varying orders, due to the richness of the data available in the healthcare sector [14][15][16].

The reported volume of financial damage caused by cybercrime has grown dramatically across all industries. Figure 2 below provides details of this loss as reported to the Federal Bureau of Investigation’s Internet Crime Complaint Center [17].

Figure 2: Total reported losses by year in U.S. dollars as reported to U.S. Federal Bureau of Investigation’s Internet Crime Complaint Center



Several key factors have driven this growth. First, there are many more systems at organizations, large and small, that store information, than there have ever been before. Second, some of the information stored in this proliferation of information systems is highly valuable and as a result the number of cybercriminals, and networks of cybercriminals has grown substantially [18]. Third, managing the security controls required to protect the information stored electronically is expensive, rapidly changing [19], and complex [20]. As a result, many organizations across most industry sectors have not, or are simply unable to, establish a strong information security environment [21]. Culbertson notes that the volume of threats to healthcare organizations is steadily growing, and that mitigating risk to an acceptable level will be a massive undertaking [22]. When looking specifically at healthcare organizations it should be noted that patient health records contain all the information a thief needs to perpetrate identify theft [23]. Agrawal claims that continuous data breaches targeting these invaluable medical records have become a nemesis for healthcare organizations [24]. Finally, according to HIMSS Analytics over 80 percent of the security breaches in the healthcare sector since the enactment of HIPAA trace back to people within the organization [25][26]. Human behavior and simple mistakes, regardless of industry, are a large factor in data loss [27].

Information security risks are presented to organizations through multiple vectors – system transmission paths, hardware, software, or the internet for example. Cybercriminals utilize a variety of nefarious tools to gain access to sensitive data,

systems, or people (e.g., phishing, malware, zero day exploits, denial of service attacks, SQL injections, ransomware, man-in-the-middle attacks) [11][28]. This collection of vectors and approaches is rapidly changing and is difficult for most organizations to remain responsive to.

Healthcare organizations need to be mindful not only of patient privacy concerns but also of the negative business impacts such as billing theft, identity theft or interruption of critical business functions posed by cybercriminals. The negative impact of breaches in healthcare organizations is extreme. Not only are these events costly, routinely reaching beyond seven-figure price tags, but the reputational harm can be difficult to recover from. Most importantly, some information security incidents could prohibit the healthcare organizations from providing critical patient care activities. In May 2017, the WannaCry ransomware incident not only shutdown transportation systems and other governmental systems across the globe, but also forced Britain's public health systems to turn away patients even though no patient data was compromised [29]. These incidents not only have the potential of causing financial loss to individuals and organizations, but also pose a very real threat to healthcare organizations in serving their critical mission of treating patients. Clinicians rely on electronic medical records, infusion pumps, and many other tools in order to provide the current standard of care [30]. In September of 2020, the first patient death attributed to cybercriminals occurred when a woman did not survive a

transfer between healthcare facilities that had been necessitated as a result of a cyberattack at Düsseldorf University Hospital [31].

2.2 Information Security Environment and Compliance

The environment of the organization in support of information security has tremendous importance in the effectiveness of information security compliance. While there are a number of definitions for organizational culture/environment, the definition provided by Deal (1982) has often been cited as particularly relevant in the evaluation of information security environments. This specific definition identifies the follow key characteristics: 1) shared values, which define the expected behavior in the workplace; 2) heroes who have earned distinction by living the organizational values; 3) rituals and ceremonies, which are physical expressions of the organizational culture/environment; and 4) the cultural social network within the organization, which perpetuates the culture/environment and guards against deviations [32]. Creating an environment where information resources are protected is a necessary component of a successful information security strategy. The characteristics identified by Deal are readily mapped to the key criteria of effective information security programs as noted below:

- Technical controls (reinforcing shared values and rituals);
- Management process controls (reinforcing shared values, rituals, cultural network);
- Training; (reinforcing shared values, heroes, cultural network) and

- Governance programs (reinforcing shared values, heroes, cultural network).

These criteria are described in greater detail below.

2.2.1 Technical Controls

Technical controls are hardware or software solutions that provide automated protection from unauthorized access and misuse of systems and related institutional data. The number and variety of technical controls is vast. Some may be used to mitigate the threat of access to protected data by provisioning and monitoring who has access to information across the enterprise (e.g., access/identity management and control), others prohibit certain types of information from leaving the organization through unauthorized channels (e.g., data loss prevention). Many healthcare organizations deploy data loss prevention (DLP) tools in order to ensure that protected health information (e.g., medical record number, diagnosis, social security number) does not leave the organization unless they are sent through a secure channel. Other technical control technologies may protect data at rest (e.g., encryption technologies). For example, many institutions both within and outside of healthcare, have implemented mobile device management (MDM) solutions to ensure that only cell phones, or other mobile devices, that are encrypted access their secure networks and that any data on those devices is encrypted and therefore very difficult, if not impossible, to access. Still other technical controls help to facilitate detection and diversion of external threats (e.g., firewalls, anti-virus software). Organizations

are more likely to implement technical controls than they are to provide financial support for other information security risk mitigation strategies (e.g., training) [33].

In many organizations, information security has largely been considered a technology issue [34]. However, despite the technology-based measures that are generally implemented, there is often little improvement in information security compliance behavior [23] and as a result information security remains a problem. Organizations tend to design information security solutions by defining a strong technical perimeter and keeping intruders out [35]. For best results, technology controls must be combined with human solutions in order to create a strong environment and defense for information security [36][37]. Technical controls are never one hundred percent effective in eliminating information security threats.

2.2.2 Management process controls

Management process controls for information security consist primarily of policies and sanctions designed to guide, and where appropriate, modify user behavior.

Policies in support of information security cover a broad range of topics from appropriate use of computing resources within an organization to specific guidelines regarding supported equipment and applications. Policies often fall short of meeting organizational objectives if they are not married with procedure level documentation to support the “how” of policy compliance or execution. For example, information security best practices would support a security review of all new applications or

hardware that was to be introduced to an organization, and many organizations have policies requiring such security reviews. If this policy was not matched with clear instructions (procedure level documentation) regarding how an individual would go about obtaining such a security review it is likely that employees within the given entity would not comply with the policy. Some regulatory agencies have been known to issue fines and/or sanctions (e.g., temporary loss of accreditation) when an organization has a policy that is not followed by members of the organization. It is essential that policies are combined with procedures to aid in compliance. Maintenance of the large volumes of policies required to provide guidance at complex healthcare organizations can be overwhelming, and many organizations are unable to commit the resources required to regularly update their policies and procedures as frequently as necessary to ensure they remain relevant in the dynamic environment of information technology and healthcare regulations. When policies do not maintain relevancy, or are not properly vetted within the organization, they lose their efficacy and may even cause greater confusion, thereby increasing the threat of unintended information security breaches or policy violations.

Sanctions are the documented consequences of failure to comply with organizational policies. Sanctions are generally aligned with the intent associated with non-compliant behavior. For example, a policy violation may be accidental or inadvertent, due to carelessness or negligent behavior, intentional but without harmful intent, or intentional with harmful intent. In the event of an inadvertent or

careless mistake it is likely that the appropriate sanction for violation could be a “letter of discipline or warning” delivered to the individual who was non-compliant. In the event of a more purposeful or ill-intended policy violation, termination of employment status could be called for. It is important that sanctions be applied appropriately in order to provide proper incentives to employees to drive compliant behavior. Organizational members must believe “the punishment fits the crime” so to say. It is equally important that there be no perception of preferential status in application of sanctions. For example, in a healthcare setting a physician must be subject to the same applications of sanctions as the nursing staff. Failure to apply sanctions consistently and fairly would result in an ineffective and potentially harmful compliance tool.

When used properly, policies, procedures and sanctions become a powerful aid to drive an environment of information security compliance. Creating a strong environment around information security is crucial as users are the largest source of breaches despite technical controls [38]. The Online Trust Alliance stated in 2014 that 29 percent of data breaches were a result of employee actions, either accidental or intentional [39]. Further, in many organizations end users are viewed as the “weakest link” in information security management [27][40], creating an information security gap. In many healthcare organizations, there is minimal awareness of the information security threat, and as a result, staff pose a significant threat to information security [41].

User perception of information security is often a barrier in creating a strong environment of information security compliance. Many users are concerned that the task overhead imposed by complying with information security measures is burdensome and therefore see these measures as a threat. Users often view information security measures as work stressors, privacy invasions, constraining and inconvenient. They feel compelled to maintain their operational performance while including information security tasks in their daily work [42][43][44]. Employee compliance behavior is critical to ensuring the information resources of the organization are protected [18][38].

Information security is as much about managing people as it is about managing technologies [45][46][47] and access control and authentication systems must be simple and easy to use or users will bypass them [48]. It must be recognized that there is a tradeoff between usability and information system requirements, and this balance must be actively managed [49] if information security systems are to be successful. Combining technical controls with human controls provides a strong framework for improving and maintaining an environment that values high levels of information security. Information security environments influence security compliance, security effectiveness, security awareness, and most importantly, security behavior [50][51][52][53]. People controls combined with technical controls lead to an improved information security environment and a strong information security program is critical to creating a strong information security

environment[51][54]. Information security is not merely the responsibility of information technology (IT) teams, it is the responsibility of everyone at the organization [55]. Even though there is agreement that technological and managerial (people) process are both required to be successful, there is a general lack of a well-developed techno-managerial structure in healthcare [56]. Organizations that have employees with a higher propensity for compliance beliefs, as well as a high level of executive engagement, and enforcement, are more likely to have a high level of information assurance compliance [56][57][58]. It is noted that user attitudes toward compliance are affected when they consider compliance-related consequences [59]. Management controls govern the behavior of people and become stronger over time. In addition, they become the information security solution with the highest value [60] over time as they are cheaper to implement and maintain than technical solutions [61].

2.2.3 Training

Policy and sanctions alone are not sufficient and organizations need to employ other means such as training to ensure individuals internalize information security policies and best practices [62]. Training about information security has become a cornerstone of creating an environment that supports information security [63]. The creation of an information security environment by educating users about information security risks and their responsibilities is essential [64]. As individual's understanding and awareness of information security increases, compliance

improves remarkably [65]. Karjalainen and Siponen [63] describe effective training as being made up of three components: (a) provide elementary characteristics of information security; (b) explain how these characteristics support the information security training; and (c) create models on how to evaluate training.

Some of the elementary characteristics of information security which users must be aware of are the need for data integrity, authentication and confidentiality requirements. Data integrity, simply put, is trust in the information that is being presented to users in the conduct of their daily tasks. That information, or data, must be not only trusted as a valid source of record, but also be consistently available when access is needed. Authentication and confidentiality are also key components in information security, ensuring that only those individuals who should have access to data are provided that access. These elementary characteristics are the “what” component of the training – as in “what is it that we want to talk about?”

The next key component of effective training programs is the “how.” Providing employees with information about specifically how their actions can improve information security within the organization is essential. For example, a common threat vector to information system integrity and confidentiality is phishing. Phishing is the action of sending an email, either broadly to all potential victims within an organization or specifically targeting high-profile/high access individuals (spear-phishing) within an organization. Phishers design their emails with the intent of getting their intended victims to either download a malicious file to their computing

devices or to otherwise provide their personal information or credentials to them. They do this by masquerading as trusted conveyers of the request for information (e.g., institutional information technology department, financial institutions). While there are some technical tools that can minimize the volume of phishing emails, there will certainly be some phishing emails that get past those technical controls. When that happens, it is critical that individual users know what characteristics are common of phishing emails so that they do not become victims of phishers. Organizations must therefore train their employees to mitigate this risk which can negatively impact both the organization as well the individual user.

Training programs should be multi-dimensional in order to be successful. Individuals have different learning styles, and effective training programs respect and cater to those differences. Multiple delivery channels and venues are needed. Computer-based training is an effective tool for many and it provides fairly reliable mechanisms for tracking training comprehension, through testing embedded within the training, as well as tracking of training at the individual level across the organization (i.e., who has completed the training and who has not). However, computer-based training is not always the best training for increasing a deep level of understanding or for evoking understanding at an emotional level. Many individuals are more likely to understand the content being delivered if they are able to do so in interactive ways such as in-person training or group-based training.

There is some evidence that greater success in information security awareness can be found with small group training workshops and discussion activities as opposed to more standard top-down messaging or large presentations with no opportunities for interaction [65][66][67]. Further, positive motivators may be more effective in attaining information security compliance than stringent enforcement [23]. In addition, positive peer influence on compliance [44], security values and attitudes of the users are re-informed by the consistent behavior of senior management and their peers toward these security values [68]. It's possible that these peer attitudes would become more pronounced in the small group environment. For these reasons, and many others, a diverse and multi-dimensional training program is key to success.

Training and education will be more effective if it outlines not only what is expected of individuals and how to prevent information security breaches, but also provides an understanding of why it is important, thereby influencing attitude [69][70][71][37]. Without the knowledge of why information security is important introducing stringent information security measures could be perceived and attributed to a lack of trust toward the users which could significantly increase internal user information system abuse [72]. Conveying information about the impacts of breach of patient's medical records or other personal information about employees or affiliates of the organization is required. Employees must understand the reputational damage that can be inflicted on the institution, as well as the ways

that criminals may use the information to cause harm, both reputational and financial, to individuals. Security practices should be supported by an organizational environment that not only improves security awareness but also enhances the individuals' motivation to act responsibly and in accordance with policies [73][74].

Finally, the success of information security training programs must be measured as a key component of the overall success of information security compliance. Due to the complicated nature of combining technology solutions and human management solutions as the framework of an effective overarching information security program, isolating the success of training program alone may be a challenge. Certainly, competency-based testing is one avenue of measuring knowledge gained and therefore the success of training programs. However, measuring employee performance in the conduct of practicing effective information security is quite another. The overall interest in measurement of information security training has increased significantly in recent years, although no definitive model for doing so has yet been identified.

2.2.4 Governance

The National Institute of Standards and Technology (NIST) defines information security governance as the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of

responsibility, all in an effort to manage risk [75]. Typically information security governance programs have the following foundational criteria: 1) governing the ongoing operations of the organization's information security technology framework; 2) governing the conduct of employees in ensuring compliance with information security policies and procedures; 3) ensuring adequate funding is available for the execution of information security programs; 4) ensuring compliance requirements are met, often through monitoring by outside or unrelated organizational entities; and 5) protecting organizational reputation.

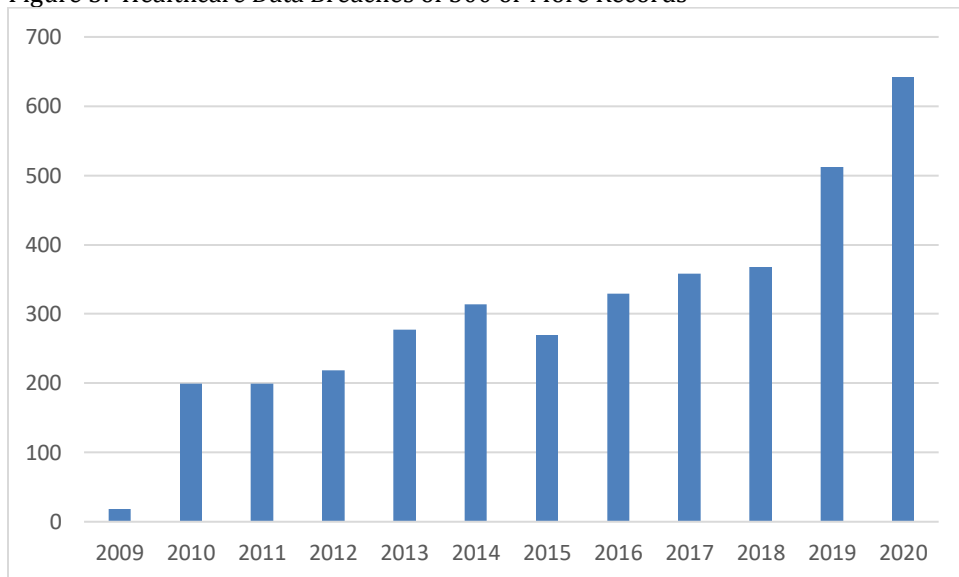
Most information security governance programs obtain feedback and report results across multiple levels within the organization. Given the large reputational and financial damage that can be wrought by poor information security management practices it is important that the highest levels within the organization are informed of the risks and mitigation programs related to information security. Equally important is a "boots on the ground" understanding of the business impact of decisions related to implementation of information security solutions. The technologists must understand workflows within the enterprise well enough to deliver solutions that will not severely hamper the ability for individuals to conduct their daily tasks in the interest of improving information security. In addition, information security best practices suggest a separation of duties between the owners of the technology solution operations and the auditing of performance against information security standards. As such, these two specific functions often follow

distinct reporting channels within an organization. For example, information security engineering might sit within the information technology department, while information security auditing might sit within the compliance or legal department of a given organization. These multi-level and multi-channel approaches are key criteria of successful information security governance programs.

2.3 Assessing Information Security Environment in Healthcare

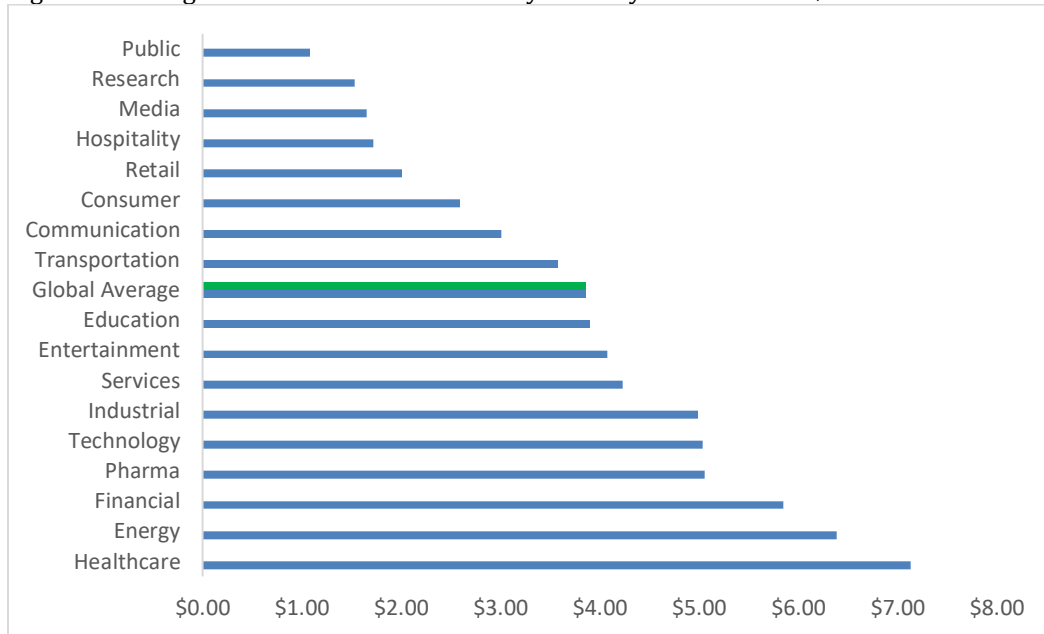
There has been significant research documenting the volume of breach activity and likely threat vectors. Figure 3 below illustrates the increase in volume of healthcare breaches of more than 500 records from 2009 to 2020 as reported to the HHS Office for Civil Rights [76]. In 2020 those breaches resulted in over 268,189,693 records being inappropriately disclosed [76].

Figure 3: Healthcare Data Breaches of 500 or More Records



In addition, there is a fair amount of research on which specific industries are being impacted by breaches and the cost associated with those breaches. Figure 4 [77] below illustrates the average total cost of a data breach by industry for 2020 in U.S. dollars. The average cost of a healthcare breach is \$7.13M, higher than the average total cost of a data breach in any other sector, and nearly double the global average cost regardless of industry. The research cited below in Figure 4 excluded very small and very large breaches, capturing only those that ranged in size between 3,400 and 99,730 compromised records and included costs associated with detection and escalation, notification, post data breach response and lost business.

Figure 4: Average total cost of a data breach by industry for 2020 in US\$ millions.



This cost data, when combined with information about the number of healthcare breaches noted in Figure 3 exceeds an annual cost above \$4.5B and this

number underestimated the total cost as it excludes the cost of very small and very large breaches.

Clearly the threat is rising, especially in the healthcare sector, and the cost of breaches is disproportionately high for healthcare organizations. The problem is well documented, but more research is needed in identifying solutions to better manage the risk. There is little research addressing the promotion of compliance behaviors within organizations [23] and more research is required in the health profession to understand motivating behaviors for adoption of an information security environment [78].

An understanding of organizational environment related to information security compliance can significantly aid in the execution of a successful information security program. The following measures have been identified as being helpful in assessing information security environments: security awareness, security ownership, top management support and influence, information policy enforcement and security training [79]. There appear to be mixed findings in the research related to environments of information security awareness and compliance in healthcare systems. Alumaran, Bella and Chen found that human behavior toward protection of medical information is one of the main threats to information security; and that the current environment in healthcare falls short in protecting health information due to "values and norms" toward information security [80]. However, Hasib [81] and Brady [50] surveyed leaders at healthcare organizations in the United States and

Canada and found fairly high levels of confidence in a high level of information security compliance and environment. This dichotomy of opinion serves as the context for further inquiry into the question of how to measure information security compliance effectiveness and attitudes, and further the impact of organizational environment in shaping the adoption of a strong information security practices. Organizations that recognize the value of committing resources, and enhancing capabilities and cultural value in the face of organizational issues can enhance their performance [82].

2.4 Information security models and metrics

In order to prepare for, and respond to, information security threats models, also known as cybersecurity frameworks, have been developed and refined over the years in order to identify information security best practices. Information security models and metrics were recognized on the Hard Problem List of the United States INFOSEC Research Council in 2005, a situation confirmed by the United States National Science and Technology Council in 2011 and further supported as one of the five hard problems in Science and Security in 2015 [83]. The next few pages explore existing models and associated metrics and suggests how those models could be used as a foundation for creation of an information security maturity model for healthcare organizations in the United States.

2.4.1 Information Security Models

Information security's key objective is the protection of Confidentiality, Integrity and Availability of data, often referred to as the CIA triad, without impinging on organizational productivity [84]. In order to best serve this objective in a systematic way, the development of information security models and metrics began in the 1980s and has continued to evolve since that time. The Information Security and Control Association (ISACA) has defined the following key outcomes for information security governance [85].

- Strategic Alignment – Security requirement defined by the business enterprise.
- Value Delivery – Baseline security following best practices.
- Risk Management – Delivering to agreed-upon risk profile.
- Performance Management – A defined set of metrics that are consistently measured.

There are numerous information security models currently in use with similar but not identical desired outcomes documented and similar, but not identical, methodologies proposed. There are a great number of models that assess information security risk. Some of these models are qualitative in nature and others are more quantitative [86][87]. A few have become standards, however there is no definitive maturity model that could be used for reference benchmarking [88][89][90].

Maturity models are instruments that define an evolutionary path to increasingly meeting the defined objective. General maturity models have been widely used in information systems research [91]. Maturity models have also been used in the healthcare domain specifically in the information system sector [92][93][94]. In the case of information security, the defined objective would be defined as an environment that has robust controls to mitigate information security risk as aligned with organizational business objectives. Models must be simple enough that organizations of all sizes can measure their maturity as well as develop action plans to improve maturity levels. This is a significant challenge with existing models. Listed below is a brief description of the most prevalent information security models that are considered standards.

Information Security and Control Association (ISACA) COBIT 5 for Information Security [95] – The Information Security and Control Association (ISACA), an international association of professionals focused on information technology governance, developed the Control Objectives for Information and Related Technologies (COBIT) in 1996. The original model was largely focused on governance and processes associated with technology delivery. In 2012 ISACA released an add-on for COBIT 5 specifically related to information security. The model is high level and is largely audit and compliance focused with an accreditation process available.

International Organization for Standardization (ISO) 27000 series (also known as ISO/IEC) [96] – The International Organization for Standardization (ISO) is a consortium of national standards institutes across more than 150 countries. ISO has developed an information security framework and associated code of practice documentation in their 27000 series. ISO's 27000 series was first published in 2005 and was based on the United Kingdom Government's Department of Trade and Industry standard for information security, referred to as BS 7799. Most recently updated in 2014, it can be viewed as an overall program that combines risk management, security management, governance and compliance. The standard is largely compliance focused and has an associated certification process available.

National Institute of Standards and Technology (NIST) 800 series including CyberSecurity Framework [97]– The National Institute of Standards and Technology is a non-regulatory federal agency within the United States Department of Commerce. NIST has developed information security standards and guidelines to increase the planning, implementation and management of information security. NIST's 800 series was first published in 2002 and the most recent cybersecurity framework document was published for feedback in 2017. Developed to support private sector organizations, it does not offer a certification program but rather is a self-assessment tool.

Operationally Critical Threat, Asset, and Vulnerability Assessment (OCTAVE) [98]– created by the Software Engineering Institute (SEI) at Carnegie

Mellon University for the United States Department of Defense, OCTAVE was first published in 1999. OCTAVE is primarily a high-level risk assessment methodology designed for organizations with more than 300 employees. The focus of OCTAVE is on identifying threats and vulnerability and then developing strategies to mitigate those threats. OCTAVE does not offer a certification process and is free to use.

Health Information Trust Alliance (HITRUST) CyberSecurity Framework (CSF) [99]- The Health Information Trust Alliance is a not-for-profit collaborative of healthcare, technology and information security leaders in the United States. In 2009 HITRUST developed the Common Security Framework in an attempt to harmonize the multiple existing standards and respond to regulatory requirements associated with healthcare organizations. HITRUST is compliance focused and available free of charge, although the certification process is fee-based.

Each of these models were developed to meet specific objectives [86]. While most of the models have common themes their specific objectives, steps, structure and level of application vary considerably. Table 1 below provides a summary of the risk phases/processes, and framework components of each model noted above.

Table 1: Comparison of Information Security Standards

Model	Risk Model Phases/Process	Framework Components	Categories in Framework	Sub-categories in Framework
COBIT [95]	<ol style="list-style-type: none"> 1. Align, Plan, Organize 2. Build, Acquire, Implement 3. Monitor, Evaluate, Access 	<ol style="list-style-type: none"> 1. Principles 2. Policies 3. Procedures 4. Requirements & Documents 	7	N/A
ISO 27001 [96]	<ol style="list-style-type: none"> 1. Define Methodology 2. Identify Assets 3. Identify Threats & Vulnerabilities 4. Qualify Risk 5. Mitigate Risk 6. Document Risk Report 7. Review, Monitor, Audit 	N/A	18	124
NIST 800 series [97]	<ol style="list-style-type: none"> 1. System Characterization 2. Threat Identification 3. Vulnerability Identification 4. Control Analysis 5. Likelihood Determination 6. Impact Analysis 7. Risk Determination 8. Control Recommendations 9. Results Documentation 	<ol style="list-style-type: none"> 1. Identify 2. Protect 3. Detect 4. Respond 5. Recover 	22	108
OCTAVE 5 for Info Sec [98]	<ol style="list-style-type: none"> 1. Establish Drivers of Risk 2. Profile Assets 3. Identify Threats 4. Identify and Mitigate Risks 	N/A	10	N/A
HITRUST [99]	<ol style="list-style-type: none"> 1. Prioritize and Scope 2. Orient 3. Create a Target Profile 4. Conduct a Risk Assessment 5. Create a Current Profile 6. Perform Gap Analysis 7. Implement Action Plan 	N/A	14	47

As illustrated in Table 1 above, the variety and depth of the models covers a broad spectrum, from light-weight to very detailed. This variety is also apparent in the approach each of the standard models uses when considering definitions of maturity as illustrated in Table 2 below.

Table 2. Comparison of Maturity Model Levels

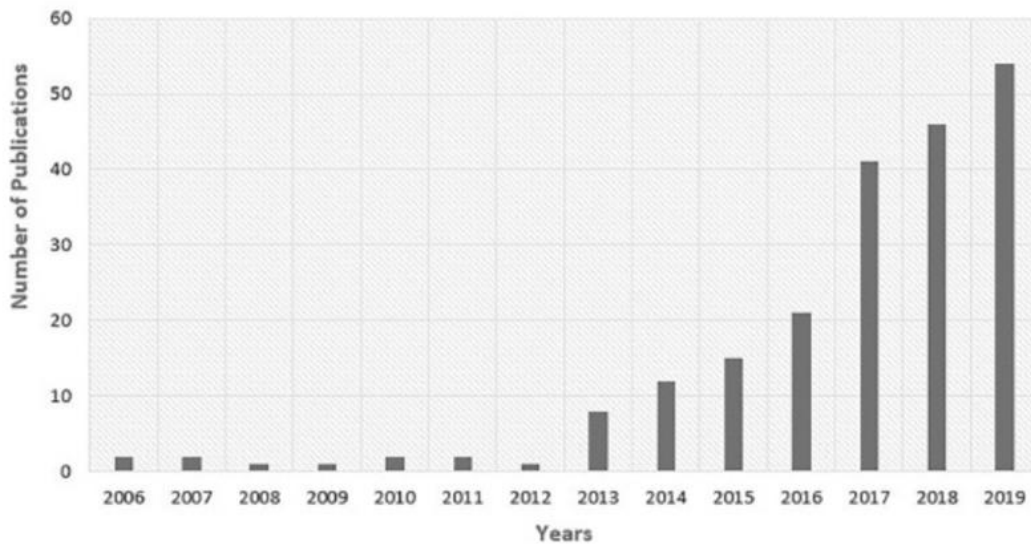
Model	Maturity Levels
COBIT Model [95]	<ol style="list-style-type: none"> 1. Non-existent 1. Initial/ad hoc 2. Repeatable but intuitive 3. Defined process 4. Managed and measurable 5. Optimized
ISO 27001 [96]	Not documented
NIST 800 * [97]	<ol style="list-style-type: none"> 1. Partial 2. Risk Informed 3. Repeatable 4. Adaptive
OCTAVE [98]	Not documented
HITRUST CSF 2009 [99]	<ol style="list-style-type: none"> 1. Basic 2. Aspirational 3. Developing 4. Integrated

* Identifies tiers but also explicitly states “does not necessarily represent maturity level” [97]

NIST [97] notes that “organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances.” This interest in flexibility is common in the models described above; however, the lack of consistency of approach, evaluation and measurement across the models creates confusion among information security practitioners and leaves the industry as a

whole searching to fill the gaps left by each respective model and without a common nomenclature or benchmarks. As a result, there has been significant independent research on model variants or completely new models developed in the past several years. Figure [5100] below provides a snapshot of the increase in systemic review of cyber-resilience assessment frameworks from 2006 through 2019.

Figure 5: Standard Risk Assessment Process



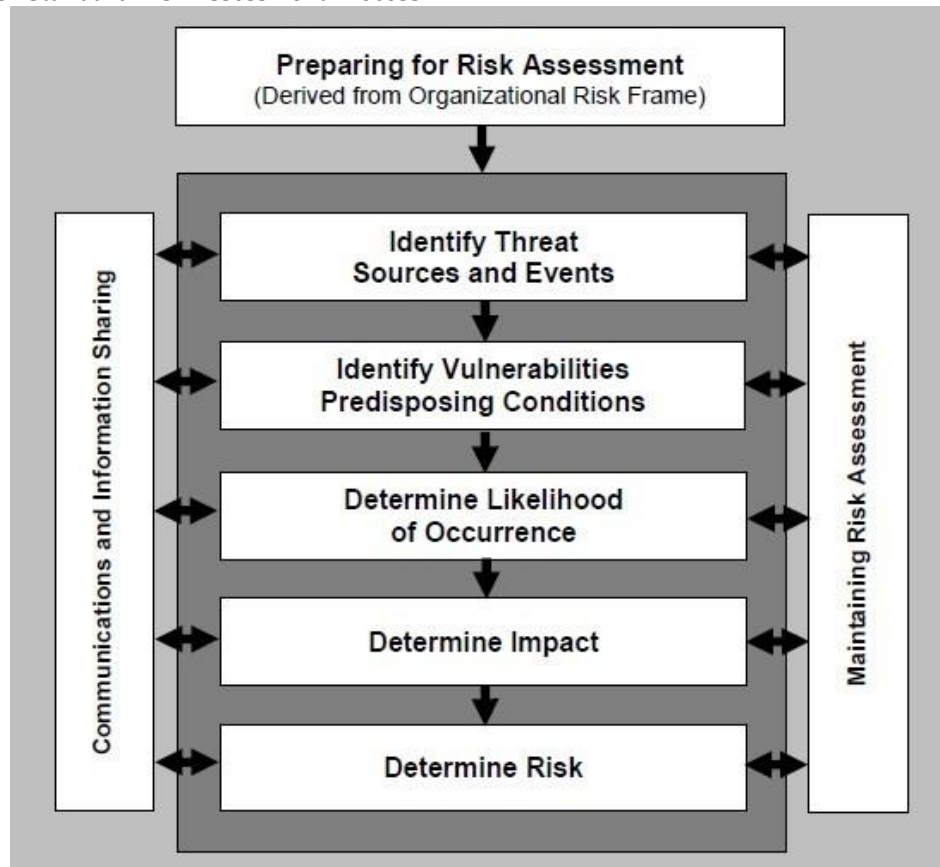
This increase in development of new models, despite existing standards is largely driven by two key factors. First, increased utilization of technology has heightened the visibility and importance of information security. Second, frustration with existing models due to their gaps and complexity has driven individuals to create new models that better suit their specific needs. Table 3 below provides a summary of information security models that were identified in the literature outside of the standards noted above.

Table 3: Information Security Models Identified in Literature Outside of Standard Models

Model Variants	Authors
Culture Based Changes to Existing Models	Van Niekerk & Von Solms 2010 [101]; Da Veiga & Eloff [102], 2010; Da Veiga & Martins 2015 [65]; Hajny et al., 2021 [103]; Chowdhury et al., 2020 [104]
Financial Based Changes to Existing Models	Bodin & Loeb, 2005 [105]; Nazareth & Choi 2015 [106]; Lui et al., 2020 [107]; Gordon, Loeb, Zhou 2020 [108]; Lee 2021 [109]
Creating Software Based Solution	Solic, Ocevci & Golub, 2015 [110]; Zaki et al., 2021 [111], Gourisetti et al., 2020 [112]
Combining/Consolidating Existing Models	Shamala, Alfantookh & Yusoff 2013 [88]; Vorster & Labuschagne 2005 [113]; Pavleska, et al., 2020 [114]; Benz & Chatterjee, 2020 [115]
Entirely New Models	Karabacak & Sogukpinar 2005 [116]; Feng & Li 2011 [117]; Henriques De Gusamao 2016 [118]; Maglaras et al., 2020 [119], Rea-Guaman, et al., 2020 [120]

Existing models, while somewhat divergent as illustrated in Table 1, generally follow a risk assessment theme with an approach as noted in Figure 6 [121] below; however, they largely lack the detailed action level objectives for measurement in a prioritized manner.

Figure 6: Standard Risk Assessment Process



The healthcare sector, while recognizing the need for flexibility, is in need of more specific guidance related to information security [99]. Barlette [122] notes that many organizations may be skeptical about information security effectiveness due to the difficulty in evaluating the benefits. In addition, most if not all existing standard models lack any metrics associated with changing information security culture [70] or human behavior [123], which is a significant gap given the prevalence of security incidents associated with human error. Compliance is evolving from a focus on technical controls to one that includes the human element in the context of coherent business practices [124]. Finally, most current models are quite complex,

lack certainty [125][126] and may be difficult for small organizations to utilize [122] due to lack of expertise.

2.4.2 Information Security Metrics

Metrics can be used to provide performance indicators for organizations against some defined goal. They may also be used to compare and differentiate performance across different organizations. Effective utilization of metrics can help organizations in measuring and monitoring their performance outcomes.

Information security metrics should tell organizations how well they are doing in keeping institutions safe from harm, how they can improve their security posture, and how they compare with others in the field when it comes to information security. According to Brotby [127] contemporary metrics largely fail in this regard. Most information security metrics are focused on technical controls [86][128] and say little about overall security. While technology is important, it is far from the only element that is necessary in providing an environment with high levels of information security [20][129]. Due to the confidential nature of information security, very few organizations are willing to share information about their information security profile with others [129], making comparison of standards and maturity exceedingly challenging.

Metrics are more than a list of things to be counted or boxes to be checked off. In the case of information security, they should be used to tell a story about performance of people, technology, and processes. Security metrics strive to provide

a quantitative and objective basis for security assurance [126]. Their main uses fall into the following broad categories:

- Strategic planning – assessment to support decision making and program planning.
- Quality Assurance – product development lifecycle and vulnerability management.
- Tactical Oversight – monitoring for compliance and improvement opportunities.

It is critical that organizations define specific objectives if they are to create meaningful metrics. Nearly all current models measure risk components as “red”, “yellow”, and “green”. They often do this by assessing each risk element against two key factors – probability of event occurring and impact of event should it occur. While this bucketing of risks and measurement provides flexibility for organizations, it does not always provide quantitative, specific and actionable information. Healthcare organizations specifically have difficulty prioritizing the work that may be required to remediate risks [124]. As noted by Black [130] one problem with the current metrics is that they lack specificity of definition. For example, if the information security metric is defined as “percentage of systems patched” would that mean only operating system patches or would it include service and application patches? NIST notes that the concepts of fundamental units, scales, and uncertainty measures that are prevalent in scientific metrics have not

been applied to information technology [126]. Difficulty in measurement is a common challenge in information security metrics which makes benchmarking challenging as well. Another common problem with existing model metrics is the accuracy of qualitative measures. In many instances, especially those involving metrics related to information security culture [102][131][105] self-evaluation surveys are employed for measurement over time. Such surveys often produce inaccurate or skewed results, depending on the nature of questions asked [130].

Good metrics are SMART – Specific, Measurable/Manageable, Actionable, Relevant, and Timely/Trending as illustrated in Table 4 [132][133]below.

Table 4: SMART Metrics

Specific	Clearly define target and area of measurement.
Measurable/Manageable	Data can be obtained consistently and efficiently.
Actionable	Provides information that is easy to understand and provides direction about improvement opportunity.
Relevant	Measurement is related to objective and importance.
Timely/Trending	Can be compared over time.

SMART metrics are lacking in current models for information security. Black [130] notes that current models provide many suggestions for the types of metrics that should be collected for information security but no definitive list has been created. NIST has provided very good templates for defining metrics and

documenting measurement, however they have only provided a few examples of what these measures and metrics might be [121]. Further, little work has been done to determine the value of the metrics in operational environments [134] nor have specific measures been defined for the metrics that have been suggested.

2.5 Maturity Models in Healthcare and the Benefits of Certification

Lacking consistent and effective maturity models for information security, we look to maturity models that have been developed in healthcare for other purposes. The HIMSS Electronic Medical Record Adoption Model (EMRAM) is such a model. HIMSS EMRAM was designed to identify the various stages of maturity in the area of Electronic Medical Records (EMR) for hospitals. The maturity model, shown below in Figure 7 [135], consists of 8 stages and provides a recommended adoption model for increasing the maturity of utilization of EMRs.

Figure 7: HIMSS Analytics US EMR Adoption Model

US EMR Adoption Model SM	
Stage	Cumulative Capabilities
Stage 7	Complete EMR; CCD transactions to share data; Data warehousing; Data continuity with ED, ambulatory, OP
Stage 6	Physician documentation (structured templates), full CDSS (variance & compliance), full R-PACS
Stage 5	Closed loop medication administration
Stage 4	CPOE, Clinical Decision Support (clinical protocols)
Stage 3	Nursing/clinical documentation (flow sheets), CDSS (error checking), PACS available outside Radiology
Stage 2	CDR, Controlled Medical Vocabulary, CDS, may have Document Imaging; HIE capable
Stage 1	Ancillaries - Lab, Rad, Pharmacy - All Installed
Stage 0	All Three Ancillaries Not Installed

Beginning with Stage 0, where the EMR alone is installed, to full maturity at Stage 7 which includes characteristics such as Continuity of Care Documents (CCD) readily available. The model offers a certification process that ensures that the next higher level is only reached upon completion of clearly documented measures within each stage.

The model was developed in 2005 and has been refined over time. It, along with government incentives, has driven the market to increase adoption and

optimization of EMRs rapidly. The model has provided a clear path for the logical evolution of EMR adoption, providing not only a roadmap for hospitals of all sizes, but also a means of benchmarking best practices across the country [136]. The model is now used in many countries around the globe and the benefits of this model have been widely reviewed and include increased efficiencies in clinical staff quality performance [137] as well as improved patient safety [138]. There are similar models in support of maturity in healthcare analytics [139], but neither of these are appropriate for measurement of healthcare information security maturity.

Models that offer a certification process, such as ISO, COBIT, and the HIMSS US EMR adoption model noted above, offer numerous benefits to industry and well as independent organizations. The following key benefits of certification have been noted [140][141][142]:

- 87% of respondents stated that ISO 27001 had a “positive” or “very positive” outcome on their information security.
- 82% of those surveyed noted an increase in quality control of information.
- 39% reported a decrease in down-time of IT systems and the same number a decrease in the number of security incidents.
- 78% reported an increased ability to meet compliance requirements.
- 44% reported increased sales or competitive advantage.
- 51% reported increased customer satisfaction.

2.6 Findings, Recommendations and Gaps in Literature

The literature reviewed confirms that information security is a significant risk to healthcare organizations. Further, when organizations understand their information security maturity they are better positioned to ensure protection of confidentiality, integrity and availability of their data, avoiding costly information security incidents which cause both financial and reputational harm.

The role of user motivation and attitude in information security, while recognized, has not been treated seriously [143]. Despite user training, information security compliance remains problematic [144] and more research should be done to explore what types of learning are most effective. Additional research must also be done to determine what instills a strong information security environment in organizations [145][146]. Further, not all groups within an organization will react similarly to the same initiatives for promoting security awareness [147]. Studies which specifically examine the human component of information security are needed [148]. All to these factors distill to a core theme around a necessity for further research in defining the current state of information security environment within organizations and ways in which that environment might be improved.

There is a significant gap in information security models that provide a maturity score, clearly defined metrics, and recommendations that may be used as a roadmap for healthcare organizations. Many authors suggest the need for new information security models that address the gaps of existing models

[142][149][150]. There is a specific need in the industry to provide a maturity model that is easy to understand and provides clear direction regarding prioritization for investment of information security resources. A new model is required that, while not replacing existing models or comprehensive risk assessments, would provide a framework of best practices for healthcare organizations of any size. Such a model could serve as a benchmark for comparing security profiles across the industry.

CHAPTER 3: RESEARCH APPROACH

3.1 Research Problem

Healthcare organizations are faced with increasing challenges in implementing and sustaining high-functioning information security environments. These challenges will continue to increase as regulatory monitoring increases and information security threats persist. Focusing on improving the information security environment within these organizations is likely to help provide protection of protected health information (PHI) and personal information as well as support the continued operations of critical business functions including the very critical mission of providing urgent life-saving care.

Consistent performance evaluation and management leads to increased performance – what is measured matters. Current information security evaluation programs exist, but are complicated, resource intensive, difficult to use and as result are not used [151][152]. The ability to adequately measure information security performance against peers or manage performance over time in a quantitative way is a significant challenge.

Healthcare organizations have limited resources and must be diligent in the execution of funding decisions. Given the growing investment in information security at healthcare organizations, decision support tools that clearly define the tactics that will have the biggest impact on improving performance would allow for objective and transparent decision making. The best decision support tools also provide the ability

to measure performance over time, answering the question “was the promised value achieved?”

An easy to use, generalizable model, that provides a holistic set of metrics with performance scores for information security maturity is much needed.

3.2 Research Scope and Objectives

This study presents a new holistic approach in the evaluation of information security maturity at healthcare organizations. This index can help organizations in developing strategic, practical and effective methods for improved information security behaviors. Once deployed within an organization, a baseline compliance score would be created. The index score could then be used to compare maturity with an ideal, with other organizations, or to monitor progress toward an enhanced maturity of the information security environment over time. Further, it could be used to deepen understanding of the mechanisms that will improve the environment of information security. In this way, organizations may learn not only from the conduct of an individual assessment, but may also have a means of learning from others in similar or diverse organizations, experiencing the same information security challenges.

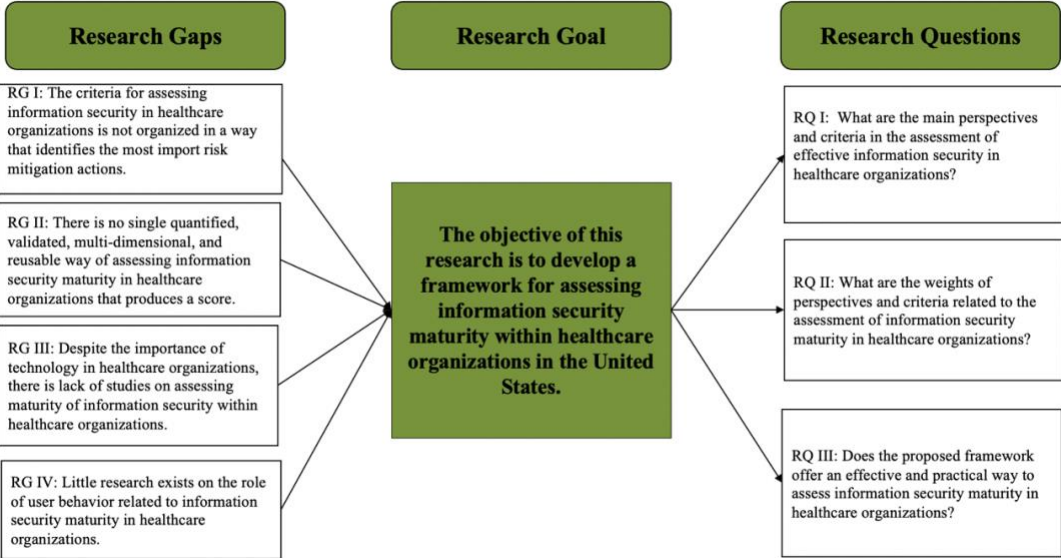
A number of diverse healthcare organizations are used to test and analyze the model’s ability to calculate a valid and appropriate performance evaluation score.

This research has four objectives:

1. Define a set of outputs that create a balanced and comprehensive image for information security maturity;
2. Develop a framework and metrics that gauge performance evaluation related to these outputs;
3. Evaluate performance of a variety of healthcare organizations using this framework;
4. Introduce a new method for healthcare organizations to measure performance, extending the literature.

Figure 8 maps the gaps to research questions that were developed leading to research objectives noted above.

Figure 8: Research Gaps, Goals, Questions

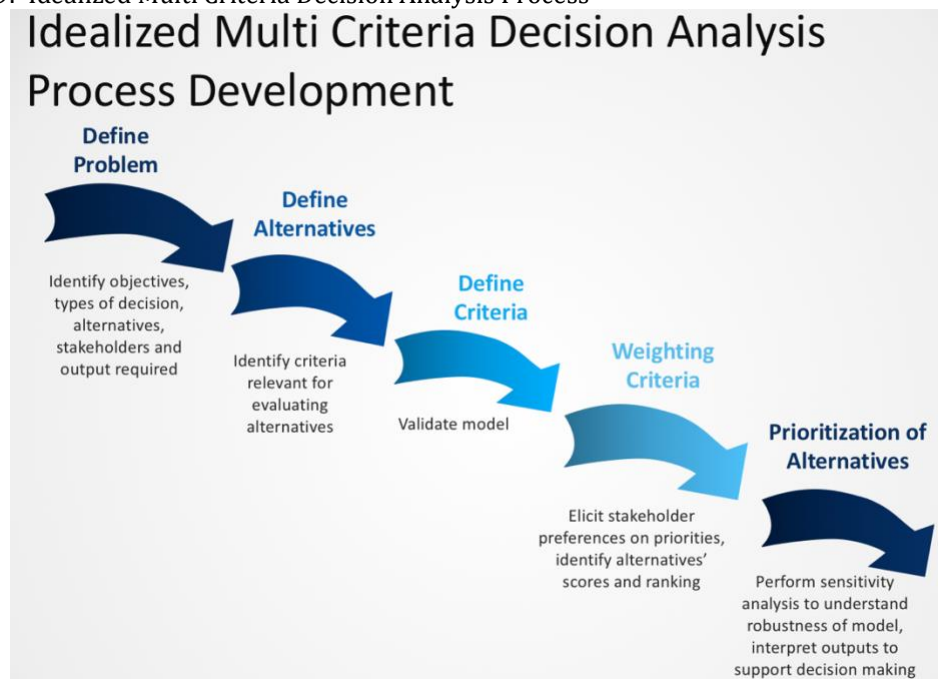


3.3 Multi Criteria Decision Problem

Providing a solution to the complex issue of improving information security in healthcare organizations is clearly a problem that requires a multi criteria approach to decision making. In order to understand the best method for evaluating the maturity level of information security environments, many well documented approaches to multi criteria decision analysis were considered prior to selection of Hierarchical Decision Model (HDM).

Multi Criteria Decision Analysis (MCDA) is often used to analyze complex problems when a single optimal solution does not exist. MCDA is defined as “a set of methods and approaches to aid decision-making, where decisions are based on more than one criterion, which make explicit the impact on the decision of all the criteria applied and the relative importance attached to them” [153]. Often time the criteria may be related to one another and decision making may require trade-offs. The typical process for MCDA begins with definition of the problem at which time the objective and types of decision are identified. Next a number of criteria are defined for the conduct of evaluating alternatives. This is followed by validation and weighting of both the criteria and model itself. The process is concluded with performance of sensitivity analysis and ultimately a prioritization of alternatives. Figure 9 [154][155] below provides a visual representation of this process.

Figure 9: Idealized Multi Criteria Decision Analysis Process



According to Thokala [154], Adunlin [156], and Drake [157] there has been an increase in utilization of MCDA methods in healthcare as it provides a sound and rigorous approach to decision making. There are numerous examples of research that has used MCDA to address healthcare questions [154][156][157][158][159][160] and volumes have been increasing since 2011. As a specific example, Marsh used MCDA as a decision support tool for determining fields of approval, assessment, pricing and utilization of new drugs and medical technologies [161]. In addition MCDA has recently been used to address information security questions [162][163][164][165].

MCDAs Modeling Approaches MCDAs approaches can be broadly classified into value measurement models, outranking models, and goal programming models. Value measurement models require construction and comparison of numerical scores, representing value, to identify the degree to which one decision is preferred over another. The use of individual weighted scores of criteria to create an overall score for each alternative solution is provided. Outranking methods generally involve pairwise comparison of alternative criteria which are then combined to create a rank order set of alternatives. Goal programming entails searching for the alternative that most closely matches minimum levels of performance acceptance [166]. Below the methods in each broad classification are discussed in more detail.

3.3.1 Value measurement methods

Value measurement methods require the construction and comparison of numerical scores (individual and total value) to represent how one alternative is preferred over another [161][167]. The aggregation rule for these models usually uses a weighted sum approach. As shown by Marsh [161] and colleagues [167], value measurement is the most common MCDAs approach. Examples of these methods are described below.

Additive Aggregation - Additive Aggregation is simple linear aggregation and is a common MCDAs approach. In this approach each score on each criterion is multiplied by its weight and then the weighted scores are summed for the overall score of that option and possibly compared with other options [153].

Analytical Hierarchy Process (AHP) – AHP uses expert knowledge to create a hierarchical structure for systematic alternative selection and justification problems. AHP decomposes a difficult MCDA problem into a systematic hierarchy procedure [168] then utilizes experts to prioritize the importance of individual criteria. AHP assumes each criterion evaluated as independent of other criteria. AHP asks experts to use an eigenvector method , where a linear transformation is created stretching the X-Y line chart, during the prioritization process. Decision-makers are usually more comfortable giving interval judgments than absolute value judgments. Using feedback from experts, a matrix is prepared, indicating the relative importance of criteria and alternatives for consideration.

Analytical Network Process (ANP) – ANP is a general form of AHP. The key differentiator between AHP and ANP is that unlike AHP, ANP allows for consideration of interdependence among criteria.

Hierarchical Decision Modeling (HDM) - HDM is a well-known tool that helps provide a framework for quantifying subjective information so that effective qualitative judgements may be made for decision-making purposes [169][170][171]. HDM breaks down complex issues into key components that can be singularly identified and measured at the individual level with respect to criteria across multiple levels of the hierarchy. Components are broken down into pairwise comparisons segments, where industry experts can evaluate their relative preference of one criterion over another as opposed to declaring an absolute preference. The constant

sum approach requires experts to provide a numeric and relative value among options to largely qualitative questions. The researcher can then validate each expert's opinion with other experts, thereby validating the evaluations. The key differentiator between AHP and HDM is that AHP uses the eigenvector method for creating values whereas HDM uses the constant-sum method.

Multi Attribute Utility Theory (MAUT) – MAUT considers additive value for multiple objectives [172] considered “bundles”. AHP and HDM are sometimes considered MAUT methods [173]. The MAUT process considers the perspective of a decision maker through the use of utility functions or desirability curves. One of MAUT's strengths is that it accounts for uncertainty.

Program Budgeting and Marginal Analysis (PBMA) – PBMA is a framework that helps decision-makers to reallocate resources so that benefits are maximized [174]. Developed specifically for healthcare decision analysis, PBMA has eight stages: choose a set of meaningful programs; identify current activity and expenditure in those programs; identify improvements; weigh incremental costs and benefits; prioritize; consult and consider changes; effect the changes; and evaluate progress [174]. The decision maker is providing as much information as possible related to the relative size of gains and losses related to reallocation and divestment of resources. PBMA addresses the issue of allocation efficiency, maximizing the benefits of available resources [175].

3.3.2 Outranking methods

Outranking methods are based on a general concept of dominance using an outranking relationship. Using pairwise comparison to prioritize criteria [154] for the purposes of determining which alternative outranks another in relative importance. Strict dominance, where one criterion is rigidly preferred over another given criterion, is a requirement within these methods. Examples of these methods are described below.

Elimination and Choice Expressing Reality (ELECTRE) – ELECTRE is a method for selecting the best choice, the choice with the greatest advantage and the lowest level of conflict among criteria [176][177][178]. Sometimes known as the French school of decision making, it was originally developed in 1965 by Bernard Roy. Different versions of ELECTRE have been developed over time including ELECTRE I, II, III, IV and TRI. ELECTRE I is intended for problems of selection, ELECTRE II, III, and IV are intended for problems of ranking, and ELECTRE TRI is intended for assignment problems. All methods follow the same basic concepts however they differ according to type of problem and operational execution. ELECTRE requires construction of one or more outranking relationships by first comparing pairs of actions followed by coordination of indices based on information obtained in the first phase. During the process some alternatives are eliminated which don't meet the defined minimum value.

Preference Ranking Organization Method for Enrichment of Evaluations

(PROMETHEE) – PROMETHEE is an outranking method that provides a framework for decision making focused on conflicts and synergies and clusters of specific actions [179]. PROMETHEE uses generalized criteria to facilitate inclusion of uncertainty. According to Hyde [180] PROMETHEE is executed by identification of stakeholders, selection of criteria, formulation of alternatives, weighting the criteria, assessment of the performance of alternatives against the criteria, selection of the generalized criterion function and associated indifference and preference values for each criterion, sensitivity analysis, leading to a final recommendation.

Geometrical Analysis for Interactive Aid (GAIA) – GAIA is an extension of PROMETHEE which provides graphical representation of the problem [181]. GAIA strives to provide decision makers with information about the relationship between criteria and alternatives [182].

3.3.3 Other Methods

Other methods aim to identify the alternative that best meets a predefined level of achievement [183][161]. Using a mathematical formulation of the satisfactory heuristic, a model that may not be optimal but is generally acceptable [158]. The satisfaction model is focused on achieving a defined level of satisfactory performance for each criterion by considering the preference of criteria in their order of importance. The levels represent the ‘goals’, while an algorithm is used to identify the alternatives that satisfy the goals in priority order [184]. These models may be

thought of as an extension of linear programming that handles multiple, and sometimes conflicting measures.

Technique for Order Preference by Similarity to Ideal Solutions (TOPSIS) -

TOPSIS is based on the concept that the chosen alternative should have the shortest geometric distance from the positive ideal solution (PIS) and the longest geometric distance from the negative ideal solution (NIS) [185][186][187]. A series of comparisons of these relative distances provides the preference order for the alternatives. FUZZY TOPSIS method is sometimes used to evaluate the criteria in each region and then all the criteria may be ranked based on the region [188].

3.3.4 Advantages and Limitations of Predominant MCDA Methods

The above listed MCDA methods have been applied widely across many industries and for diverse problems. The Table 5 below illustrates a summary of the most popular methods and their advantages as well as limitations.

Table 5: Advantages and Limitations of Predominant MCDA Methods

Class	Method	Advantages	Limitations
Value Measurement	Analytic hierarchy process (AHP)	<ul style="list-style-type: none"> • Allows for both qualitative and quantitative criteria • Provides ability to express the relative importance of the multiple criteria • Allows the decision maker to focus on the comparison of just two objects, improving consistency in the decision-making process 	<ul style="list-style-type: none"> • Comparison process could be considered cumbersome which may lead to inconsistency in ranking • Additive aggregation is used, as result some important information may not be considered.
	Analytic Network Process(ANP)	<ul style="list-style-type: none"> • Independence among elements is not required • Prediction is accurate because priorities are improved by feedback 	<ul style="list-style-type: none"> • Time consuming • Uncertainty is not supported
	Hierarchical Decision Model (HDM)	<ul style="list-style-type: none"> • Allows for both qualitative and quantitative criteria • Since problem is constructed into a hierarchical structure, the importance of each element becomes clear • Experts do not have to select ultimate preference 	<ul style="list-style-type: none"> • Potential for inconsistency and bias • Comparison process could be considered cumbersome
	Multi-Attribute Utility Theory (MAUT)	<ul style="list-style-type: none"> • Takes uncertainty into account • Incorporates preferences 	<ul style="list-style-type: none"> • Requires large amounts of input • Preferences need to be precise
Outranking	Elimination and Choice Expressing Reality (ELECTRE)	<ul style="list-style-type: none"> • Outranking is used • Takes uncertainty and vagueness into account 	<ul style="list-style-type: none"> • Time consuming Its process and outcome can be difficult to explain in layman's terms • Strengths and weaknesses are not directly identified
	Preference Ranking Organization Method for Enrichment of Evaluations (PROMETHEE)	<ul style="list-style-type: none"> • Easy to use • Criteria do not have to be proportionate 	<ul style="list-style-type: none"> • Does not provide a clear method by which to assign weights
Other	Technique for Order Preferences by Similarity to Ideal Solutions (TOPSIS)	<ul style="list-style-type: none"> • Easy to use • Number of steps remains the same regardless of the number of criteria 	<ul style="list-style-type: none"> • Uses Euclidean Distance so does not consider the correlation of attributes • Difficult to weight and keep consistency of judgment

The table above identifies classification of MCDA methods as derived from Thokala and Duenas [184], Ishizaka and Nemery [189], and Belton and Stewart [190]. Other less popular methods are found in literature related to MCDA. Only predominant methods have been identified in the preceding pages.

Most methods have seen improvement and evolution over time. Utilization of outranking methods, like ELECTRE and PROMETHEE, which were prevalent early on in the development of the MCDA field, have waned as use of value measurement

approaches such as AHP and MAUT have increased. Recently combining different methods has become commonplace in MCDA. The combination of multiple methods addresses deficiencies that may be seen in certain methods [191]. Specific user needs and decision problems must be evaluated to determine which MCDA approach is most appropriate to use [161].

3.3.5 Appropriateness of HDM Combined with Delphi for Research

When considering the appropriateness of HDM for the proposed research the following questions were considered:

- Is the proposed methodology an effective method for assessing the findings in literature related to information security programs in healthcare such that a maturity index could be created?
- Is the proposed methodology appropriate for assessing the multiple criteria that are necessary for development of a mature information security environment?
- Does the proposed methodology allow for criteria with varying levels of importance?
- What level of effort is required to obtain necessary information to build the model and is access to the necessary resources attainable?
- Has the proposed methodology been proven successful in conducting similar research or varied research in the same or similar industries?
- Could the model be used for industries outside of healthcare?

HDM is a way of documenting the framework for analysis of a given system. There are several benefits to using HDM for analysis and decision-making purposes. HDM permits complex issues to be presented to key stakeholders in understandable ways by illustrating relationships among key criteria in a given decision. In the case of HDM, the model allows for an easily understood aggregation of literature reviewed and expert feedback, presented in a quantified manner with the intention of presenting viable options to decision makers.

Strengths of HDM as a research method are as follows:

- Provides a comprehensive abstraction of problem under consideration;
- Illustrates multi-level relationships among elements of model;
- Aggregates the opinions in an easy to digest way for decision makers;
- Structures both qualitative and quantitative data in a single view;
- Allows for variability of value for each criterion within the model;
- Allows experts to express relative preference as opposed to ultimate preference;
- Constant sum model with scoring 0-100 is easily understood by experts;
- Experts can be engaged at a moderate effort level; and
- Proves a reasonable tool for predicting outcomes.

The mixed research methodology combining Hierarchical Decision Modeling (HDM) and Delphi Method is well-suited to the proposed research. Obtaining validated sources of data related to information security is challenging due to both limited prior research in this field as well as the confidential nature of information security work in general. Information security professionals and organizations do not freely discuss their risks and vulnerabilities for fear that those weaknesses will be exploited. Similar challenges have been faced by others in the emerging technology space. Gerd Sri and Kocaoglu applied Delphi method to collect data from industry experts in order to validate strategic information about emerging technologies [192]. The Delphi method is used when basic demographic, economic or historical information is inadequate to conduct desired research [193][194]. Delphi is a way of structuring communication among a group of experts such that they are able to contribute their expertise independent of one another, so as not to be unduly influenced by one another. The key characteristics of Delphi are as follows:

- Anonymity – members of the group are not aware of the specific composition of the group.
- Iteration – members of the group are asked questions in several stages and are often allowed to change their opinions in each stage.
- Group Analysis – at each iteration the group’s responses are measured in aggregate providing information such as mean, median and variability.

Using this blended approach allows for dynamic discussion panels to be used in constructing the original hierarchy and defining criteria as findings of literature review are validated by mutual agreement of experts, followed by Delphi, a means of providing anonymous feedback, which aids in mitigating the potential bias created by strong personalities for actual quantification of the criteria within the HDM. Phan states that “...this process (HDM) makes the experts more comfortable because their decisions are based on the relative preference of one criterion over another rather than an absolute preference” [195]. Further, HDM is an effective method for this specific research in that it allows for both qualitative as well as quantitative data to be incorporated in the model [196]. HDM is effective at illustrating multi-level relationships and posing alternatives in a systematic and quantitative way [197].

HDM has demonstrated success as an appropriate methodology for evaluating multi criteria decisions [195][197][198]. HDM has been used to provide frameworks for solving research questions in strategic planning [197][199][200][201], healthcare [202][203][204][205][206], organizational change [207] and technology fields [208][209][210][211][212][213][214][215][216][217][218]. In a recent and relevant example Phan used HDM to calculate an innovation index for sustainable technology [195].

Given the well-documented success of HDM across industries and problem types, the complex nature of the research problem and the effective mitigation strategies for limitations of the model, HDM is an effective method for application to

the issue of creating a maturity index for information security in healthcare environments.

3.4 Expert Judgement

Utilization of expert panels in creating models for complex decision making, where limited quantitative data is available, is broadly supported in the literature across many industries [154][158][159] and specifically in the healthcare industry [155][219][220].

Experts are individuals who have deep knowledge of a specific skill or area and are not likely to be challenged by others. Fink [221] defines experts as “representative of their profession, have power to implement findings...not likely to be challenged as experts in the field...”. McKenna [222] defines as “a panel of informed individuals’, therefore the “expert” title is applied. It is important to identify the criteria by which you determine the composition of the expert panel prior to the conduct of research [223]. ISC², an international organization that provides the industry standard in information security credentials, defines an information security expert as having the following qualifications [224]:

- Advanced theoretical knowledge proven by international certifications;
- Practical experience in applying security;

- Ability to communicate with all levels, according to their level of understanding, from board level to end-user;
- Ability to find solutions which are not in books and prioritize them;
- Ability to view the risks beyond the obvious and act upon - be proactive and not reactive; and
- Ability to choose a solution which represents a fair trade-off between security and usability.

3.4.1 Validation

Expert panels are used to validate the constructs, content and relative importance of criteria within multi-criteria decision models as shown in Table 6 below [225].

Table 6: Summary of Expert Panel Application to Model

Validity	What is measured	Methods
Construct	The degree to which a measure relates to expectations formed from theory for hypothetical construct	Judgmental Correlation Convergent-discrimination Factor analysis Multi-trait/multi-method
Content	Degree to which the content of the items adequately represents the universe of all relevant items under study	Judgmental
Criterion-related	Degree to which the criterion can capture the true value of the variable	Judgmental Correlation

3.4.2 Selecting Experts

Careful consideration is required selecting experts to ensure that they will be relatively impartial when providing feedback as well as be up-to-date on current knowledge and perceptions in their field of expertise [226]. The relationship among experts as well as the relationship of experts to particular organizations should be carefully considered when developing expert panels. By definition, experts are intimately familiar with the given topic and as such may be biased, or perceived to be biased, based on their industry relationships. As an example, in the case of information security experts, an expert that worked for a particular software vendor could be perceived as providing feedback through the research process that if enacted would drive business back to the organization that employed them. Bias may also be introduced if experts are permitted to discuss research questions with one another. Strong voices or personalities in the community may influence the thinking of a panel of experts thereby skewing the feedback received. Additionally, experts must be provided some level of flexibility in their ability to provide feedback. A rigid feedback structure (e.g., structured survey without option for additional feedback) could be limiting and as such would not take full advantage of the experts' knowledge. Finally, the ability to access experts in some fields, especially emerging fields, and the willingness of those experts to participate in research activity may be limited.

When identifying experts and forming panels it is important to recognize that different levels of the research model may require different kinds of expert feedback.

As such a variety of expert panels, with varying perspectives and skills sets, may be required for a single model. For example, in the case of researching the development of an information security maturity model for healthcare organizations, it might be appropriate to have the highest level of information privacy and security experts (e.g., Chief Information Officer or Chief Integrity Officers) be on the panel that validates the mission level of the hierarchy. Responding to questions like, “Does this mission statement make sense?”, “Is this question worthy of research?” A second panel could be identified to validate the objectives that are most likely to measure information security maturity. This panel might consist of Chief Information Security Officers (CISOs). Further, a number of smaller panels could be developed that would focus on each of the goal level criteria, and yet another to focus on strategic level criteria. It is likely that some of these smaller panels would consist of Certified Information Security Professions (CISSPs) who have deep knowledge of technical solutions.

The size of expert panels should also be considered when developing research models. There are varying opinions on optimal panel size. Okoli and Pawlowski [227] propose that a panel of 10 to 18 members produce the best results, while others [228] suggest that 6 to 12 member panels produce optimal results. Small expert panels have been shown to effectively produce valid results using Delphi method [229][230][231]. Delphi method is especially helpful when the pool of experts is limited.

Information may be gathered from experts through a variety of methods. Common approaches are surveys, interviews, group processes, individual meetings and Delphi. Regardless of method, researchers need to provide experts with a comprehensive and easily understood research background, clear instruction on perspective or parameters of the questions being posed, and instructions related to measurement of response, as well as any other information that might ensure reliable responses from experts.

3.4.3 Inconsistency in Expert Judgements

As part of the model modification process inconsistency and disagreement among experts must be considered. While experts provide valuable insight to criteria selection and evaluation, their input is subjective, and as such, the opinions of specific experts may change or vary over time resulting in inconsistency in expert feedback. Inconsistency can be defined as disagreement within an individual's responses. For example, suppose an expert was asked to compare three modes of transportation when going to the grocery store: (a) riding a bike, (b) walking, and (c) driving. The expert responds that he prefers riding a bike to walking ($a > b$) and walking to driving ($b > c$). If the expert later responded that he preferred driving to riding a bike ($c > a$) this would demonstrate an inconsistent response. In this illustration the inconsistency would be labeled ordinal, the general order of preference. Ordinal consistency does not take into account the level of preference among available choices. Experts are often asked to provide measures of preference

when responding to prioritized choices. For example, an expert might be asked how much they prefer riding a bike when compared with walking (e.g., 2X), and how much they prefer walking to driving. (e.g., 3X). In this example, if asked, the expert would have to respond that they preferred riding a bike to driving by 6X otherwise cardinal consistency, or the level of preference, would be violated. It is worth noting that if cardinal consistency is satisfied, then ordinal consistency is satisfied as well, but the inverse is not true.

The importance of measuring and managing consistency in Hierarchical Decision Models (HDM) is critical. Kocaoglu's research [219][232][233] provides a clear definition of inconsistency and uses a variance-based approach for calculation of inconsistency in HDMs. Further, Kocaoglu recommends a 10% limit above which the reliability of expert feedback would be considered questionable. At the 10% level or greater expert feedback may be unreliable, as consistency of response is a critical factor in acceptance of feedback into the model. This recommendation is consistent with Saaty's [198] proposed consistency ratio with an upper limit of 10% for Analytical Hierarchy Process (AHP) models. Portland State University's Department of Engineering and Technology Management has created ©HDM software [234] which calculates inconsistency in experts compared against the 10% threshold discussed above, using the arithmetic mean of the standard deviation as shown below.

$$Inconsistency = \frac{1}{n} \sum_{i=1}^n \sigma_i$$

Any value which exceeds the 10% threshold would be worthy of deeper examination.

A new model for measurement of inconsistency in HDM was recently proposed by Abbas [235]. This new model provides a more flexible and less conservative approach to the standard 10% threshold recommended by Saaty and Kocaoglu. Abbas posits that the 10% threshold is overly conservative and that acceptable levels of inconsistency can be measured using the Root Sum Variance (RSV) method illustrated below. In Abbas' model the number of decision elements and alpha (α) level are linked for the purposes of evaluating the soundness and validity of the judgment.

$$RSV = \sqrt{\sum_{i=1}^n \sigma_i^2}$$

where:

σ_i^2 is the variance of the mean of the i^{th} decision element,

n is the number of decision elements:

$$\sigma_i = \sqrt{\frac{1}{n!} \sum_{j=1}^{n!} (x_{ij} - \bar{x}_{ij})^2} \quad \forall i = 1, \dots, n$$

where:

x_{ij} is the normal relative value of the variable i for the j^{th} orientation in n^{th} factorial orientations;

\bar{x}_{ij} is the mean of the normalized relative value of the variable I for the j^{th} orientation:

$$\bar{x}_{ij} = \frac{1}{n!} \sum_{j=1}^{n!} x_{ij}$$

When inconsistencies are identified in expert opinion the most important mitigation strategy is to carefully review the process by which the research is administered as well as review of the research instrument itself to ensure quality, clarity and consistency of information presented [236]. For example, if an inconsistency were identified for a specific expert, the researcher might re-run the analysis without that individual expert's contribution to determine if the overall value of the criteria changed. If the overall value of the criteria did not change then it would be appropriate to assume the expert's inconsistency did not negatively impact the model. Utilization of Delphi method also helps provide a measure of control such that any single expert's opinion would not have a significant negative impact on the model.

3.4.4 Disagreement Among Experts

In addition to the potential risk for inconsistency in expert feedback when using HDM, it is also possible that there will be disagreement among the experts. It is not altogether uncommon for experts to disagree. This could be due to a number of factors including professional or personal experiences of individuals. There are also issues that could cause disagreement among experts based on research design. Some disagreements may simply be the outcome of misunderstandings of individual experts. It is important to understand the key drivers leading to disagreement and to clarify any potential misunderstanding. Clarity and level of detail provided in the questions posed to experts is critical in mitigating the risk of disagreement. The risk of disagreement may also be mitigated by ensuring that each expert panel is assigned at the appropriate level in the decision model.

In order to determine if disagreement among experts exists two statistical methods are commonly used: Intraclass Correlation Coefficient (ICC or r_{ic}) and F-test with hypothesis testing. ICC provides an assessment of the degree to which all experts agree by comparing the means among the judgements of experts to determine high or low disagreement between the range of zero (0) and one (1). Zero represents absolute disagreement and one represents ultimate agreement. A value of $>.07$ is considered strong agreement [238][239]. The formula for ICC is provided below:

$$r_{ic} = \frac{MS_{BS} - MS_{res}}{MS_{BS} + (k - 1)MS_{res} + \frac{k}{n}(MS_{BJ} - MS_{res})}$$

where:

MS_{BS} is the mean square between decision elements,

MS_{res} is mean residual square,

MS_{BJ} is the mean square between experts,

k is the number of experts,

n is the number of decision elements

$$MS_{BS} = \frac{SS_{BS}}{df_{BS}}$$

$$SS_{BS} = \sum_{i=1}^n \left[\frac{(\sum S_i)^2}{k} \right] - \frac{(\sum X_T)^2}{nk}$$

$$df_{BS} = n - 1$$

$$MS_{res} = \frac{SS_{res}}{df_{res}}$$

$$SS_{res} = SS_T - SS_{BJ} - SS_{BS}$$

$$df_{res} = (n - 1)(k - 1)$$

$$SS_T = \sum X_T^2 - \frac{(\sum X_T)^2}{nk}$$

$$MS_{BJ} = \frac{SS_{BJ}}{df_{BJ}}$$

$$SS_{BJ} = \sum_{j=1}^k \left[\frac{(\sum X_j)^2}{n} \right] - \frac{(\sum X_T)^2}{nk}$$

$$df_{BJ} = k - 1$$

In order to increase confidence of assessment of disagreement Shrout and Fleiss [240] propose conducting a hypothesis testing procedure (F-test) as well. The null hypothesis (H_0) would indicate significant disagreement among experts. Each F-value is calculated and compared against the F-critical value to determine if the null hypothesis can be rejected. If H_0 is rejected, it can be concluded that no significant disagreement is present among experts. F-value and F-critical values are computed readily using the ©HDM Software created by the Engineering and Technology Management Department at Portland State University.

If disagreement among experts is identified using the techniques described above, the Hierarchical Clustering Method (HCM) may be used to identify individuals or groups that are similar. Analyzing these groupings can help to determine the cause of disagreement and in some cases identify groupings of experts that create better alignment. Hogaboam [220] used HCM techniques to create sub-groups within her expert panels that diminished disagreement on specific panels while leaving model alternatives unchanged.

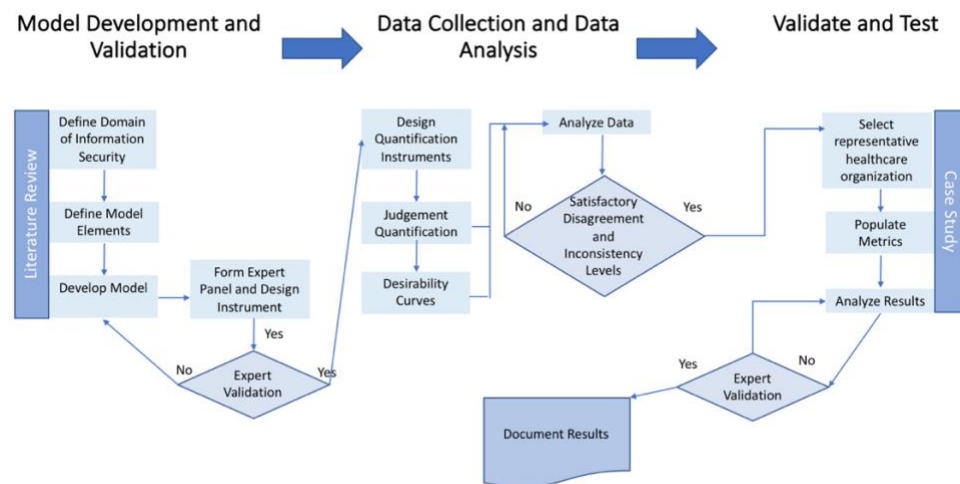
The techniques described above allow for disagreement to be identified and analyzed by comparing similarities and differences among sub-groups of experts. Analyzing the cause of disagreement can provide valuable information to inform the research process and outcomes.

3.5 Research Approach

It is clear from the literature review that due to the complexity of the issue a multi-criteria approach to decision making and evaluation of effectiveness of information security environments is required. It is also important to note that much of the information available to evaluate this issue is not publicly available due to the inherent risk associated with sharing information security knowledge relative to individual organizations. Further, current evaluation of the criteria that are typically identified as important to a strong environment of information security have been judged so through a qualitative process and have not been quantified.

The structured process illustrated in Figure 10 below was designed to guide this research.

Figure 10: Structured Research Process



Key steps of this process are discussed below:

Model Development and Validation – Conduct a comprehensive literature review to define the key objectives, goals and outputs related to information security maturity and develop a generalizable model which represents appropriate relationships among these elements. Use panel of industry experts to validate model for information security maturity.

Data Collection and Analysis – Utilize validated model to design research instrument to quantify data and create desirability curves by obtaining expert judgement. Analyze data for inconsistency and disagreement levels.

Validate and Test – Validate and test research instrument by conducting case studies to obtain metrics from representative healthcare organization. Analyze and document results.

3.5.1 HDM as a framework

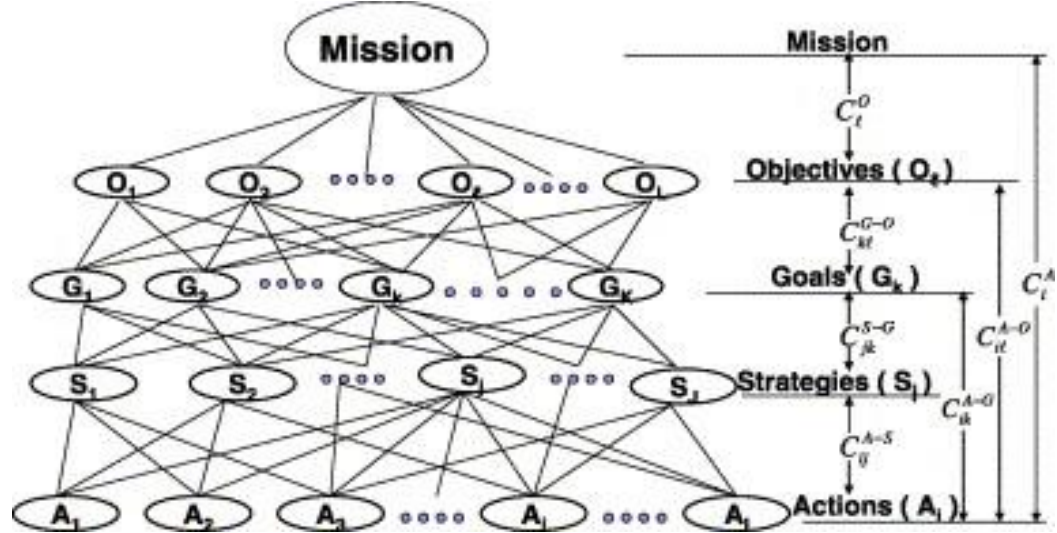
The Analytical Hierarchy Process (AHP) was introduced by Saaty [198] as multi-criteria decision model (MCDM) capable of deconstructing a problem into hierarchical levels of linked components. The Hierarchical Decision Model (HDM) is similar to AHP in providing a hierarchical approach to problem solving but differs in using a constant sum approach to quantifying judgements as opposed to the eigenvector approach used by AHP. HDM is well-known for providing a framework for quantifying subjective information so that effective qualitative judgements may be made for decision-making purposes [169][170][171]. A key capability of HDM is

the ability to quantify expert judgement thereby incorporating both structured and unstructured data into the model. HDM breaks down complex issues into key components that can be singularly identified and measured at the individual level with respect to criteria across multiple levels of the hierarchy. Components are broken down into pairwise comparison segments, where industry experts can evaluate a level of preference of one criterion over another as opposed to declaring an absolute preference. The constant sum approach requires experts to provide a numeric and relative value among options to largely qualitative questions. The researcher can then verify each expert's opinion with that of other experts, thereby validating the proposed model and documenting values across multiple opinions. HDM models have been broadly used to compare technology options for decades.

Phan [171] used HDM to create a framework of determining the level of innovativeness within organizations in the semi-conductor industry. Gibson [240] utilized HDM to create a measurement system for evaluating the performance of engineering and science research centers. Tran [225] used HDM to develop an index to measure the effectiveness of a technology transfer office based upon fulfillment of the stated mission. Estep [241] developed a technology transfer score for evaluating research proposals using HDM. These researchers effectively used the HDM method to construct measures of effectiveness in fields where data is both qualitative and quantitative.

Introduced by Cleland and Kocaoglu [232] in 1981, HDM is well-suited for evaluation of a problem based on mission, objectives, goals, strategies, and activities/actions (MOGSA). Figure 11 [219] below is a generalized form of the MOGSA framework typically utilized in developing HDMs.

Figure 11: Generalized Hierarchical Decision Model



The purpose of the model is placed at the top of the hierarchy at the “mission” level. Organizational “objectives” associated with the mission are located at the next lower level in the model. “Goals” associated with each objective are documented in the third level of the model, followed by “strategies” related to the defined goals. Measurement of the desirability of strategies leads to the creation of a number of actions or alternatives that might be considered to meet the stated mission. In the case of developing an index for measuring information security maturity, various alternatives will ultimately be identified that align with defined maturity levels. Some

strategies will certainly contribute more than others to the overall maturity index. The relative value of each strategy will be determined by experts.

Experts will be utilized at various stages of the research process. When collecting expert feedback to validate the model's content and construct a structured Delphi process will be used.

3.5.2 Delphi

The Delphi method is an iterative multi-step process designed to elicit expert opinions and achieve group consensus from different stakeholder perspectives [242][243][244]. Delphi is a popular method used in healthcare research [222][223][245]. The initial research instrument used for model validation will include the opportunity for experts to provide qualitative feedback, which will then be fed back to the experts in subsequent assessment [223]. The Delphi method is used when basic demographic, economic or historical information is inadequate to conduct desired research [193][246]. Delphi is a way of structuring communication among a group of experts such that they are able to contribute their expertise independent of one another, so as not to be unduly influenced by one another. The Delphi method and the HDM are frequently combined when using expert panels to validate model construct and content [240][220].

3.5.3 Desirability Curves

A comprehensive review of literature identified objectives, goals and strategies as key elements required to measure the maturity of information security within any given organization. A generalizable model was developed and presented to experts for validation of content and construction.

Estep, Gibson, Phan and Tran [195][26] [240][241] all used desirability curves in the conduct of their research. The purpose of desirability curves is to identify how “desirable” or valuable a specific metric is to decision makers. Estep [241] used the mathematical representation below when incorporating the influence of desirability curves in creating a healthcare information security maturity score:

$$TT\ Score = \sum_{n=1}^N \sum_{jn=1}^{Jn} (STT_{n, jn}) (D_{n, jn})$$

$STT_{n, jn}$ = Relative value of the jn^{th} success attribute under the n^{th} perspective with respect to the Technology Transfer score (TT)

$D_{n, jn}$ = Desirability value of the performance measure corresponding to the jn^{th} success attribute under the n^{th} perspective

Desirability curves will be used in conduct of future research when a comprehensive model is prepared.

3.5.4 Sensitivity Analysis

As mentioned earlier in this chapter, two measures of sensitivity analysis must be conducted when validating HDMs – inconsistency and disagreement.

Inconsistency is related to individual expert's responses when responding to quantification of the model. In general, inconsistency should be measured at less than 10% for valid results. Disagreement among experts must also be measured. Experts are likely to have some variability in responses across expert populations, but there should be general consistency to validate the model. If disagreement is identified, a deeper analysis must be conducted to determine the cause of disagreement and appropriate mitigation efforts should be employed.

3.5.5 Challenges and Mitigation Strategy

There are two notable challenges associated with the proposed application of HDM. First, as the number of criteria for evaluation increases, quantification of each criterion can become difficult. Second, as new technologies are identified the whole series of judgement measurement may need to be repeated. In order to mitigate this challenge a composite index, sometimes called a "technology value", will be developed by combining the relative values of each strategy along with desirability scores for each strategy. In doing so, a semi-absolute value for each strategy's impact on the named objectives will be created and utilized instead of a relative value [247].

3.5.6 Limitations of Hierarchical Decision Model (HDM) with Delphi

The research uses a Hierarchical Decision Model (HDM) to assess the ways in which an information security maturity index is created for healthcare organizations. HDM relies on expert judgement to validate the criteria relevant to the model and

apply weighting to said criteria. In this way, HDM provides a comprehensive view of the issue under consideration in a way that is easily understood by decision makers.

Like any multi criteria decision model, HDM has both strengths and weaknesses. The key limitations of HDM are noted below.

Risk of using experts to validate and quantify model. While utilization of experts can be extremely valuable where quantitative data is hard to obtain, there is risk of both inconsistency in expert feedback and disagreement among experts. This risk can be mitigated with sensitivity analysis and the strategies identified previously. In addition, results of expert opinion are highly subjective and experts are sometimes difficult to access. Careful selection of experts and reliable access to industry experts is required to mitigate this limitation.

Risk associated with pairwise comparisons. The number of pairwise comparison required to describe the issue in a comprehensive way can be significant. This can not only be a deterrent to expert participation, but can also cause fatigue in experts leading to rushed or not well considered feedback [248][249]. This risk was mitigated by careful structure of the expert panel groups and by limiting the number of comparisons in each iteration. In addition, the framework of collecting data (e.g., pairwise comparisons) can be considered restrictive. This risk was mitigated by careful validation of the criteria of the hierarchical model prior to quantification of the model, including providing paths for experts to provide unsolicited feedback at the model development stage.

Risk of overgeneralization. There is a tendency for HDM to be thought of as a solution rather than a model to be used to inform decisions. It must be made clear that the model is not a specific answer to a given problem but rather a tool to be used by decision makers.

Durability of model over time. HDM is well suited to complex issues in emerging fields. However, that specific fit also poses a risk as these emerging fields may be rapidly changing. This model will need to be revisited over time to ensure it remains relevant.

3.5.7 Identification of Information Security Experts for Panels

Experts are a valuable resource to the research community. There are a number of well-known methods for identifying industry experts. Some of those methods are identified below.

Snowball sampling uses a small pool of initial contacts to identify other participants who meet the eligibility criteria and could potentially contribute to a specific study [250]. The term "snowball sampling" reflects an analogy to a snowball increasing in size as it rolls downhill. This method of acquiring experts is best used where it is difficult to identify experts but has limitations in that it is non-random and has a high incidence of community bias.

Citation analysis is a method of identifying experts based on an analysis of citations of published documents [251]. This popular and long used method of identifying academic experts works well in identifying academic experts on a given

subject, but it is less valuable when there may be a limited number of experts published in emerging fields or when operational industry knowledge is required.

Social network analysis is a method of identifying experts by mapping relationships among individuals, web pages, organizations and other connected units of measure [252]. Nodes in the network analysis are individuals and groups associated with key identifying labels (e.g., information security). While effective at identifying relationships that may not be readily apparent, it can also present anomalies and as a result is sometimes less reliable and requires additional validation [219].

National expert databases may be purchased from a variety of sources. These databases are culled from numerous sources and generally sold for the purpose of sales leads. While they may be used as a source of information to define industry experts they are often out of date, non-granular and expensive to acquire.

Professional organizations are yet another source for identifying subject matter experts that may serve as resources in expert panels. Most professional organization rosters have the benefit of self-affiliation. In other words, individuals identify themselves as experts in a given field and seek to join these organizations in order to be part of a community of interest to share best practices, access to one another, and up-to-date industry information. It can be challenging to gain access to a list of members if one is not a member of said organizations. Many professional

organizations do not provide lists of their members to others, some do provide access to list of members but often this is provided at a substantial fee.

For the conduct of this research, this researcher has the benefit of access to a number of professional organizations in both the information security and healthcare information technology fields. Below is a list of some organizations that could be accessed to identify experts in information security.

CompTIA is a non-profit trade association, dedicated to advancing the interests of IT professionals and IT vendor organizations. They provide education, certifications, advocacy and philanthropy as well as networking opportunities for IT professionals. <https://www.comptia.org/>

EC-Council is a member-based organization dedicated to providing resources to information security professionals. The organization provides training standards for education and certifications as well as forensic resources. <https://www.eccouncil.org/#>

GIAC - Global Information Assurance Certification is a professional organization focused on certification of information professionals. <https://www.giac.org/>

ISACA is a non-profit organization committed to providing information on development and adoption of information security best practices to professionals in the field. <http://www.isaca.org/about-isaca/Pages/default.aspx>

(ISC)² – International Information System Security Certification is an organization that specializes in providing certification to information security professionals. Their Certified Information System Security Professional (CISSP) is the industry standard. <https://www.isc2.org/>

ISSA – Information Systems Security Association is a non-profit, member-based organization dedicated to providing a community of best practice for information security professionals. They provide educational forums, publications and peer interaction opportunities. <http://www.issa.org/>

In addition to the professional organizations identified above, focused broadly on information security, there is also a single professional organization specifically focused on information security professionals in the healthcare industry.

AEHIS – Association for Executive in Health Information Security <http://www.issa.org/> was founded in 2014 and offers a professional development and networking forum for Chief Information Security Officers (CISOs), and other top-ranking information security leaders, in the healthcare sector. AEHIS provides educational resources, networking opportunities and other resources related to both information security and information privacy. Although it has a brief history, it was created by CHIME, the College of Health Information Management Executives <https://chimecentral.org/>, an organization that brings 25 years of experience as the industry leading professional organization for healthcare information technology professionals. Through membership in CHIME, individuals are permitted access to

send member-to-member surveys to CHIME and AEHIS members. CHIME currently has more than 3,000 members.

CHIME and AEHIS members are ideal candidates in the development of expert panels for the conduct of research associated with developing a maturity model for information security in healthcare organizations. As such, due to researcher's access to CHIME and AEHIS database as a member of CHIME, these organizational membership lists served as the foundation of all expert panels. In addition, a number of panel members were identified through social networks of the researcher.

3.5.8 Expert Panel Development

This study used a multi-stage process where a total of fifty-one selected experts formed six discrete panels to validate, and then quantify, model elements. Many experts met the criteria to serve on multiple panels and agreed to participate in such. A seventh panel was created to validate and quantify metrics of desirability.

An original candidate pool of 214 potential experts was culled from the CHIME members (3,337) and AEHIS membership (900) lists as noted above. Care was taken to ensure that no more than one person from any given healthcare organization was identified as a potential participant, that all experts held a title of either Chief Information Officer, Chief Privacy Officer, or Chief Information Security Officer, and that they remained employed in the field of health information security. In addition, experts were selected from a variety of healthcare organization types: academic medical centers, critical access hospitals, small stand-alone community hospitals,

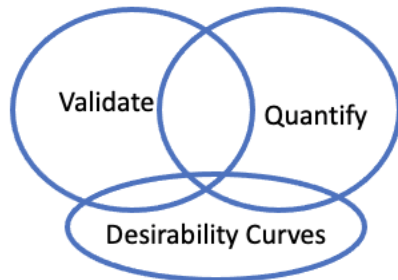
mid-size stand-alone community hospitals, large healthcare systems and integrated delivery networks. Finally, experts were selected with the objective of broad geographic representation across the United States in mind.

An invitation was sent to all candidates requesting participation in the research study. The invitation identified the researcher as both a student and a colleague in order to obtain greater likelihood of participation. Those that agreed to participate received consent forms, a summary of the proposed research and targeted research collection instruments. A copy of all research instruments is provided in Appendix A.

Of the fifty-one consenting subject matter experts, thirty-five were Chief Information Officers (CIO), five were Chief Privacy Officers (CPO), and eleven were Chief Information Security Officers (CISO). A comprehensive list of experts, identified by organization type but not specific affiliation in order to protect confidentiality, can be found in Appendix B-2. Each panel was created taking into consideration the specific skill set of the given subject matter expert. For example, expert panel P₁ was used to validate the literature based HDM. CIO, CPO and CISO experts were selected for participation in this panel due to their broad knowledge of information security. These experts assessed the overall landscape of information security and the objectives and goals that have influence on the stated mission of the model. As illustrated below in Figure 12 overlap in panels occurs as some experts serve support

roles for multiple functions: validation, quantification, and development of desirability curves.

Figure 12: Expert Functions



A comprehensive list of each panel is provided in Appendix B-1.

3.5.8 Data collection and analysis approach

As noted earlier in this chapter, Delphi method was used to facilitate data collection for the conduct of this research. This method uses a series of surveys to obtain feedback at controlled intervals in a structured way from a variety of perspectives. This method was used to validate the construction and content of the HDM model. For example, in phase 1 of this research expert opinion was obtained using well-defined yes/no acceptance to validate model criteria. Agreement rate of 80% is acceptable [234]. This model's strength is a transparency which leads to consensus; however, it can inhibit unique feedback. In order to mitigate this concern, an open text box was provided to experts to facilitate collection of additional feedback related to the model. Results of this process are provided in Appendix C.

Once the model has been validated each element must be quantified. For this second phase of research experts were presented with pair-wise comparisons through a carefully designed online quantification instrument provide by Portland State University Engineering Management Department's HDM software. The HDM software uses a constant-sum method for allocating 100 points between two model elements. Distribution of the 100 points provides a relative importance under the parent element. The values are then normalized relative to each related element. The process results in an overall value rating for each element with respect to the linked objective in the decision model.

The HDM software also provides analysis for inconsistency and disagreement as discussed previously. Research instruments and data collection are provided in Appendix D.

3.5.10 Case studies

Five case studies were developed to illustrate how the model calculates a score and how these scores can be used to conduct a comparative analysis and develop a roadmap for improvement of the information security environment. The following organization types were identified as case study candidates in order to confirm the maturity model was appropriate for both small and large healthcare organizations.

- Critical Access Hospital
- Stand-alone Community Hospital

- Integrated Delivery Network
- Large Healthcare System (more than one hospital and over 500 beds)
- Academic Medical Center

Case studies were conducted through interviews with highest level information technology executive at each site. The results of case study were presented to experts to determine the degree to which the model effectively reflected the actual performance of each site. Ideally an external evaluation of case study results would be conducted, however the confidential nature of information security and the lack of publicly available data related to information security makes such an assessment infeasible at this time. Gibson successfully utilized the approach of expert self-assessment in her study related to the development of a measurement system for collaborative research centers [240].

CHAPTER 4: HDM DEVELOPMENT

The hierarchical decision model (HDM) provides a flexible and stratified structure for decision making. The purpose of the model is to determine the maturity level to which a given healthcare organization has created a strong information security program. It is a generalizable model that outputs a performance evaluation score for a healthcare organization by evaluating a comprehensive set of metrics.

At the top of the model, the objective is the organizational maturity score. At the second level, objectives represent areas or categories of information security protection. At the third level, goals are identified which relate to each information security objective. Finally, desirability curves are used to measure each goal. The remainder of this chapter documents the model elements, their links to one another, and shows how the generalizable model is constructed.

4.1 Objectives

The following five information security objectives were identified:

1. Organizational support for information security;
2. Information security policies and standards;
3. Information security awareness and training;
4. Information security technical hygiene; and
5. Mitigation of external threats.

These objectives were derived by exhaustive review of existing literature related to cybersecurity, feedback from experts and by review of the cybersecurity frameworks themselves such as NIST [97], HITRUST [99], CIS [253], ONC [5]. Each of the five objectives is discussed in greater detail in the following sections.

4.1.1 Organizational support for information security

Organizational support is a key pillar of successful information security programs and can be defined as a high level of support for information security, including support at the Board level of the organization. Support is demonstrated by engagement and understanding of information security risk by modeling behaviors and by provision of financial support. The original model was modified from “leadership support” to explicitly named “Board of Directors” level support based on feedback from subject matter experts. As seen in broadly publicized recent information security incidents at healthcare organizations, such as the incident at Scripps Health [254], the potential for reputational harm to organizations who experience information security incidents is high.

4.1.2 Information security policies and standards

Information security policies and standards are of critical importance to any cybersecurity framework and are especially important in highly regulated healthcare organizations [5]. Organizations who document their information security policies

and procedures, update them routinely, and make them available to all users of technology are likely to have a more robust information security environment.

4.1.3 Information security awareness and training

Human behavior is a significant factor in information security environments [27]. When workforce members possess an understanding and acceptance about the need for all organizational members to protect information assets, organizations are better positioned to have a mature information security environment. Through diverse training and awareness events, organizations can share information with organizational members about the risks and risk mitigation strategies related to information security and thereby improve their performance. During the model validation process two subject matter experts called out the need to reinforce the notion of “shared accountability”- i.e., information security is not a singular IT responsibility but rather it is everyone’s responsibility. This is a common theme in speaking with information security professionals. In order to incorporate this feedback into the model this objective definition was modified to reflect this interest.

4.1.4 Information security technical hygiene

Information systems require active system maintenance in order to prohibit information security vulnerabilities. Organizations that implement technology and process controls to maintain system health are well positioned to minimize their information security risks and improve their information security maturity. Routine

technical hygiene is the foundation of information security best practices, as is well documented in all cybersecurity frameworks [96][97][99][253].

4.1.5 Mitigation of external threats

External information security threats are pervasive [255], as recent cybersecurity incidents in healthcare organizations [29][31] illustrate. Organizations with mature information security programs implement technical controls to mitigate external threats. These tools help organizations understand when restricted data may have left the organization, minimize incoming spam, which may be phishing attempts, and prevent and detect unauthorized users from accessing an organization's network.

The original HDM model consisted of a single goal related to technology controls; however, given the high volume of expert feedback received, the original goal of "technical controls" was split into two goals 4.1.4 and 4.1.5, information security technical hygiene and mitigation of external threats respectively. The high volume of feedback is unsurprising given the vast number of technical controls available and the technical orientation of the subject matter experts.

4.2 Goals and Outputs

Each of the five objectives noted above has either four or five associated measurable goals. As the model was finalized the Delphi method was extremely useful in validating the goals associated with each objective, clarifying goal definitions, as

well as identifying new goals where it is required to ensure a comprehensive model. Each of these goals is documented below with appropriate details where the model changed over time to response to the feedback of subject matter experts.

4.2.1 Organization Support - Governance

Established governance processes are key components of existing cybersecurity frameworks [97] and are critical in shining a spotlight on the risks associated with poor information security in healthcare organizations including compliance risk [50][55]. Robust governance systems also aid in assuring that information security solutions are mindful of needs of the business to continue to operate. A framework to provide assurance that information security strategies are aligned with business objectives as well as applicable laws and regulations is fundamental to a successful information security program.

All subject matter experts agreed that a comprehensive governance structure is required, with the exception of one SME who did not think governance was required upon initial evaluation of model. Follow up was provided by this expert which indicated that they believed that governance, while “not unimportant, was the least important of the goals identified under the organizational support objective”.

4.2.2 Organization Support - Leadership and management

Information security professionals have long faced the challenge of engaging organizational leadership and management in support of a strong information

security culture. Often information security is thought of as the responsibility of technology professionals as opposed to the responsibility of all at the organization. Technology alone will not provide the level of protection required. Strong support from leadership and management, including organizational Board members, who are engaged in understanding information security risk [75] and model behaviors to protect organizational assets is an important driver in culture change and sustainability of effective information security programs. A regular review of key performance indicators by leadership ensures that the philosophy of consistent improvement is embedded in information security programs [50][65].

Subject matter experts uniformly agreed to the importance of this goal and requested the definition be explicit about the importance of board engagement.

4.2.3 Organizational Support - Resource availability

Information security programs require diverse resources in order to be successful – people, tools and community engagement [50][53]. Most healthcare organizations are woefully under-resourced to respond to the current cyberthreat landscape [256]. Successful programs must have assurances that adequate financial resources are available to support information security [256], including dedicated information security resources. While closely linked to governance and leadership support, provisioning of adequate resources is a discrete need of successful programs.

Subject matter experts agreed that resource availability was worthy of a discrete goal within the model. Two experts noted that dedicated information security resources were required and as a result the goal description was revised to include this clarity in definition.

4.2.4 Organizational Support - Risk assessment, risk management, disaster recovery and incidence response

Regular risk assessments are a foundational element of existing cybersecurity frameworks [79][253] and are specifically called out by the office of the national coordinator for health information technology's guide to privacy and security of health information [5]. The companion product to the risk assessment is a risk management plan, providing the ability to manage known organizational risks [257].

Subject matter experts broadly agreed with the inclusion of risk assessment and risk management plan as a model criterion. They also suggested that disaster recovery and associated incident response plan where appropriate to include within this portfolio of assessment and response tools. The model and associated definition were revised to include these interests.

In summary, the suite of tools required to support a mature information security environment within the context of organization support are an unbiased information security risk assessment performed on a regular basis and used to

commit to the development and execution of a risk management plan as well as a disaster recovery and associated incident response plan.

4.2.5 Policies and Standards - Policy documentation and awareness

Policies are used to define the rules by which an organization agrees to operate and are important in the realm of information security programs. A set of policies issued and updated regularly by the organization to ensure that all members understand requirements related to information security is a baseline expectation for information security programs [37][55][79] to ensure that not only are shared interests understood but also to enable compliance with federal and state laws.. Policies should be accessible [52] and well communicated to organizational members. Compliance with policies should be routinely audited.

All subject matter experts agreed with inclusion of this criterion in the model, with the exception of one SME who did not think policy documentation and awareness was required. Four subject matter experts suggested that auditing of compliance with policies was also necessary. This audit interest was included in the final definition of the model element.

4.2.6 Policies and Standards - Procedure documentation and awareness

Information security procedures are the companion to information security, essentially providing the “how” of compliance related to procedures. A set of procedures that are updated regularly and provide guidance to members about how

to ensure compliance with information security policies are needed [38][52][54][55]. Procedures should be accessible and well communicated to organizational members and compliance with procedures will be routinely audited.

Subject matter experts agreed with the inclusion of this criterion in the model.

4.2.7 Policies and Standards - Technical standard documentation and awareness

Technical standards (e.g., hardware standards, configuration standards, patch management standards [96][97][253] should be documented and updated regularly by the organization to ensure all organization members (as appropriate) understand requirements related to information security. Technical standards should be accessible and well communicated. Compliance with standards will be routinely audited.

Technical standards were not originally defined as a discrete goal within the model as they are generally a part of the overall policy and procedure documentation. Five subject matter experts provided feedback that their importance was such that they should be specifically noted independent of other policies and procedures so the model was revised to reflect this feedback, which is also supported by the literature.

4.2.8 Policies and Standards - Sanction documentation and awareness

Sanctions are defined as a set of repercussions associated with non-compliance related to information security policies. Non-compliance may be the result of a simple mistake, may be intentional and associated with harmful intent, or fall somewhere between those ends of the spectrum. Employees must believe that sanctions are appropriate to the behavior and must believe that they will be consistently applied across an organization regardless of role in order to have a fully functional information security program [38][79][257][258]. Sanction documentation should be accessible and well communicated to organizational members. Compliance with sanction guidance should be routinely audited.

While most subject matter experts believed that sanction documentation was important, five experts indicated they were unsure of its importance or that they thought it less important than other model elements. This is not surprising as sanction documentation is not always included in existing cybersecurity frameworks; however, the literature strongly supports the inclusion of this criteria from a culture perspective so the criterion remains part of the overall model.

4.2.9 Awareness and Training - Communications

Broad communication about information security is a cornerstone of successful information security programs. The creation and internal delivery of collateral, such as articles in newsletters, blogs, posters and other internal

communication venues are valuable in raising awareness and changing behaviors [41][50][65][259].

Subject matter experts uniformly agreed to the importance of communications related to information security as part of an effective information security program.

4.2.10 Awareness and Training - Awareness events

Awareness events are planned occasions designed to raise awareness of information security knowledge throughout an organization and have been determined to improve information security programs and the culture related to information security [65][79][260].

Subject matter experts uniformly agreed to the importance of awareness events related to information security as part of an effective information security program.

4.2.11 Awareness and Training - Information portal

An information portal is defined as an easily accessible internal source that provides a knowledge base of security related information [260]. As part of the broad information toolkit [259], this could include information both about how to be aware of security threats, how to be secure when working from anywhere, and how to report information security incidents [65]. It would also likely serve as a source for

information security policies and procedures. Information portals are common in most organization, built out to varying degrees.

While subject matter experts generally agreed to the importance of an information portal in support of a strong information security program, six subject matter experts did not believe an information portal was important on first review. Upon further investigation it became clear that the experts were considering this information portal, in isolation, as if an information portal might be the only way to communicate information about training or awareness. Given this feedback, the definition of this goal was re-written to be more explicit about an information portal's importance as part of a broader toolkit of information security training and awareness tools.

4.2.12 Awareness and Training - Training

Information security training may be delivered either by computer, in-person, or both. One-on-one training could be in the form of seminars, departmental meetings, or one-on-one sessions. Some training may be mandatory while other training may be optional. Training, while sometimes discounted by trainees, is a powerful tool in creating a culture which supports strong information security practices [37][55][63][146][261].

Subject matter experts universally agreed that training was appropriate for inclusion in the model.

4.2.13 Awareness and Training - Behavioral and real-time teaching

Behavioral testing and real-time teaching, used appropriately, are effective tools in testing work force member's compliance behavior in an attempt to demonstrate the common schemes to penetrate information security defenses [52][65]. It is important that behavioral and real-time teaching be conducted in such a way that individuals are not embarrassed or shamed if they initially fail these tests [37][259]. Rather these events should focus on the learning opportunity and improvement over time. Common tools in this arsenal are related to teaching about phishing and USB drive drops (e.g. if you find a USB drive you should not stick it in your computer to see what is on it).

Subject matter experts generally agreed that behavioral testing and real-time teaching were appropriate for inclusion in the model.

4.2.14 Technical Hygiene - Physical controls

Physical access controls which limit access to technology infrastructure (equipment/media) or confidential information are essential. Typical controls generally include, but are not limited to, locked barriers, badged access, and security cameras. This information security element can be found not only in predominant cybersecurity frameworks [97][99][253] but also as guidance from the office of the national coordinator for health information technology [5].

While this element was not part of the original model it was included based on subject matter expert feedback.

4.2.15 Technical Hygiene - Asset management

Under the theory that you can't protect what you don't know about, all major cybersecurity frameworks [97][99][253], as well as the office of the national coordinator for health information technology [5] recommend robust asset management systems as part of a comprehensive information security program. Asset management systems are defined as technology that supports life cycle management related to physical and virtual technology assets.

While this element was not part of the original model it was included based on subject matter expert feedback.

4.2.16 Technical Hygiene - Routine security updates

Mature information security programs are characterized by processes and technical tools that facilitate routine security updates for software, endpoints, biomedical devices, and other systems. These security updates are a key element in minimizing security vulnerabilities that are often exploited by cybercriminals and are often incorporated in existing cybersecurity frameworks [97][99][253].

Subject matter experts consistently agreed to the importance of this model element and suggested the inclusion of biomedical devices in the definition. This is

most appropriate for healthcare organizations and was included in the definition. If this generalizable model was used outside of healthcare the reference to biomedical devices should be removed but could be replaced with references to the “internet of things” – other devices often out of the span of control of classic information technology operations but vulnerable nonetheless.

4.2.17 Technical Hygiene - Protection of stored information and information in transit

Most modern information security programs include technology (e.g., encryption technologies) that ensures data at rest and data in transit are not vulnerable to misuse.. All major cybersecurity frameworks [97][99][253], as well as the office of the national coordinator for health information technology [5] recommend protection of stored information and information in transit as a key criterion in a strong information security program.

Subject matter experts consistently agreed to the importance of this element in the model.

4.2.18 Technical Hygiene - Identity, authentication, access management and monitoring

Technical tools that ensure only those individuals and systems that need access to sensitive data and systems are able to do so. Identity, authentication, access management and monitoring are components of comprehensive information security

programs as well as major cybersecurity frameworks [97][99][253], In addition, they are recommended by the office of the national coordinator for health information technology [5] as components of strong information security programs.

Subject matter experts consistently agreed to the importance of this element in the model.

4.2.19 External Threats - Data loss prevention

Monitoring data as it leaves an organization provides a yellow flag of sorts to potential compromise of information security integrity within an organization. Technology tools that monitor data as it leaves the organization help ensure appropriate levels of security for sensitive information. Data loss prevention tools are components of comprehensive information security programs as well as major cybersecurity frameworks [97][99][253], In addition, they are recommended by the office of the national coordinator for health information technology [5] as components of strong information security programs.

Subject matter experts consistently agreed to the importance of this element in the model.

4.2.20 External Threats - Anti-spam and malware protection

In recent years technologies that minimalize incoming spam and mitigate the threat of malware infection have become ever more important as nefarious phishing

campaigns have flooded both personal and business environments. These tools are consistently components of comprehensive information security programs as well as major cybersecurity frameworks [97][99][253]. In addition, they are recommended by the office of the national coordinator for health information technology [5] as elements of strong information security programs.

Subject matter experts consistently agreed to the importance of this element in the model.

4.2.21 External Threats - Intrusion detection and prevention

The most mature information security programs include 24x7 intrusion detection and prevention (a.k.a. Managed Detection Response) programs utilizing Security Information and Event Management (SIEM) tools. This information security element has received more attention in recent years and is included in both the NIST cybersecurity framework [97] as well as the Center for Internet Security framework [253].

This element was not included in the initial model but was added based on feedback from nine subject matter experts. In one case, an expert noted that if they had a managed detection response program in place they would not have been the victim of a recent cyberattack which cost the organization both significant financial loss as well as reputational harm.

4.2.22 External Threats - Protection of network

Some of the most fundamental and long standing elements of information security relate to protection of an organization's network. Technical tools that minimize threats from outside the network (e.g., network access control, network segmentation, firewalls, routine vulnerability scanning) are key elements of an effective information security plan. This element is found in nearly all cybersecurity frameworks [97][99][253].

Subject matter experts consistently agreed on the importance of this element in the model and two experts called for a clearer definition that included network access control and routine vulnerability scanning. The definition of this goal was modified to reflect this interest which is also supported in the literature.

In conclusion, each element in the model was evaluated by subject matter experts using the Delphi process. Experts were asked the binary yes/no question related to appropriateness of individual element to be included in the model. The results of those responses all exceeded the 80% or greater agreement threshold [234].

4.3 Metrics

Measurement of information security metrics is more art than science, due to the complexity of the information security environment and the ever changing information security threat landscape. Existing cybersecurity frameworks lack

specificity of measurement [130] and should strive to provide a quantitative and objective basis for security assurance [126]. As noted in Chapter 2, information security metrics were recognized on the Hard Problem List of the United States INFOSEC Research Council in 2005, a situation confirmed by the United States National Science and Technology Council in 2011 and further supported as one of the five hard problems in Science and Security in 2015 [83].

Metrics were established for the output associated with each goal in the model and presented to experts for validation. Following validation, experts were utilized to develop desirability curves for each goal level criteria within the model in order to quantify the output. Specific metrics and their associated desirability curves are provided in the next section of this document.

4.4 Desirability Curve Development

As noted above, expert judgement is used to quantify desirability curves for each metric. Development of desirability curves is a method which converts qualitative or quantitative data for a given element in the model to a scaled quantitative value. Using a scale of 0 to 100, where 0 is the least desirable state and 100 is the ideal state, a scale with normalized values is developed. The concept is clarified by Kocaoglu [232] as a method to utilize expert judgement to create values about how good or desirable an output is to decision makers. It is important that the

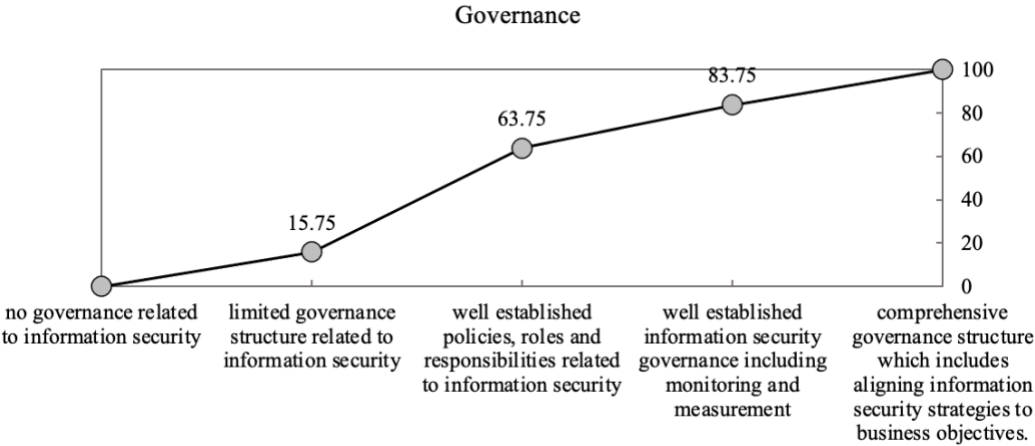
experts identified to aid in the development of desirability curves are decision makers as the model will rely on these metrics to define “goodness” of output.

Metrics and desirability curves relative to each of the twenty-two goals within the model are presented below. Figures 13-34 show their respective desirability curves. Appendix E-1 provides an example of the tool that was shared with experts in the development of desirability curves and Appendix E-2 provides the metric definition and values used to create the curves.

4.4.1 Desirability Curves Associated with Governance

Information security governance metrics consist of measures associated with established governance structure, defined roles and responsibilities, monitoring and measurement of information security performance, and alignment of information security strategies with business objectives. As noted below experts determined the ideal state as one that included a comprehensive governance structure which includes aligning information security strategies with business objectives. There is a notable increase in desirability from node 2 to 3 in the curve below associated with the move from a general structure to defined roles and responsibilities.

Figure 13: Desirability Curve for Governance Goal



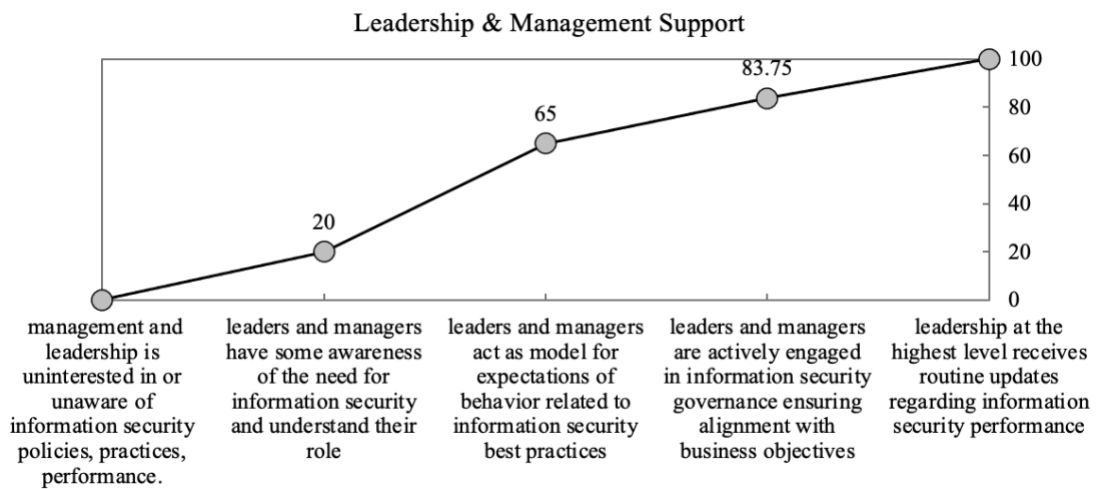
4.4.2 Desirability Curves Associated with Leadership and Management

Support

Information security leadership and management metrics consist of measures associated with awareness, understanding, and engagement related to information

security, up to and including, modeling of best practices and engaging in alignment of business practices associated with information security, as well as routine review of information security performance. Experts determined the ideal state as one that included all of these characteristics, with a significant increase in desirability between nodes 2 to 3 where leaders begin to model information security best practices.

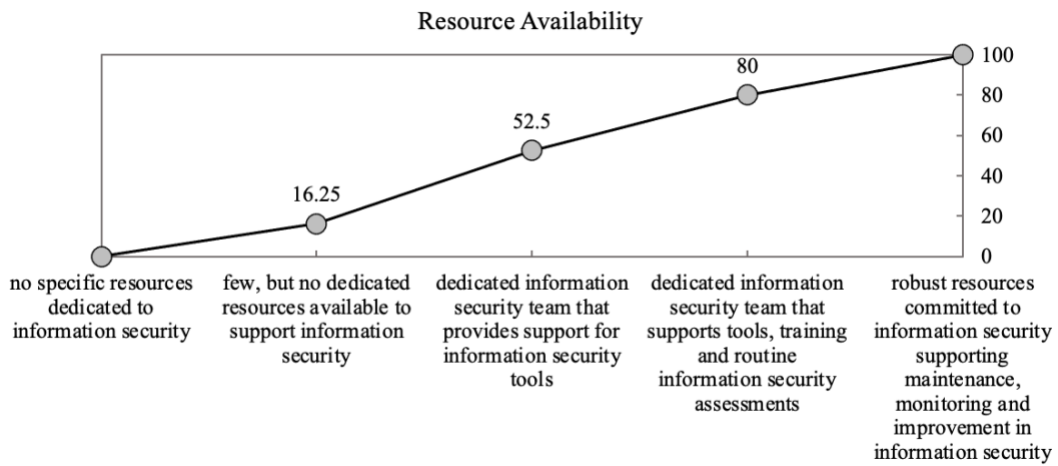
Figure 14: Desirability Curve for Leadership and Management Support Goal



4.4.3 Desirability Curves Associated with Resource Availability

Information security resource availability metrics consist of measures associated with dedicated information security teams that support tools, training, routine assessments, monitoring and consistent improvements in information security at an organization. Experts determined the ideal state as one that included all of these characteristics, with a curve that rose steadily.

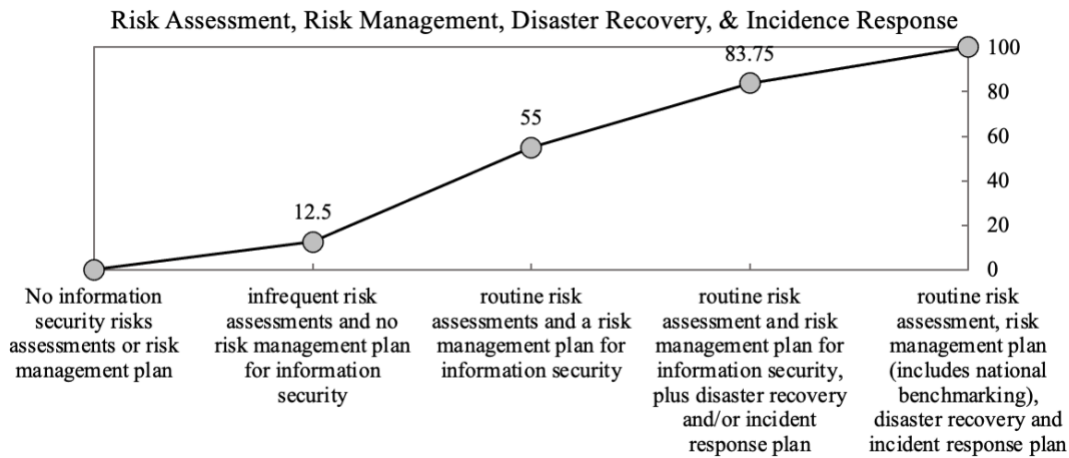
Figure 15: Desirability Curve for Resource Availability Goal



4.4.4 Desirability Curves Associated with Risk Assessment, Risk Management, Disaster Recovery and Incidence Response

Information security risk assessment, risk management, disaster recovery and incidence response metrics consist of measures associated with documentation and practices explicitly named in the title as well as benchmarking against peers. Experts determined the ideal state as one that included all of these characteristics. Several experts reported node 3 to be a minimally acceptable standard within healthcare organizations.

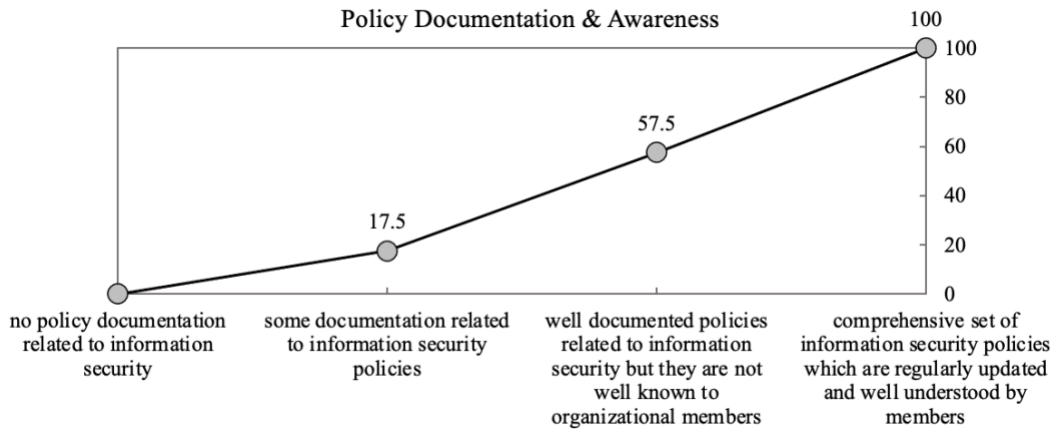
Figure 16: Desirability Curve for Risk Assessment, Risk Management, Disaster Recovery and Incidence Response Goal



4.4.5 Desirability Curves Associated with Policy Documentation and Awareness

Information security policy documentation and awareness metrics consist of measures associated with comprehensiveness of documentation, frequency of policy review and update and understanding by organizational members of relevant policies. Experts determined the ideal state as one that included all of these characteristics. Experts noted anecdotally that reaching node 3 was especially important in healthcare environments where compliance agencies routinely review policy documentation and use it as a measure associated with facility accreditation.

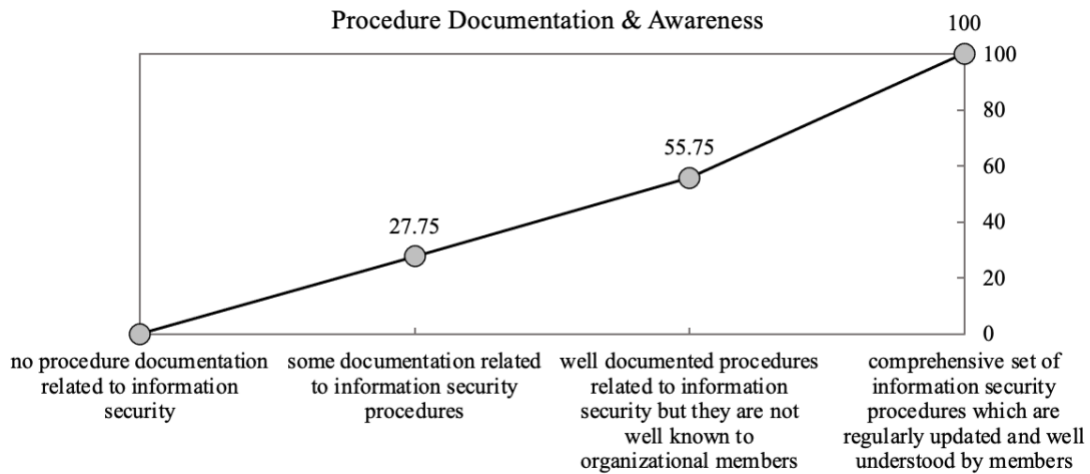
Figure 17: Desirability Curve for Policy Documentation and Awareness Goal



4.4.6 Desirability Curves Associated with Procedure Documentation and Awareness

Information security procedure documentation and awareness metrics consist of measures associated with comprehensiveness of documentation, frequency of procedure review and update and understanding by organizational members of relevant procedures. Experts determined the ideal state as one that included all of these characteristics, with a curve that rose steadily.

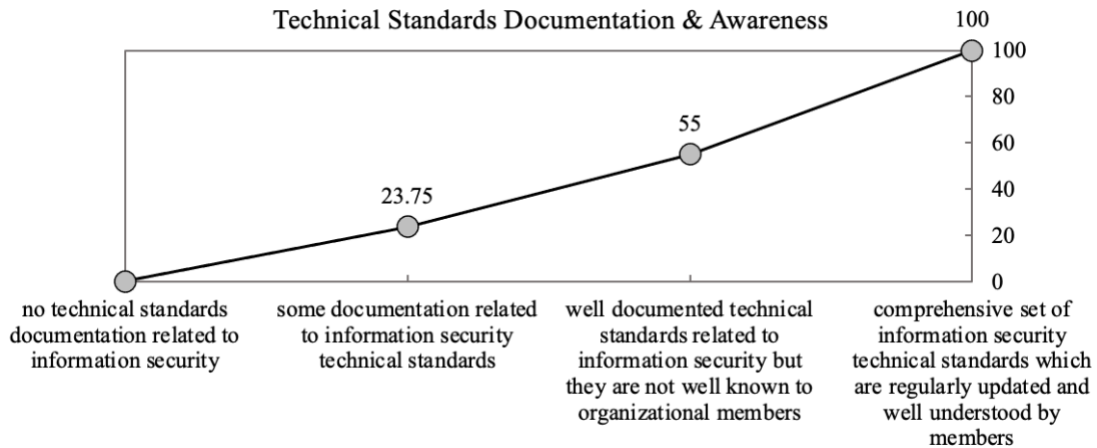
Figure 18: Desirability Curve for Procedure Documentation and Awareness Goal



4.4.7 Desirability Curves Associated with Technical Standards Documentation and Awareness

Information security technical standards documentation and awareness metrics consist of measures associated with comprehensiveness of documentation, frequency of technical standards review and update and understanding by organizational members of relevant standards. Experts determined the ideal state as one that included all of these characteristics, with a curve that rose steadily.

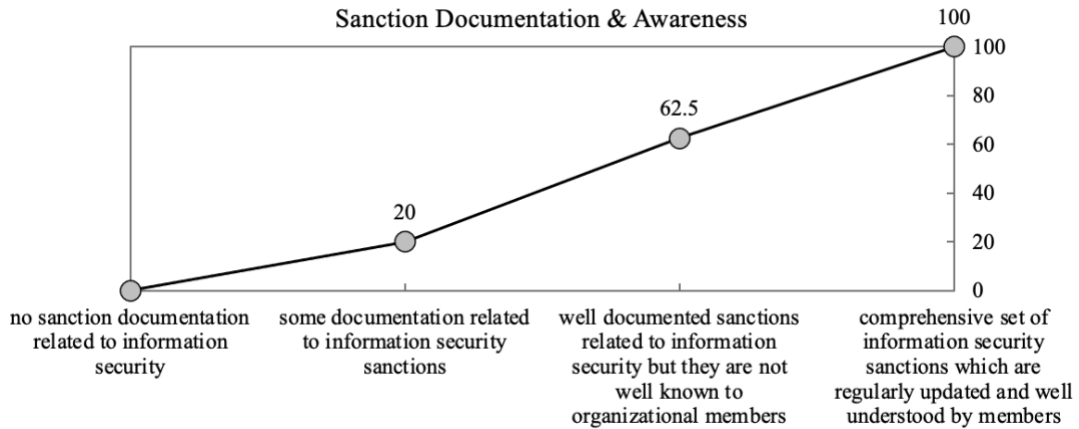
Figure 19: Desirability Curve for Technical Standards Documentation and Awareness Goal



4.4.8 Desirability Curves Associated with Sanction Documentation and Awareness

Information security sanction documentation and awareness metrics consist of measures associated with comprehensiveness of documentation, frequency of documentation review and update and understanding by organizational members of relevant sanctions. Experts determined the ideal state as one that included all of these characteristics, and there is a notable increase in desirability between nodes 2 and 3 where the level of documentation is increased.

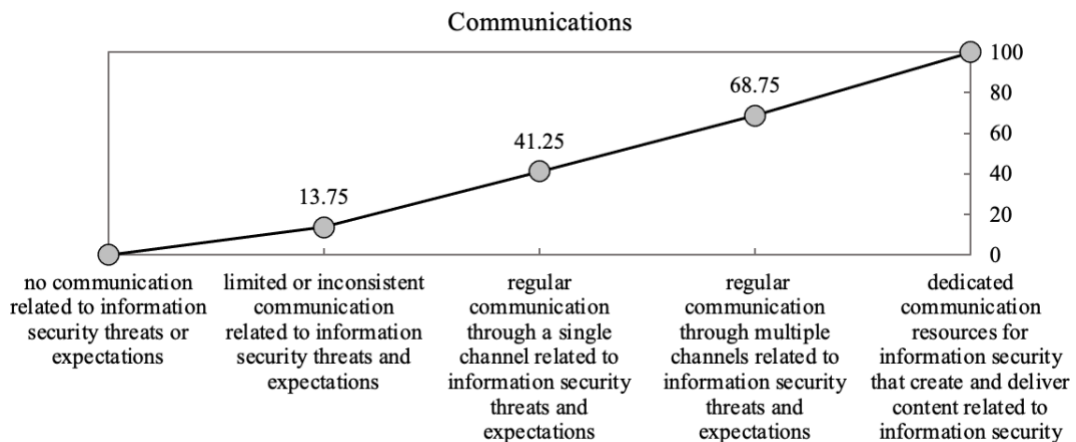
Figure 20: Desirability Curve for Sanction Documentation and Awareness Goal



4.4.9 Desirability Curves Associated with Communications

Information security communication metrics consist of measures associated with channels and frequency of communication and ultimately include resources dedicated specifically to communication related to information security. Experts determined the ideal state as one that included all of these characteristics, with a steadily rising curve.

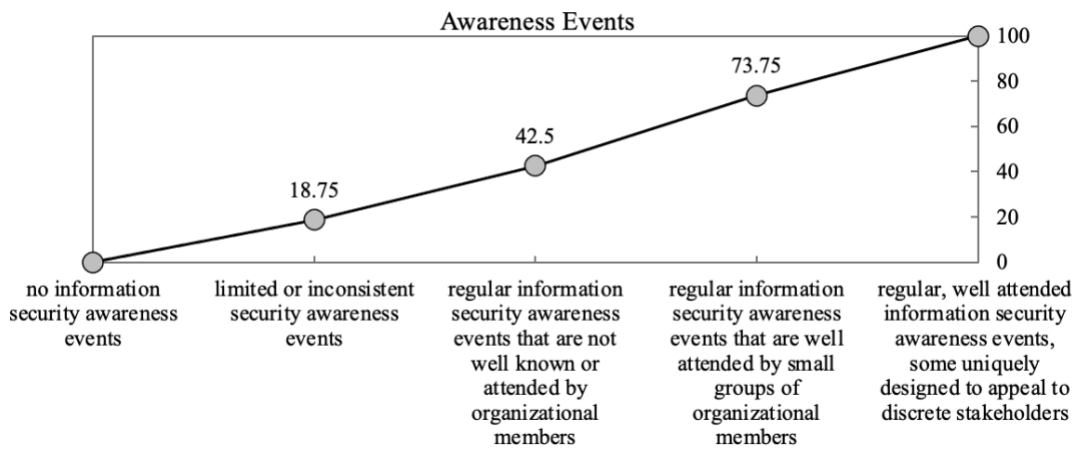
Figure 21: Desirability Curve for Communication Goal



4.4.10 Desirability Curves Associated with Awareness Events

Information security awareness events metrics consist of measures associated with frequency, attendance and variety of events related to information security. Experts determined the ideal state as one that included all of these characteristics, with a steadily rising curve.

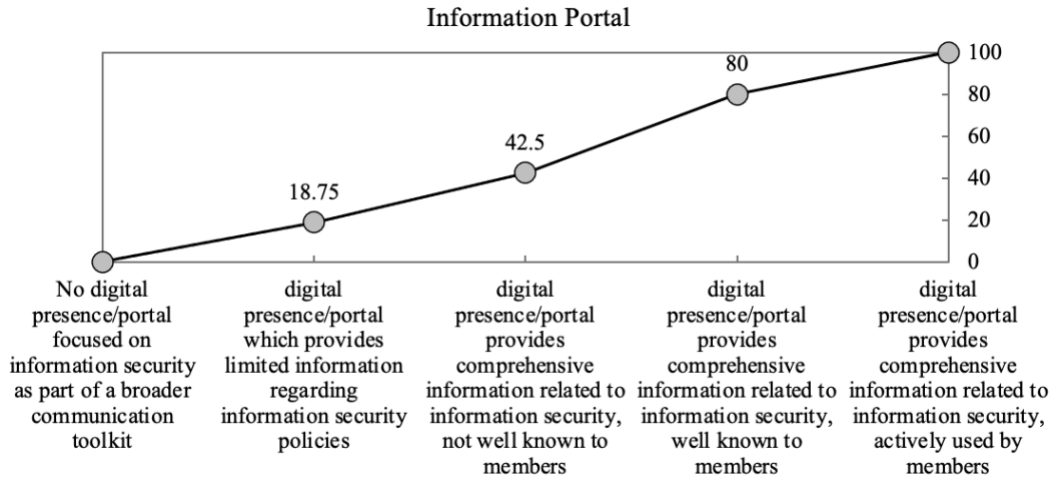
Figure 22: Desirability Curve for Awareness Events Goal



4.4.11 Desirability Curves Associated with Information Portal

Information security portal metrics consist of measures associated with existence, content, awareness and usage related to the portal. Experts determined the ideal state as one that included all of these characteristics, with a notable increase at node 4 where the portal is well known to institutional members.

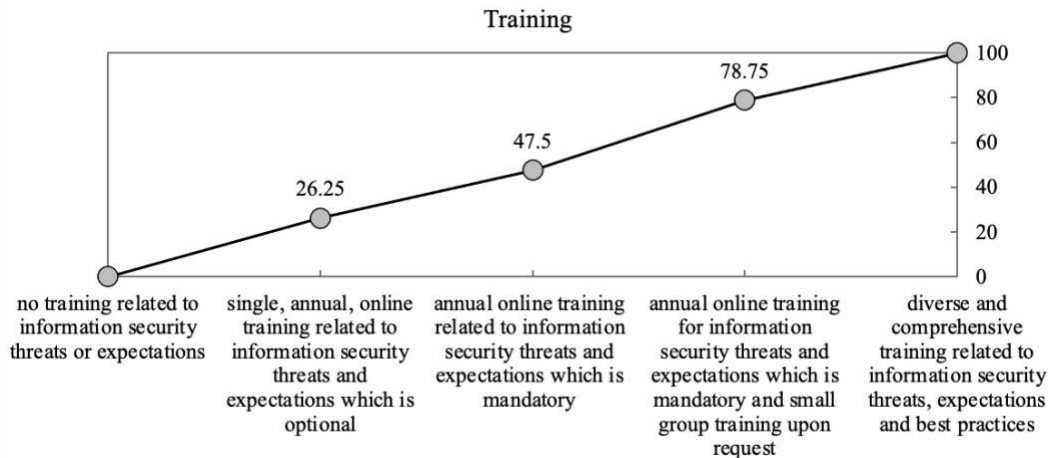
Figure 23: Desirability Curve for Information Portal Goal



4.4.12 Desirability Curves Associated with Training

Information security training metrics consist of measures associated with mode, frequency and diversity of training as well as whether some training is required of all institutional members. Experts determined the ideal state as one that included all of these characteristics, with a steadily rising curve.

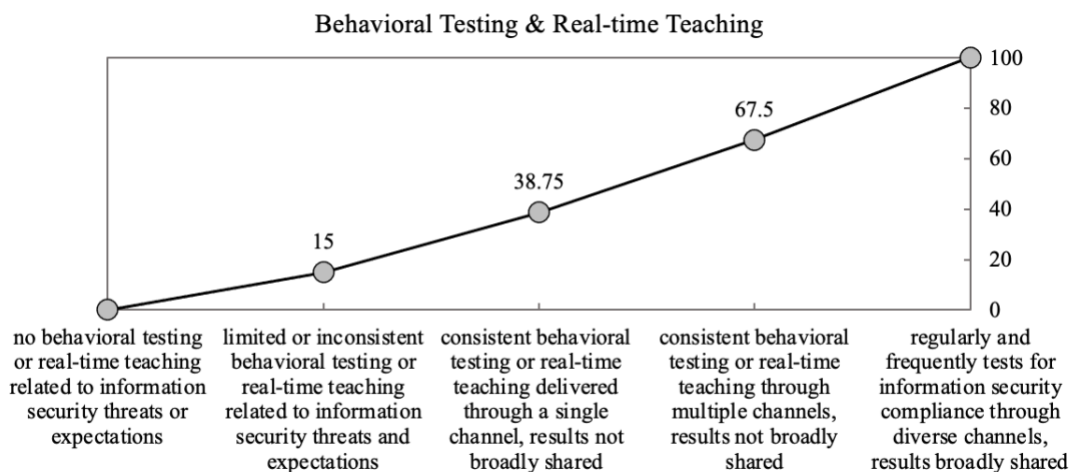
Figure 24: Desirability Curve for Training Goal



4.4.13 Desirability Curves Associated with Behavioral Testing and Real-time Teaching

Information security behavioral testing and real-time teaching metrics consist of the frequency of testing, the sharing of results related to testing and the number of channels used for testing. Experts determined the ideal state as one that included all of these characteristics with a steadily rising curve.

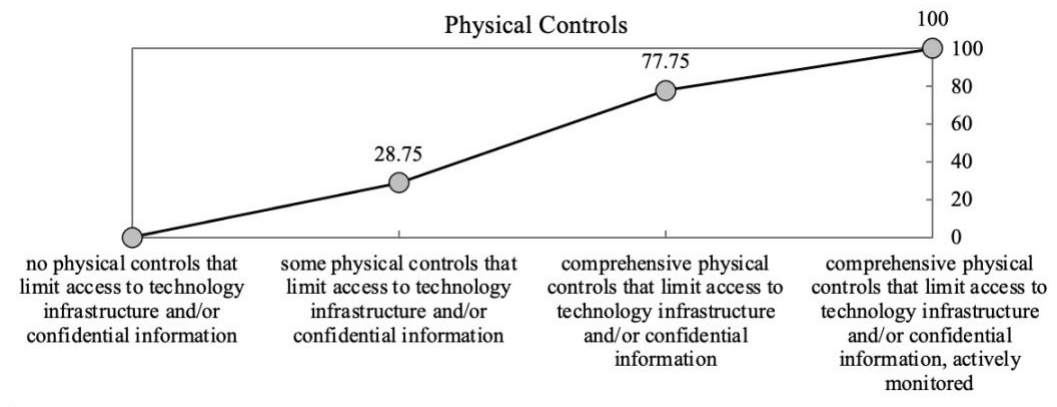
Figure 25: Desirability Curve for Behavioral Testing and Real-time Teaching



4.4.14 Desirability Curves Associated with Physical Controls

Information security physical controls metrics consist of measures associated with degree and monitoring of physical access to technology resources. Experts determined the ideal state as one that included all of these characteristics, with a notable increase in desirability at node 3 where comprehensive physical controls were in place.

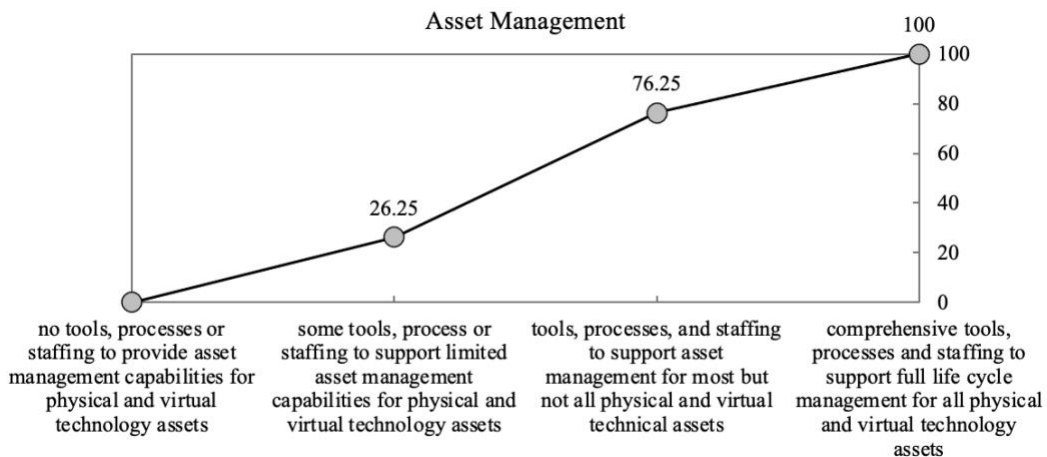
Figure 26: Desirability Curve for Physical Controls Goal



4.4.15 Desirability Curves Associated with Asset Management

Information security asset management metrics consist of measures associated with tools, processes and staffing to support full life cycle management for both physical and virtual assets. Experts determined the ideal state as one that included all of these characteristics, with a notable increase in desirability where most physical and virtual assets are managed.

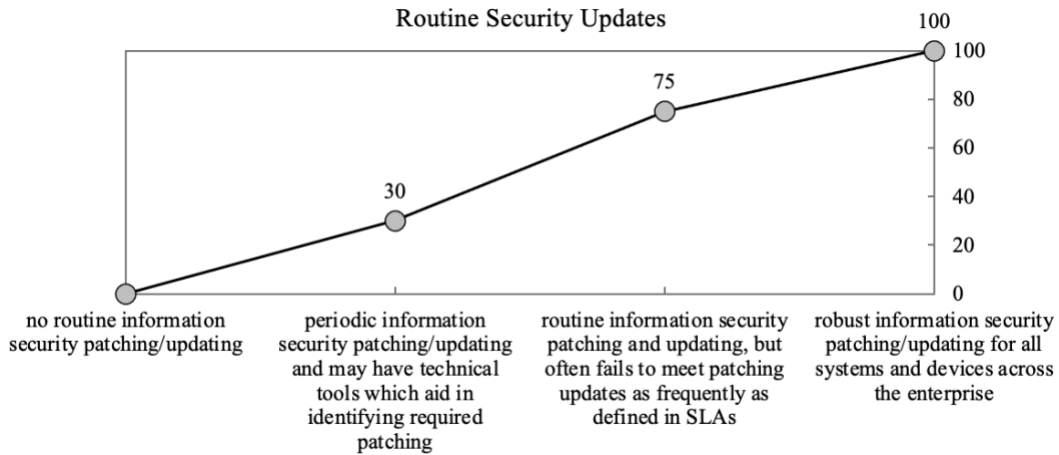
Figure 27: Desirability Curve for Asset Management Goal



4.4.16 Desirability Curves Associated with Routine Security Updates

Information security routine security updates metrics consist of measures associated with frequency of updates as aligned with defined service levels and comprehensiveness of systems updated. Experts determined the ideal state as one that included all of these characteristics, with a notable increase at node 3 where updates are routine even if they don't strictly meet service level agreements.

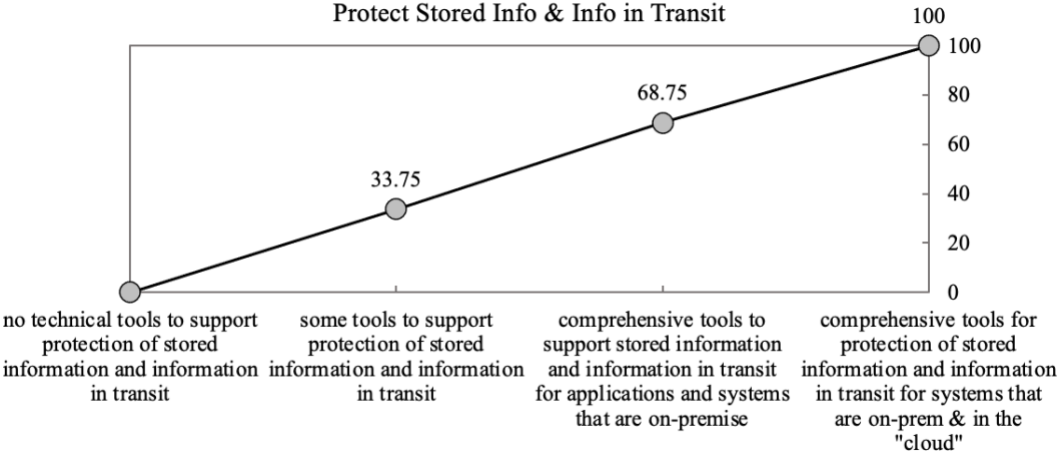
Figure 28: Desirability Curve for Routine Security Updates Goal



4.4.17 Desirability Curves Associated with Protection of Stored Information and Information in Transit

Information security metrics for the protection of stored information or information in transit consist of measures associated with tools utilized to monitor and manage information both on-premise and in cloud-based platforms utilized by the organization. Experts determined the ideal state as one that included all of these characteristics, with a consistent upward curve.

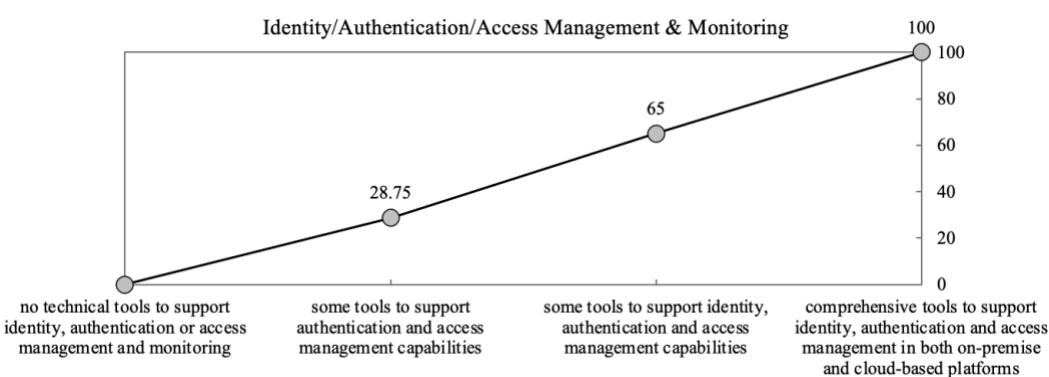
Figure 29: Desirability Curve for Protection of Stored Information and Information in Transit Goal



4.4.18 Desirability Curves Associated with Identity, Authentication, and Access Management and Monitoring

Information security metrics for identity, authentication and access management and monitoring consist of the comprehensiveness of the toolset to manage both on-premise and cloud-based systems. Experts determined the ideal state as one that included all of these characteristics, with a steadily rising curve.

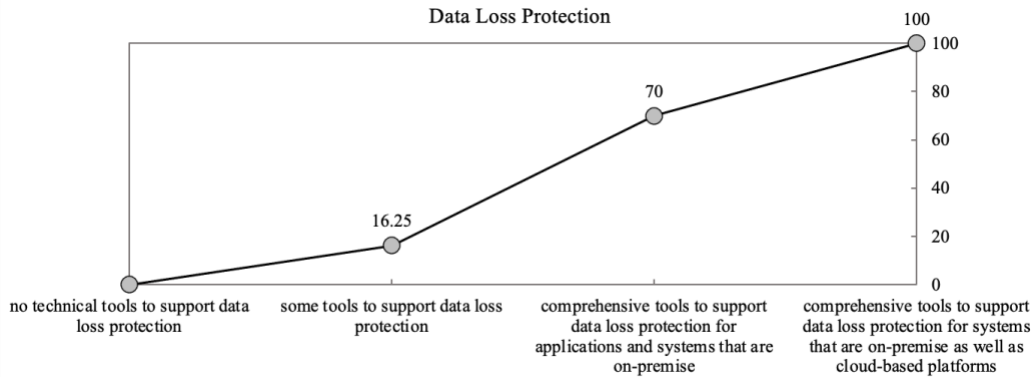
Figure 30: Desirability Curve for Identity, Authentication, and Access Management and Monitoring Goal



4.4.19 Desirability Curves Associated with Data Loss Prevention

Information security metrics for data loss prevention consist of measures associated with tools utilized to monitor and manage data loss both on-premise and in cloud-based platforms utilized by the organization. Experts determined the ideal state as one that included all of these characteristics, with a notable increase at node 3 where a comprehensive toolset for on-premise solutions is available.

Figure 31: Desirability Curve for Data Loss Prevention Goal

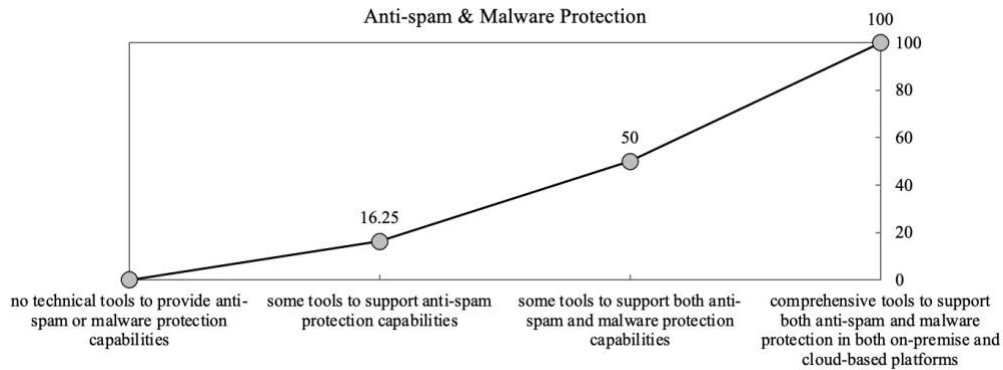


4.4.20 Desirability Curves Associated with Anti-spam and Malware Protection

Information security metrics for anti-spam and malware protection consist of measures related to capabilities of the tools utilized to manage both on-premise and cloud-based platforms utilized by the organization. Experts determined the ideal state as one that included all of these characteristics, with a notable increase at node 4 where comprehensive tools are implemented for both on-premise and cloud-based

platforms. This is unsurprising given the specific threat posed by phishers in the current information security threat landscape.

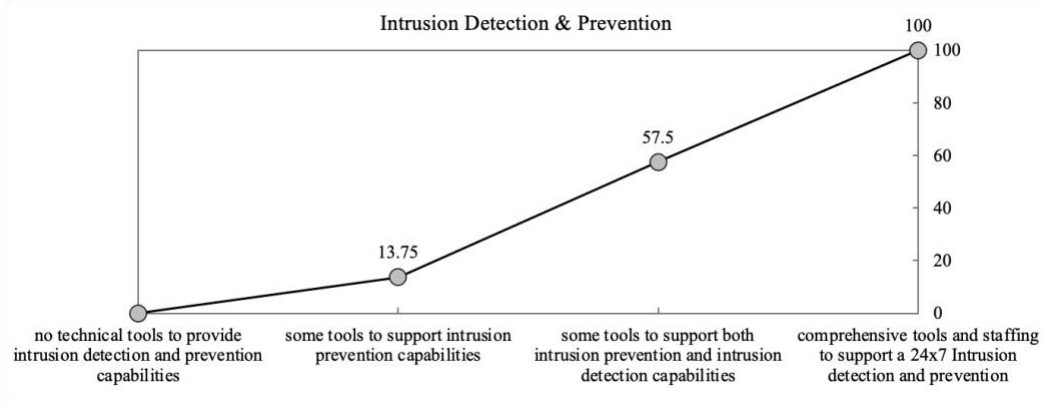
Figure 32: Desirability Curve for Anti-spam and Malware Protection Goal



4.4.21 Desirability Curves Associated with Intrusion Detection and Prevention

Information security metrics for intrusion detection and prevention consist of measures associated with both tools and staffing, including support around the clock. Experts determined the ideal state as one that included all of these characteristics, with a notable increase in desirability at node 3 where the toolset is richer although 24x7 monitoring is not seen.

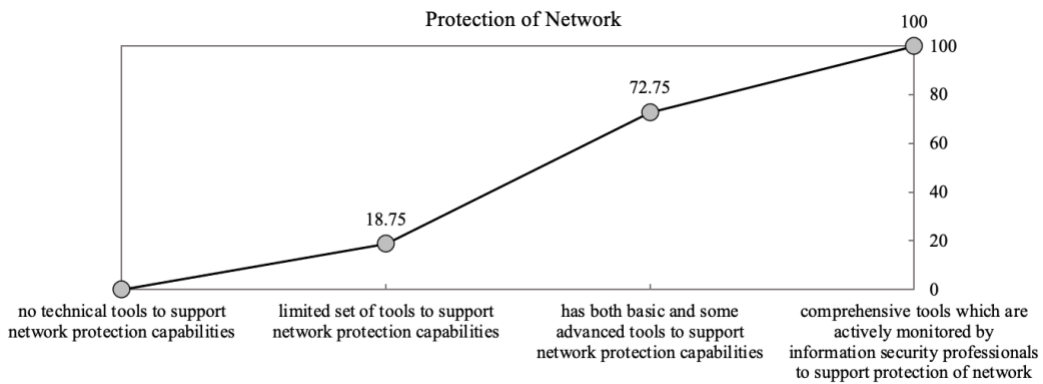
Figure 33: Desirability Curve for Intrusion Detection and Prevention Goal



4.4.22 Desirability Curves Associated with Protection of Network

Information security metrics for protection of network consist of measures associated with both tools and staffing for monitoring. Experts determined the ideal state as one that included all of these characteristics, with a notable increase in desirability at node 3 where the toolset is more diverse although systems may not be routinely monitored.

Figure 34: Desirability Curve for Protection of Network Goal



CHAPTER 5: FINALIZING THE MODEL

The following section discusses the finalization of the generalizable maturity model, beginning with expert validation of the model content and construct, followed by expert quantification of the decision criteria importance and finally establishing weights for model elements. The use of experts in the field of information security, both from a variety of roles as well as diversity of organization type, was a critical component of the development and validation of the model.

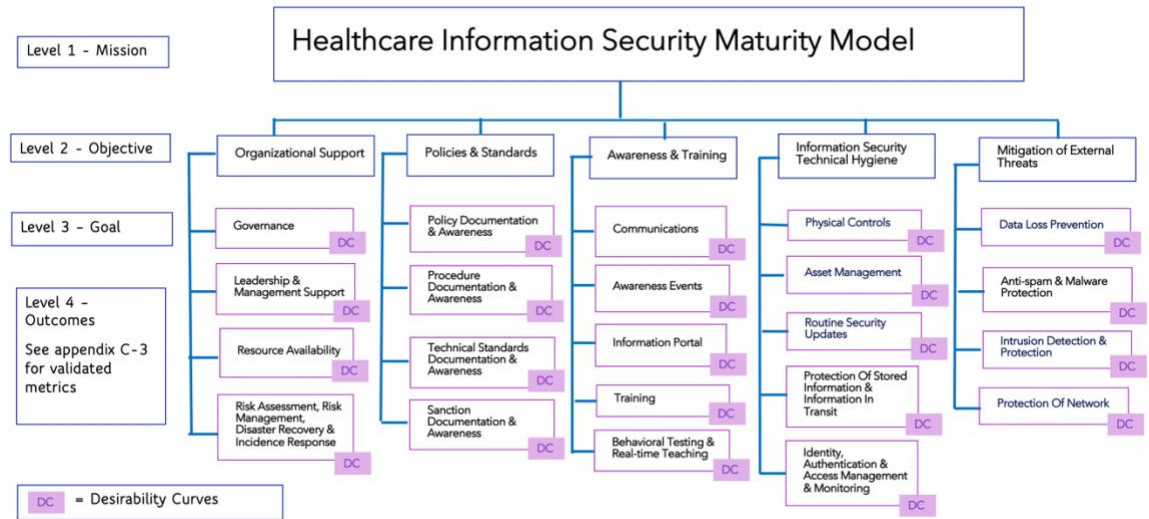
5.1 Model Validation

It is important to select outputs that reflect the desired mission outcome of the model. Objectives, goals and outputs were originally defined based on literature and were then validated and quantified by industry experts. Elements of the model were validated by binary acceptance data (yes/no) and were included in the model at the 80% agreement level [234]. Appendix C shows how 5 objectives (Appendix C-1), twenty-two goals (Appendix C-2), and associated output elements (Appendix C-3) were validated and accepted. The validation of objectives and goals required an iterative process. The initial validation step included 50 expert opinions and the secondary validation step included six experts.

Figure 35 shows how the validated elements were joined to develop a comprehensive model, linked together to develop the HDM. Five objectives fill level

2, twenty-two goals fill level 3, level 4 output details are provided in Appendix C-3 and each goal has an associated desirability curve to complete the model.

Figure 35: Validated HDM



5.2 Quantification of model

The pairwise comparison technique was used for the quantification process for each decision element. Judgment quantification instruments (Appendix A-4) were designed and administered to each panel of experts to collect pairwise comparison information. HDM © 2.0 software was used to collect pairwise comparison data. Raw data tables are available in Appendix D. HDM software was also used to complete inconsistency and disagreement measures.

5.3 Inconsistency

This research utilized the average standard deviation method to measure inconsistency as calculated by the HDM 2.0© software. Inconsistencies at or above

the tolerance threshold of 10% were further examined under the lens of research conducted by Abbas [235], who found that the 10% threshold limit was increasingly conservative as the number of decision elements increase from the range of three elements to twelve elements.

Two experts demonstrated a moderate inconsistency measurement when providing pairwise comparison judgments at the objective level of the model. Figure 36 shows that expert 8 has an inconsistency value of 0.11, and expert 24 is at the threshold of .10.

Figure 36: Inconsistent expert data

Expert	Org Support	Policies & Standards	Awareness & Training	Technical Hygiene	External Threats	Inconsistency
E1	0.17	0.1	0.29	0.24	0.2	0.01
E2	0.19	0.12	0.25	0.26	0.18	0.02
E3	0.19	0.12	0.19	0.29	0.2	0.02
E4	0.2	0.16	0.15	0.18	0.31	0.04
E5	0.27	0.07	0.2	0.16	0.3	0.01
E6	0.23	0.14	0.18	0.27	0.18	0.01
E7	0.27	0.14	0.17	0.2	0.22	0.01
E8	0.16	0.03	0.12	0.28	0.4	0.11
E9	0.13	0.2	0.18	0.22	0.27	0.02
E10	0.08	0.15	0.2	0.27	0.29	0.03
E11	0.17	0.21	0.24	0.16	0.21	0.02
E12	0.19	0.12	0.16	0.27	0.27	0
E13	0.1	0.14	0.21	0.23	0.33	0.02
E14	0.13	0.1	0.12	0.34	0.32	0.03
E15	0.17	0.13	0.24	0.24	0.21	0.02
E16	0.25	0.18	0.16	0.21	0.21	0
E17	0.21	0.08	0.16	0.28	0.27	0.09
E18	0.19	0.13	0.11	0.26	0.31	0.01
E19	0.18	0.14	0.27	0.15	0.27	0.03
E20	0.23	0.1	0.18	0.34	0.15	0.01
E21	0.18	0.12	0.28	0.14	0.28	0.06
E22	0.17	0.17	0.18	0.23	0.25	0
E23	0.3	0.15	0.15	0.25	0.15	0.1
E24	0.21	0.17	0.2	0.24	0.19	0.02
E25	0.14	0.13	0.18	0.4	0.16	0.02
E26	0.23	0.08	0.19	0.27	0.23	0.01
E27	0.18	0.17	0.21	0.22	0.22	0.05
E28	0.2	0.2	0.2	0.2	0.2	0
E29	0.22	0.18	0.15	0.25	0.2	0
Mean	0.19	0.14	0.19	0.24	0.24	
Minimum	0.08	0.03	0.11	0.12	0.15	
Maximum	0.3	0.21	0.29	0.4	0.4	
Std. Deviat	0.05	0.04	0.05	0.06	0.06	
Disagreement						0.048

The decision variables in this case include the five different objective elements: organizational support, policies and standards, awareness and training, technical hygiene and mitigation of external threats. Abbas found the 10% threshold to be quite conservative when experts were asked to make comparative judgment involving 5 elements [235]. Therefore, the data for experts 8 and 24 were accepted into the study as they were either at or near the .10 threshold.

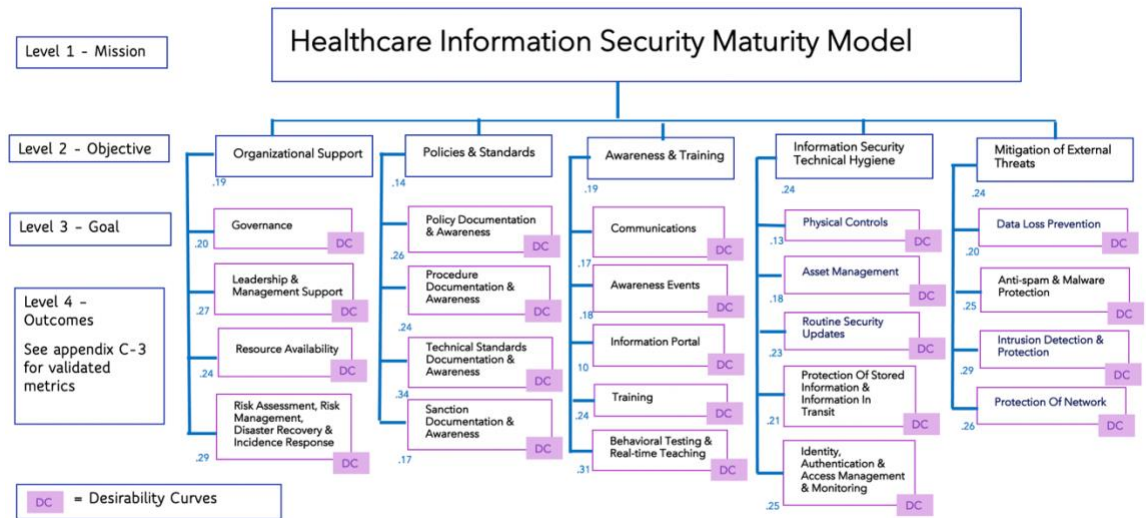
5.4 Disagreement Analysis

While experts may disagree for many reasons as noted in Chapter 3. Disagreement levels were below the 0.10 threshold [195][225] using the HDM 2.0© software; therefore no further action was taken. If disagreement had been found experts may have been asked to repeat judgement in order to ascertain whether disagreement might decrease to acceptable levels.

5.5 Finalized HDM

Figure 37 shows the finalized validated model with decision element weights as derived from expert feedback.

Figure 37: Generalizable model for healthcare information security maturity



It is no surprise that the two technically focused objectives, information security hygiene and mitigation of external threats given the generally technical nature of the of the topic and the proliferation of tools to aid in the projection of information. These results reinforce the technical focus of existing information security models. This model does however provide a different perspective on the importance of training and organization support elements, which are rarely quantified in other information security frameworks. Further discussion is presented in Chapter 7.

CHAPTER 6: CASE STUDIES

Case studies were conducted to illustrate how the model works and to validate model elements as to the degree which the model reflects actual performance. Data were acquired from five healthcare organizations by means of a data collection instrument to populate the metrics, identifying those outputs for each organization and aligning with the respective desirability values to create a score for each case study site. Analysis of results were presented to experts for feedback. This chapter is organized in four sections:

Section 1 Broad description of five healthcare organization types included in case studies and a brief introduction of each case study site with specific identification information removed to protect confidentiality of the participant site;

Section 2 Illustration of how data was collected and used to calculate a maturity model score for a single case study site;

Section 3 Review of performance evaluation for all case study sites including strengths and suggested areas for improvement;

Section 4 Discussion of sensitivity analysis of model, assessing the impact of changes at the objective level to test the robustness of the model.

6.1 Healthcare organization selection

Healthcare organization come in many different sizes and shapes. In order to test the model for generalizability a variety of different organization types and sizes were selected for case study inclusion. The following organization types were included in the case studies:

- Critical Access Hospital – Critical Access Hospital is a designation given to eligible rural hospitals by the Centers for Medicare and Medicaid Services (CMS). The designation is designed to increase access to healthcare for rural communities and reduce the financial vulnerability of these sites. Critical Access Hospitals have 25 or fewer acute care inpatient beds, are located 35 miles from another hospital, and provide 24/7 emergency care services.
- Stand-alone Community Hospital - Stand-alone community hospitals are generally the sole or predominant healthcare provider in the market they serve. They are independent and are not aligned to any larger health system. These community hospitals are generally closely aligned with local physician groups.
- Integrated Delivery Network (IDN) – An integrated delivery network is a system of healthcare facilities and providers that offer both healthcare services as well as healthcare insurance plans to a defined patient population which may, or may not, be a related to a specific

geographic area. They vary greatly in size (number of facilities, providers, patients served).

- Large Healthcare System – A healthcare system is a collection of facilities and providers, who may or may not be employed by the healthcare facility, who work together to deliver a variety of healthcare services. Unlike the IDN noted above the healthcare system does not explicitly offer healthcare care insurance plans. In this case, large is defined as greater than one hospital and over 500 inpatient beds.
- Academic Medical Center – Academic medical centers are universities that teach medical students and include one or more hospitals as well as provider practice plans to provide hands-on experience to their students as well as graduate medical education training. Academic medical centers provide a wide range of healthcare services for patients and often include cutting edge research capabilities.

The Chief Information Officer was contacted at each potential case study site to ascertain their interest and ability to participate in the study. These decision makers and experts were able to respond to the data collection instrument and in one case asked if they could include other information security experts within their organization in the process to ensure accuracy of response. Those additional experts were happily included. Table 7 provides a summary of key demographics [262] associated with each case study site for 2020.

Table 7: Summary of Key Demographics for Case Study Sites

Site	Employees	Licensed Beds	Outpatient Clinics	Inpatient Days	Outpatient visits	Emergency Visits	Gross Patient Revenue
Critical Access Hospital	750	25	12	4,000	74,000	14,000	\$170M
Stand-Alone Community Hospital	1,500	176	unknown	18,000	unknown	30,000	\$640M
Integrated Delivery Network	6,000	330	80	60,000	unknown	unknown	\$1.8B
Large Health System	14,000	1,250	unknown	320,000	unknown	unknown	\$2.4B
Academic Medical Center	18,500	549	100	170,000	1,000,000	30,000	\$4.6B

A more specific description of each case study site is provided below, although the information is anonymized to protect that site’s confidentiality.

6.1.1 Critical Access Hospital (CAH)

The case study site has been rated one of the top 100 Critical Access Hospitals in the nation by the Chartis Group many times in the past decade. Serving their rural community for over 100 years, they are committing to ensuring those they support thrive.

6.1.2 Stand-alone community hospital

The case study site is a community owned, non-profit community hospital. It is characterized as a social and economic asset focused on serving its local community. Serving more than 80,000 individuals, it is the only hospital in a 10,000 square mile area and serves as a teaching hospital.

6.1.3 Integrated Delivery Network (IDN)

The case study site is a not-for-profit network of five hospitals, numerous clinics and health plan services serving more than 250,0000 members in their

community. It is characterized as a social and economic asset, as one of the community's largest employers and is focused on serving local communities.

6.1.4 Large health system

The case study site is a locally owned not-for-profit network of seven hospitals and numerous clinics serving both urban and rural communities. It is characterized by a high level of specialty care services, including a level 1 trauma center. It serves as a key social and economic asset to the community as one of the largest employers in the region.

6.1.5 Academic medical center

The case study site is a public non-profit serving all citizens of the state. It is characterized not only for teaching the next generation of healthcare professionals but also a site providing access to state-of-the-art healthcare including clinical trials. As the largest employer in their city, they are a key economic engine for not only the city but also the state through their tri-part mission of teaching, healing and discovery.

6.2 Illustration case: Stand-alone community hospital (SACH)

The stand-alone community based hospital case study is used to illustrate how the data were collected and the metrics were populated to create a score for the health information security maturity model. The SACH was selected as the case study because community hospitals are generally less resource rich when it comes to

support for information security. They are vulnerable to cybercriminals as a result of historic lack of investment in information security by healthcare organizations and are in need of a tool that can help them prioritize their scarce resources.

The data collection approach utilized an instrument that was designed and administered by the researcher by way of an interview with the Chief Information Officer at the case study site. The data collection instrument is available in Appendix F-1.

6.2.1 Maturity assessment score

The results of the maturity score for this case study are presented in Table 8 below.

Table 8: Maturity Assessment Score for Stand-alone Community Hospital

Perspective	O Weight	Criteria	Local W	Global W	D score	Score= GW*D
Organizational Support	0.19	Governance	0.20	0.04	0.64	0.02
		Leadership & Management Support	0.27	0.05	0.65	0.03
		Resource Availability	0.24	0.05	0.80	0.04
		Risk Assessment, Risk Mgmt, DR, and IR	0.29	0.06	0.55	0.03
Policies & Standards	0.14	Policy Documentation & Awareness	0.26	0.04	0.58	0.02
		Procedure Documentation & Awareness	0.24	0.03	0.28	0.01
		Technical Standards Doc & Awareness	0.34	0.05	0.24	0.01
		Sanction Documentation & Awareness	0.17	0.02	1.00	0.02
Awareness & Training	0.19	Communications	0.17	0.03	0.69	0.02
		Awareness Events	0.18	0.03	0.74	0.03
		Information Portal	0.10	0.02	0.19	0.00
		Training	0.24	0.05	0.79	0.04
		Behavioral Testing & Real-time Teaching	0.31	0.06	0.68	0.04
Technical Hygiene	0.24	Physical Controls	0.13	0.03	0.78	0.02
		Asset Management	0.18	0.04	0.26	0.01
		Routine Security Updates	0.23	0.06	0.75	0.04
		Protection of Store Info & Info in Transit	0.21	0.05	0.69	0.03
		Identity, Authentication, Access Mgmt	0.25	0.06	0.65	0.04
Mitigation of External Threats	0.24	Data Loss Prevention	0.20	0.05	0.70	0.03
		Anti-spam & Malware Protection	0.25	0.06	1.00	0.06
		Intrusion Detection & Protection	0.29	0.07	0.58	0.04
		Protection of Network	0.26	0.06	0.73	0.05
						0.65

6.2.1 Strengths and Opportunities for Improvement

The assessment provides a concise view of the strengths and opportunities for improvement at the stand-alone community hospital. These strengths and opportunities are presented in Table 9 below where strengths are highlighted in green, where score value as a percent of optimal value is 75 or higher, and opportunities are highlighted in yellow where score value as a percent of optimal value is less than 60.

Table 9: Strengths and Opportunities for Stand-alone Community Hospital

Perspective	O Weight	Criteria	Local W	Global W	D score	Score= GW*D	Score Value as a % of Optimal Score Value
Organizational Support	0.19	Governance	0.20	0.04	0.64	0.02	64%
		Leadership & Management Support	0.27	0.05	0.65	0.03	65%
		Resource Availability	0.24	0.05	0.80	0.04	80%
		Risk Assessment, Risk Mgmt, DR, and IR	0.29	0.06	0.55	0.03	55%
Policies & Standards	0.14	Policy Documentation & Awareness	0.26	0.04	0.58	0.02	58%
		Procedure Documentation & Awareness	0.24	0.03	0.28	0.01	28%
		Technical Standards Doc & Awareness	0.34	0.05	0.24	0.01	24%
		Sanction Documentation & Awareness	0.17	0.02	1.00	0.02	100%
Awareness & Training	0.19	Communications	0.17	0.03	0.69	0.02	69%
		Awareness Events	0.18	0.03	0.74	0.03	74%
		Information Portal	0.10	0.02	0.19	0.00	19%
		Training	0.24	0.05	0.79	0.04	79%
Technical Hygiene	0.24	Behavioral Testing & Real-time Teaching	0.31	0.06	0.68	0.04	68%
		Physical Controls	0.13	0.03	0.78	0.02	78%
		Asset Management	0.18	0.04	0.26	0.01	26%
		Routine Security Updates	0.23	0.06	0.75	0.04	75%
		Protection of Store Info & Info in Transit	0.21	0.05	0.69	0.03	69%
Mitigation of External Threats	0.24	Identity, Authentication, Access Mgmt	0.25	0.06	0.65	0.04	65%
		Data Loss Prevention	0.20	0.05	0.70	0.03	70%
		Anti-spam & Malware Protection	0.25	0.06	1.00	0.06	100%
		Intrusion Detection & Protection	0.29	0.07	0.58	0.04	58%
		Protection of Network	0.26	0.06	0.73	0.05	73%

The table highlights how the model was able to capture discrete attributes that contribute to, or detract from, overall information security maturity. In addition, it is clear how much those elements matter in the overall maturity score.

In this case study, the stand-alone community hospital scores well in resource availability, sanctions documentation and awareness, training, physical controls, routine security updates, and anti-spam and malware protection. Of note, resource availability with an optimal value of .24, training with an optimal value of .24, routine security updates with an optimal value of .23, and anti-spam and malware protection with an optimal value of .25 are high value elements within the model and ultimately lead to an improved score in overall maturity score when compared with lesser value

elements. This value is increased further as the objective level values for technical hygiene, associated with physical controls and routine security updates, has an optimal value of .24. The same is true for the optimal level value for mitigation of external threats, associated with anti-spam and malware protection, at .24.

Moving to opportunities for improvement, it is shown that the stand-alone community hospital does not score as well in risk assessment, risk management, disaster recovery and incident response with an optimal value of .29, procedure documentation and awareness, with an optimal value of .24, technical standards documentation and awareness with an optimal value of .34, information portal with an optimal value of .10, asset management with an optimal value of .18 and intrusion detection and prevention, with an optimal value of .29. This is less concerning as it relates to procedure documentation and awareness and technical standards documentation and awareness since the associated policies and standards objective level optimal value is .14, and therefore of less overall impact to the total score. The same is true with a low score associated with information portal given the relatively low optimal value of .10 with and associated optimal goal value of .19 for awareness and training. Making improvements to intrusion detection and prevention, with an optimal value of .29 and an optimal objective value of .24 for mitigation of external threats, asset management, with an optimal value of .18 and an optimal objective value of .24 for technology hygiene, and risk assessment, risk management, disaster recovery, and incident response, with an optimal value of .29 and an associated

optimal objective level value of .19 for organizational support would be good areas of focus to improve the overall maturity score.

These findings were presented to the local expert. The expert agreed with the recommendations and further indicated that enhancing intrusion detection and prevention was a current high priority program of work at the case study site in order to improve their information security environment. The expert further disclosed that the case study organization had been a recent victim of a cyberattack and that lack of an established intrusion detection and prevention program was a significant factor in the damaging impact of the event on the organization.

6.3 Comparative Analysis Across All Case Study Sites

As noted earlier a total of five case study maturity model scores were performed. Comparing information security performance across organizations is fairly rare given the high stakes associated with acknowledging information security vulnerabilities. It is well known that what we measure matters, and where we measure we have the opportunity to improve. Measurement helps us not only identify opportunities for improvement but also permits organizations that routinely participate in benchmarking with peers to better understand how they are doing when compared with others.

A side-by-side comparison of maturity model scores, with details associated with each element of the HDM is available in Appendix F-2. A summary of the health information security maturity model scores is provided below in Table 10.

Table 10: Maturity Scores for Case Study Sites

Critical Access Hosp Maturity Score	Stand Alone Comm Hosp Maturity Score	Integrated Delivery Network Maturity Score	Large Healthcare System Maturity Score	Academic Medical Center Maturity Score
0.47	0.65	0.94	0.57	0.80

It is evident from the case study maturity scores that there is great variety in the maturity of health information security across organizations. Investment in information security varies greatly across organizations, and it is unsurprising that the organization that is least likely to have access to critical resources to support a robust information security environment (Critical Access Hospital) has a lower maturity rating than organizations that generally have greater access to resources (Integrated Delivery Network). The scores are not intended to represent “good” or “bad” or “winners” or “losers”. Rather they should be used to identify opportunities of focus for utilization of scarce resources.

A closer look at the greatest strengths and most telling weaknesses of each site, as illustrated in Table 11 below, again shows great variety across sites.

Table 11: Key Maturity Scores for Case Study Sites

Case Study Site	Factor	Score Value as % of Optimal Value
Critical Access Hospital		
Strengths	Training	78%
	Governance	76%
Opportunities	Behavioral Testing and Real-time teaching	15%
	Intrusion detection & prevention	14%
Stand Alone Comm Hosp		
Strengths	Anti-spam & malware protection	100%
	Sanctions documentation & awareness	100%
Opportunities	Asset management	26%
	Technical standards documentation	24%
Integrated Delivery Network		
Strengths	Intrusion detection & prevention*	100%
	Policies & standards*	100%
Opportunities	Awareness events	74%
	Behavioral Testing and Real-time teaching	68%
Large Healthcare System		
Strengths	Risk assessment, risk mgmt, disaster recover, Incident response	84%
	Resource availability	80%
Opportunities	Asset management	26%
	Awareness events	25%
Academic Medical Center		
Strengths	Leadership & Management Support**	100%
	Training	100%
Opportunities	Asset management	26%
	Awareness events	25%

The variety shown above may be caused by several factors. Cost of some solutions may be higher than others. Some solutions will be easier to implement than others. Lack of frameworks which measure the importance of the factors related to creating a mature information security environment may have led to a less focused approach on which measures provide the greatest value. In any case, these baseline scores provide a framework to measure performance in a quantified way going forward. Information security choices are complex and the output of the health

information model should not serve as a laundry list of things to do, but instead as a tool that can be used for further analysis to prioritize high value work that could contribute to improving overall maturity in information security. Further analysis of the scores at each case study site allows for specific recommendation for each site. Sharing scores with peers, if conducted in a confidential manner, could provide an opportunity to share best practices and lessons learned. During the case study process one site suggested the model could be used by a group of regional peers at one of their periodic meetings to facilitate a discussion of this kind.

6.4 Sensitivity Analysis

Many decisions change over time as they are dependent on a given point in time and current conditions. This is certainly true in the constantly evolving information security landscape. As a result, the model's validity and quality could change in response to environment factors. In recent years the technical perspectives of information security have changed as threats shifted from lone cyber mischief makers to complicated and extremely skilled networks of cybercriminals. The technologies that are used to wage cyberthreat response have changed considerably in cost and capability as well. Organizational support too has received increasing attention as nefarious cyber activity causes significant financial and reputational harm, gaining the attention of organizational Boards of Directors. All these and other factors, move like ocean waves influencing the beach of the information security landscape.

There are different methods that can be used to conduct sensitivity analysis. In this case, scenario analysis is used where a change in relative importance at the objective level of the model is tested. This type of analysis helps decision makers understand how much the model depends on input factors [263]. In the field of technology management, due to the generally dynamic nature of change within the field, scenario analysis has been used to determine the potential impact of a change of importance of objectives as a way to ensure the robustness of the model and associated results [195][241].

Looking again at the stand-alone community hospital case study, the calculated maturity score was used as a baseline and then five extreme scenarios were applied to the model. In each of the five extreme scenarios, a maximum weight was given to each respective objective level element and then the case study's maturity level is recalculated based on the new weight structure within the model. In other words, one objective is given a weight of 96% and each of the other objectives in the model are given a weight of 1%. Table 12 below provides a visual representation of the reallocation of weights.

Table 12: Reallocated Model Weights for Scenario Analysis

Scenarios Focus	Organizational Support	Policies & Standards	Awareness & Training	Technical Hygiene	Mitigation of External Threats
Baseline	0.19	0.14	0.19	0.24	0.24
Organizational Support	0.96	0.01	0.01	0.01	0.01
Policies & Standards	0.01	0.96	0.01	0.01	0.01
Awareness & Training	0.01	0.01	0.96	0.01	0.01
Technical Hygiene	0.01	0.01	0.01	0.96	0.01
Mitigation of External Threats	0.01	0.01	0.01	0.01	0.96

In the case of the stand-alone community hospital, the overall maturity score is significantly harmed when increased emphasis is placed on the policies and standards objective. This makes sense, as the organization’s performance at the metric level within that objective is quite poor. Their overall maturity score increases materially under the scenario where mitigation of external threats is emphasized. A summary of the SACH’s maturity scores under each scenario is provided in Table 13 below. The comprehensive scenario analysis results for the SACH are provided in Appendix G.

Table 13: Summary Results of Scenario Analysis for Stand-alone Community Hospital

Scenarios Focus	Organizational Support	Policies & Standards	Awareness & Training	Technical Hygiene	Mitigation of External Threats	Maturity Score	Change
Baseline	0.19	0.14	0.19	0.24	0.24	0.65	0
Organizational Support	0.96	0.01	0.01	0.01	0.01	0.65	0.01
Policies & Standards	0.01	0.96	0.01	0.01	0.01	0.48	-0.17
Awareness & Training	0.01	0.01	0.96	0.01	0.01	0.66	0.02
Technical Hygiene	0.01	0.01	0.01	0.96	0.01	0.63	-0.02
Mitigation of External Threats	0.01	0.01	0.01	0.01	0.96	0.74	0.09

CHAPTER 7: DISCUSSION

In this chapter, the results of the model development as related to the problem statement are discussed as well as practical implications of findings. In addition, the generalizability of the model is analyzed. Expert feedback responses during the model validation process support concerns identified in literature regarding severity of threat and need for prioritization of cybersecurity strategies given limited resources. Subject matter experts were in agreement of the validity of model.

As noted in the problem statement, an easy to use, generalizable model, that provides a holistic set of metrics with performance scores for information security maturity is much needed. This tool must identify the common criteria that impact the maturity of healthcare organization's information security environments, directly impacting their ability to ensure the confidentiality, integrity and availability of the systems they rely upon to continue business operations. The directional information provided by such a model could be used to facilitate decisions about where healthcare organizations can best utilize their finite resources. In addition the tools will help organizations measure their maturity, and associated effectiveness, over time.

As part of the gap analysis, research gaps 1 and 2 specifically, it was discussed that the criteria for assessing information security in healthcare organizations is not organized in a way that identifies the most important risk mitigation actions, nor is there a single quantified, validated, multi-dimensional, and reusable way of assessing

information security in healthcare organizations that produces a score. Discussion with experts from each of the validation and quantification panels confirmed these findings.

7.1 Research and Practical Implications

The research validated the decision criteria and relative linkages for each criterion consistent with information gleaned from the literature review. One of the interesting findings is that while the research shows the importance of all criteria in the model, it specifically identifies the criteria that hold a greater level of importance, through a higher ranked weighted value. The results also confirm that technology solutions alone are not enough to create a mature information security environment.

In the remainder of this section, each of the top five weighted criteria will be reviewed. Interestingly, one of the criteria within those noted as top five was introduced to the model as a result of the expert validation and quantification process. This highlights the importance of expert feedback during the model development process. Finally, it is worth noting that the model elements were fine-tuned during the validation and quantification process, new elements were added to the model and clarification was provided to the definition for many elements. Table 14 provides a visual representation of all model criteria by weight, calling out the top 5, the bottom 5 and those criteria that were added to the model as a result of expert feedback through the quantification and validation process.

Table 14: Model Elements by Weight

Objective	Criteria	Global W
Mitigation of External Threats	Intrusion Detection & Protection	0.0696
Mitigation of External Threats	Protection of Network	0.0624
Technical Hygiene	Identity, Authentication, Access Mgmt	0.06
Mitigation of External Threats	Anti-spam & Malware Protection	0.06
Awareness & Training	Behavioral Testing & Real-time Teaching	0.0589
Technical Hygiene	Routine Security Updates	0.0552
Organizational Support	Risk Assessment, Risk Mgmt, DR, and IR	0.0551
Organizational Support	Leadership & Management Support	0.0513
Technical Hygiene	Protection of Store Info & Info in Transit	0.0504
Mitigation of External Threats	Data Loss Prevention	0.048
Polices & Standards	Technical Standards Doc & Awareness	0.0476
Organizational Support	Resource Availability	0.0456
Awareness & Training	Training	0.0456
Technical Hygiene	Asset Management	0.0432
Organizational Support	Governance	0.038
Polices & Standards	Policy Documentation & Awareness	0.0364
Awareness & Training	Awareness Events	0.0342
Polices & Standards	Procedure Documentation & Awareness	0.0336
Awareness & Training	Communications	0.0323
Technical Hygiene	Physical Controls	0.0312
Polices & Standards	Sanction Documentation & Awareness	0.0238
Awareness & Training	Information Portal	0.019
Top 5		
Bottom 5		
Elements that were introduced via the validation and quantification process		

7.1.1 Top Rated Criteria – Intrusion Detection and Prevention

The most important element of the model based on expert panel quantification is intrusion detection and prevention, and is defined as a “24x7 intrusion detection and prevention (a.k.a. Managed Detection Response) program utilizing Security Information and Event Management (SIEM) tools” based on both literature review as well as expert feedback. As noted earlier, this specific element was added to the model as a result of expert feedback. It is not surprising that this criterion ranked

highly as external cyber threats have grown in frequency and negative impact. The importance of proactive cyberthreat intelligence is noted by Khan et al. [264] in their proposal for augmented threat intelligence.

7.1.2 Top Rated Criteria – Protection of Network

The second highest rated element of the model based on expert panel quantification is protection of network, and is defined as “technical tools that minimize threats from outside the network (e.g. network access control, network segmentation, firewalls, routine vulnerability scanning)” based on both literature review as well as expert feedback. As with intrusion detection and prevention, protection of network is focused on limiting access to an organization’s network and further securing known vulnerabilities within the network. The importance of network protection was highlighted in Wang’s [265] work promoting artificial intelligence solutions in this space. The high rating received by this element is also likely related to the recent increase in frequency and negative impact of external actors.

7.1.3 Top Rated Criteria – Identity, Authentication, and Access Management and Monitoring

Third on the list of highest ranking elements of the model based on expert panel quantification is identity, authentication, and access management and monitoring, defined as “technical tools that ensure only those that need to access

sensitive data and systems are able to do so,” based on both literature review as well as expert feedback. As with intrusion detection and prevention and protection of network, identity, authentication and access management and monitoring is focused on limitation of access to organizational information systems. Unlike the two highest rated criteria, this element provides for segregation of access at the individual system level in addition to minimizing access to the organization at the global level. In this way, access to sensitive data such as protected health information (PHI) is further limited. While interest in limiting access at the system level is not unique to healthcare organizations it is especially important at healthcare organizations due to the increased risk associated with those particular data types, thus the importance of this criteria as rated by experts is understandable. The importance of identity management as part of a larger cybersecurity strategy is noted in the work of Khan et al. [266] as they explored novel solutions to this vexing challenge through use of blockchain technologies.

7.1.4 Top Rated Criteria – Anti-spam and Malware Protection

Rated fourth on the list of highest ranking elements of the model based on expert panel quantification is anti-spam and malware protection, defined as “technology that minimalize incoming spam and mitigates threat of malware infection,” based on both literature review as well as expert feedback. Anti-spam and malware protection has become increasingly important as a result of both the proliferation and maturity of phishing activity. Anti-spam tools identify and

quarantine known malicious incoming email, preventing organizational end users from ever being exposed to those threats. One expert reported that “97% of all email coming into their organization was captured by their anti-spam tool”, meaning only 3% of all incoming email was valid and delivered to end users. Even so, some malicious email gets through and malware protection software fills this gap. The combination of tools serves as a strong barrier between bad actors and organizational end users. Anti-spam and malware tools retain important positions in the maturity of information security environments [267]. In addition these tools are generally more mature and less costly than some tools associated with information security which may serve as another reason why this element ranked highly in importance within the model.

7.1.5 Top Rated Criteria – Behavioral Testing and Real-time Teaching

The fifth highest rated element of the model based on expert panel quantification is behavioral testing and real-time teaching, and is defined as “active attempts to test work force member's compliance behavior (e.g. phishing education tools and USB drive drops)” based on both literature review as well as expert feedback. The literature identified organization members as a significant threat to information security within organizations. Tools and processes that facilitate active learning for organizational members about common threat vectors such as phishing, when used consistently, have been shown to greatly influence organizational member behavior. Real-time feedback is a strong reinforcing mechanism and provides an

interactive experience that is well suited to a larger strategy associated with training and awareness. Utilization of behavioral testing tools has increased dramatically in healthcare organizations in recent years as the benefit of these tools has been seen to provide quantitative positive change in user response to phishing. Anti-phishing tools are generally inexpensive relative to other information security investments so they provide a high value proposition to healthcare organizations. Skula et al. [268] note the importance of interactive education as a mitigation to the human threat of phishing in information security. This high value proposition is likely a key contributor to the high ranking received by this element within the model.

7.2 Generalizability

Expert feedback validated the generalizable model as a valid and reasonable approach to aid decision makers in evaluation of priority setting for information security resources allocation. As noted earlier, a group of experts with diverse experience coming from a variety of healthcare organization types contributed to the model development, validation and quantification, specifically:

- Experts were either chief information officers, chief privacy officers or chief information security officers. Each of these roles provides a unique perspective to information security maturity and relative importance of specific criteria within the model.

- Experts represented a broad variety of healthcare organization types, not only large and small but diverse in terms of the communities they serve (e.g. urban, rural). These diverse organizations also provide a variety of services to their communities, some providing health insurance plans, others providing specialty clinical services, still others providing access to clinical trials. Even home-based healthcare care services are provided by some.
- The use of experts in development of desirability curves allows for the model to be reused without the need for secondary review by subject matter experts at the conclusion of each assessment.
- During conversations with experts many indicated that this model may be used by any type of healthcare organization. One expert asked the researcher to facilitate the utilization of the model to develop maturity scores within a peer-based healthcare organization forum, in order for those participating organizations to share maturity models scores with one another in an effort to share best practices. Still another expert suggested the model could easily be used by those outside of healthcare, specifically in academic settings, as the basic premise of information security remains fairly constant across industries.

It is important to note that while the model has been validated and is reusable, it will need to be periodically refreshed in order to ensure that it remains relevant.

7.3 Feedback from Experts and Other Considerations

Feedback from experts related to the conduct of this study was uniformly positive. In many cases experts expressed the sentiment “this is much needed” and “extremely important for healthcare organizations”, one expert went so far as to say “I think you have nailed this!” As noted earlier, more than one expert suggested that facilitation of the assessment in small peer-based group settings was desirable and could result in productive peer-based conversations that could not only improve information security maturity at a specific organization, but also develop a community of interest, encouraging information sharing which would promote long term improvement in information security for the greater group.

The experts were derived from diverse healthcare organizations – academic medical centers, community hospitals, critical access hospitals, integrated delivery networks, and large hospital systems. In addition, they contributed diverse perspectives to model development as chief information officers, chief privacy officers and chief information security officers. While the model was validated and quantified specifically by experts with healthcare information security knowledge, experts specifically noted that the model might be generalizable to other industry sectors as most information security threats are consistent across sectors.

This research was conducted during the COVID-19 pandemic in late 2020 and early 2021. This was a period of both significant change in healthcare

organizations in the United States as well as elevated cyber risk as illustrated by the joint announcement issued by the Federal Bureau of Investigation and the Department of Health and Human Services [269] in the Fall of 2020. Healthcare organizations were transitioning those employees who could work from home to do so, taking their work computers with them or using personal devices to access healthcare organizations' networks. They were also rapidly deploying digital healthcare capabilities in order to meet critical community healthcare needs at a time when many patients could not physically come to traditional healthcare locations. In addition, many healthcare organizations were setting up large scale clinical operations for the delivery of vaccines in non-traditional locations (e.g. stadium and airport parking lots). These major shifts in technology delivery and utilization, created at speed by technology professionals, also produced new and non-traditional risks for healthcare organizations [270].

Healthcare organizations onboarded many new staff to meet the increased demand for healthcare services. These new employees or contractors were likely unfamiliar with the information security culture within the healthcare organizations they were joining. Many may have been unfamiliar with the concept of information security at all and needed to be trained. Finally, as the pandemic persisted healthcare workers became increasingly stressed and exhausted, This exhaustion and stress could quite easily lead to lack of attention on required information security precautions.

The culmination of new technology, new employees and increased fatigue on existing employees certainly has the potential to threaten the information security maturity within healthcare organizations specifically. Jalali et al. [271] confirm a need for healthcare delivery organizations to ensure the safety of patient information especially during the COVID-19 pandemic. This rapidly changing environment combined with an increased cyber threat may have influenced the engagement of experts in the development of the model. For some experts, it provided an opportunity for them to be a part of helping create solutions for the healthcare community at large. For other experts it created an impediment in their ability to participate as their attention was keenly focused on solving specific problems at their home institutions and they did not have time to participate in this research. It is also possible that the environment for information security in healthcare during the pandemic influenced not only what elements of the information security maturity model were included in the model but also the importance of certain criterion. This dynamic created an environment of very engaged experts who provided feedback at a time which may have been pivotal in information security, creating a relevant and up-to-date model.

CHAPTER 8: CONCLUSIONS

This chapter will focus on addressing the research goal, gaps and questions and discuss contributions to research and the practice of health information security. In addition, the limitations of the research as well as future research opportunities will be reviewed.

8.1 Conclusions and Contributions

The objective of this research is to develop a framework for assessing information security maturity within healthcare organizations in the United States. Initiation of this research began with a comprehensive literature review of the information security environment for healthcare organizations followed by a further investigation of cyber security frameworks and metrics. As a result of this work, an initial hierarchical decision model was created which consisted of elements which have an impact on information security maturity within healthcare organizations. This fundamental model was then validated, finalized, and quantified by information security experts in the healthcare field. Desirability curves were created through the help of experts to extend the model. Five case studies were then conducted to evaluate the model's performance against expected outcomes and to confirm the generalizability of the model. Finally the model was tested by scenario analysis to ascertain the model's sensitivity to extreme changes at the objective level of the model.

By creating a maturity model for information security in healthcare environments, this research contributes to the existing body of knowledge on technology management maturity assessments in the healthcare industry, as well as maturity models in support of information security. Specifically, as noted in the literature review, more information is needed on the ways that healthcare organizations measure, monitor, and optimize their information security environments. The literature review further noted a lack of structured, comprehensive and usable assessment tools for healthcare organizations in measuring their performance so they could prioritize scarce resources and share best practices related to information security among peers. This research provides a multi-criteria tool which has been quantified and validated for repeat use in multiple healthcare organization types which produces a score. The maturity model may also provide insight into the importance of the human element of information security.

The model supports improved decision making at the institutional level by helping organizations better understand the maturity of their information security environments. This model is a cost effective solution which is easy to administer, minimizing the need for third-part resources or extensive human resources to maintain. The healthcare information security maturity model will help organizations make better decisions about where to apply their scarce resources in order to improve their information security environments. This model may be especially useful at small or less mature healthcare organizations due to the low level

of effort required to complete an institutional assessment. Using the model healthcare organizations will be able to deploy information security programs that will improve the integrity of data as well as the reliability of information systems, thereby improving their information security compliance and minimizing the risk of both internal and external threats. The potential to improve information security within the healthcare industry is vast and a successful maturity model will not only improve information security environments, potentially savings hundreds of millions of dollars, it might also literally save lives.

The model may also be used to share best practices across healthcare organizations regardless of the type of organization. There has been growing interest in the healthcare community to share, confidentially with peers, some level of information about the information security environments within respective organizations. A major provider of electronic records began the conduct of a confidential information security benchmark activity in 2018 which allows some healthcare information to learn more about the tools and staffing levels of their peers in a way that masks the individual organizations contributing to the survey. This exercise did not produce a score of any kind, but it illustrates a willingness on the part of healthcare organizations to share more about their information security in a trusted environment. As the cybersecurity threat has increased, many organizations are more willing, and even eager, to share best practices and lessons learned in confidential forums. While this may seem a minor shift, it has led to the development

of a number of communities of interest both inside and outside of healthcare, nationally and regionally. These communities build upon the trusted relationships of information technology professionals, and sometimes include partnership with federal agencies. It is evident that where cybersecurity used to be a cloak-and-dagger exercise, it has become a team sport as organizations learn that they are better prepared to fight the cybersecurity battle informed by the knowledge and experience of a broader community.

Table 15 shows how this research has addressed the gaps identified in the literature review.

Table 15: Addressing Research Gaps

Research Gaps	Addressed By
RG1: The criteria for assessing information security in healthcare organizations is not organized in a way that identifies the most important risk mitigation actions.	Literature review followed by the development of the hierarchical decision-making model in the conduct of this research provides a framework where each criteria within the model is weighted by importance.
RG2: There is no single quantified, validated, multi-dimensional, and reusable way of assessing information security maturity in healthcare organizations that produces a score.	The HDM creates a quantified, validated, multi-dimensional and reusable model that produces a score for healthcare organizations. This assertion is confirmed with case studies which represent a variety of healthcare organization types.
RG3: Despite the importance of technology in healthcare organizations, there is a lack of studies on assessing maturity of information security within healthcare organizations.	This research contributes to the body of knowledge related to information security cyber security frameworks specifically for healthcare organizations and produces maturity scores.
RG4: Little research exists on the role of user behavior related to information security maturity in healthcare organizations.	This research addresses the role of user behavior related to information security through several goals and metrics embedded in the model.

Table 16 shows how the research has addressed the research questions posed earlier in this dissertation.

Table 16: Addressing Research Questions

Research Questions	Addressed By
RQ1: What are the main perspectives in the assessment of effective information security in healthcare organizations?	The research study identifies the main perspectives related to information security in healthcare organizations.
RQ2: What are the weights of perspectives and criteria related to the assessment of information security maturity in healthcare organizations?	The HDM documented weights of all elements within the model, assessing relative value to overall maturity score for healthcare organizations.
RQ3: Does the proposed framework offer an effective and practical way to assess information security maturity in healthcare organizations.	The validated model was utilized in five case studies representing various healthcare organization types. Results were validated by case study site leads.

In summary, the research offers contribution to both the research body of knowledge as well as provides practical tools for healthcare organizations in evaluating and improving their information security maturity.

8.2 Risks and Limitations

Most research comes with limitations and potential risks. This research is no exception to that principle.

The first limitation of this research is associated with the use of expert panels. While a broad variety of experts were utilized in the conduct of this research, experts are subject to the same human biases we all have. They may be inconsistent or disagreement may be found among experts. In order to protect against this specific risk, the model was tested to identify either disagreement or inconsistency. In

addition some of the data was collected through verbal interaction to minimize confusion related to complexity of some research concepts.

The second limitation of this research is that the model was validated and quantified solely by healthcare experts. While it was found to be generalizable across healthcare organizations it may not be viable as a model to support information security maturity in other organization types (e.g. entertain companies).

The HDM model methodology itself is vulnerable to limitations when there is a difference of more than one criterion under different goals. As the number of criteria within a given goal becomes larger the relative value of those particular criteria may be diminished in value in the overall construct of the model. For example, say one objective with a model value of .20 had three supporting goals and another objective, which also had a model value of .20, but had five supporting goals. The goals associated at the objective level would still only contribute to a combined .20 value in the model. This could lead to the development of a model which does not accurately reflect the true individual criterion values. In order to mitigate this risk the health information security maturity model had either four or five criteria associated with each objective within the model for a gap of no more than one element across each respective objective.

8.3 Future Research

A primary output of this research is the creation of a generalizable information security maturity model for healthcare organizations. While created solely with healthcare experts, many foundational elements related to information security are not necessarily industry specific. The model may be more broadly generalizable to a variety of industries. Exploration of this opportunity could lead to either creation of new maturity models that are industry specific or it could determine that the existing model is more broadly generalizable than tested during the current research study. If this line of research were pursued, further study could compare the resulting models and analyzing similarities or differences.

The healthcare industry is subject to change, sometimes rapid change. If threat vectors significantly change, or the overall landscape of information security changes it could impact the validity of the model. Routine updates of the model are likely necessary and may yield new findings which contribute to the overall body of knowledge associated with healthcare information security.

The model is ultimately designed to help organizations prioritize their resources in order to improve their maturity scores and resulting information security environment. Studies of individual sites or a larger group of sites over time, say over a three year period utilizing an unchanged model, would be of value to determine whether the model is meeting the desired objective of improving maturity

scores. In addition, the maturity score over time might be studied along with other measures such as number of breaches or number of security incidents to determine if a change in score impacts breach or incident activity levels. If the model were utilized by enough healthcare organizations of varying types and sizes, trends might be identified by organization type or size. In order to facilitate this outcome, process documentation would have to be created to guide research assistants to conduct the questionnaire activity and a centralized repository for scoring data would need to be created and maintained. Finally, a study comparing outcomes for those organizations that use the information security maturity model and those that don't, as measured by information security breach or incident level, could be conducted.

While not deeply explored in this study, there may be value in extending the model to include categories of performance as are found in the HIMSS Analytics Electronic Medical Record Adoption Model [113] and discussed in Chapter 2. The value of this extension would be the creation of descriptors of maturity levels, as opposed to just a numerical score. There might also be interest in creating a certification process associated with reaching certain performance categories.

As mentioned previously, at least one expert requested assistance with assessment of the health information security maturity model to a larger peer-based group of healthcare organizations. For example, a single day in-person seminar could begin with an orientation to the model, followed by a facilitated completion of

questionnaire, analysis of individual sites as well as a group analysis, review of findings and then an interactive guided discussion. If structured properly, this exercise could mitigate concerns related to expert self-assessment at the individual site level. Conduct of this activity, in a structured way, either as a single event or over time, may produce new learnings and contributions both to the literature as well as to operational improvements.

There is potential to use the model as a foundation for the development of an education roadmap for cyber security professionals either within healthcare or outside of healthcare, if the model is found to be more broadly generalizable than demonstrated by the current research. The need for information security specialists is high and current educational programs largely focus on technology solutions alone. This research has demonstrated that technology solutions alone are not enough to create mature information security environments. A comprehensive educational program that includes the human element of information security could be quite valuable.

REFERENCES

- [1] Brailer, David J. "Economic Perspectives on Health Information Technology." *Business Economics* 40, no. 3 (2005): 6–14.
<https://doi.org/10.2145/20050301>.
- [2] "Text - H.R.1 - 111th Congress (2009-2010): American Recovery and Reinvestment Act of 2009." 2010. Congress.gov. Accessed July 16, 2021.
<https://www.congress.gov/bill/111th-congress/house-bill/1/text>.
- [3] "Medicare and Medicaid Promoting Interoperability Program Basics | CMS." n.d. Wwww.cms.gov. Accessed July 16, 2021.
<https://www.cms.gov/regulations-and-guidance/legislation/ehrincentiveprograms/basics.html>.
- [4] U.S. Department of Health & Human Services. 2017. "HIPAA for Professionals." HHS.gov. Accessed July 16, 2021.
<https://www.hhs.gov/hipaa/for-professionals/index.html>.
- [5] HHS ONC. 2015. "Guide to Privacy and Security of Electronic Health Information." Accessed July 16, 2021.
<https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf>.
- [6] "U.S. Department of Health & Human Services - Office for Civil Rights." n.d. Ocrportal.hhs.gov. Accessed July 16, 2021.
<https://ocrportal.hhs.gov/ocr/breach>.
- [8] Office for Civil Rights (OCR). 2019. "Resolution Agreements." HHS.gov. Accessed July 16, 2021. <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html>.

- [9] "HIMSS Healthcare Cybersecurity Survey." 2020. www.himss.org. Accessed July 16, 2021. <https://www.himss.org/resources/himss-healthcare-cybersecurity-survey>.
- [10] Smith, Richard E. 2021. *Elementary Information Security*. Burlington, Ma: Jones & Bartlett Learning.
- [11] "More Small Businesses Hit by Cyber Attacks." n.d. GOV.UK. Accessed July 16, 2021. <https://www.gov.uk/government/news/more-small-businesses-hit-by-cyber-attacks>.
- [12] OPM. 2015. "Cybersecurity Incidents." U.S. Office of Personnel Management. 2015. Accessed July 16, 2021. <https://www.opm.gov/cybersecurity/cybersecurity-incidents/>.
- [13] Volz, Aruna Viswanatha and Dustin. 2021. "WSJ News Exclusive | FBI Director Compares Ransomware Challenge to 9/11." *Wall Street Journal*, June 4, 2021, sec. Politics. <https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003>.
- [14] "The Most Prominent Cyber Threats Faced by High-Target Industries." 2016. [Blog.trendmicro.com](http://blog.trendmicro.com). January 26, 2016. <http://blog.trendmicro.com/the-most-prominent-cyber-threats-faced-by-high-target-industries>.
- [15] Morgan, Steve. n.d. "Top 5 Industries at Risk of Cyber-Attacks." *Forbes*. Accessed July 16, 2021. <https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#280fa13f715e>.
- [16] "Why Cybercriminals Attack Healthcare More than Any Other Industry." 2016. *Naked Security*. April 26, 2016. <https://nakedsecurity.sophos.com/2016/04/26/why-cybercriminals-attack-healthcare-more-than-any-other-industry>.

- [17] United States Federal Bureau of Investigation .“2019 Internet Cyber Crime Report.” Accessed November 3, 2020.
https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf
- [18] Ransbotham, Sam, and Sabyasachi Mitra. 2009. “Choice and Chance: A Conceptual Model of Paths to Information Security Compromise.” *Information Systems Research* 20 (1): 121–39.
<https://doi.org/10.1287/isre.1080.0174>.
- [19] Kayworth, Tim, and Dwayne Whitten. 2010. “Effective Information Security Requires a Balance of Social and Technology Factors.” Ssrn.com. 2010.
<https://doi.org/>.
- [20] Werlinger, Rodrigo, Kirstie Hawkey, and Konstantin Beznosov. 2009. “An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management.” Edited by Steven M. Furnell. *Information Management & Computer Security* 17 (1): 4–19.
<https://doi.org/10.1108/09685220910944722>.
- [21] Offner, K. L., E. Sitnikova, K. Joiner, and C. R. MacIntyre. 2020. “Towards Understanding Cybersecurity Capability in Australian Healthcare Organisations: A Systematic Review of Recent Trends, Threats and Mitigation.” *Intelligence and National Security* 35 (4): 556–85.
<https://doi.org/10.1080/02684527.2020.1752459>.
- [22] Culbertson, Nick. n.d. “Council Post: Increased Cyberattacks on Healthcare Institutions Shows the Need for Greater Cybersecurity.” Forbes. Accessed July 16, 2021.
<https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=71d7f60e5650>.

- [23] Box, Debra, and Dalenca Pottas. 2014. "A Model for Information Security Compliant Behaviour in the Healthcare Context." *Procedia Technology* 16: 1462–70. <https://doi.org/10.1016/j.protcy.2014.10.166>.
- [24] Agrawal, Alka, Abhishek Kumar Pandey, Abdullah Baz, Hosam Alhakami, Wajdi Alhakami, Rajeev Kumar, and Raees Ahmad Khan. 2020. "Evaluating the Security Impact of Healthcare Web Applications through Fuzzy Based Hybrid Approach of Multi-Criteria Decision-Making Analysis." *IEEE Access* 8: 135770–83. <https://doi.org/10.1109/access.2020.3010729>.
- [25] "2008 HIMSS Analytics Report: Security Of Patient Data," 2008. Accessed January 15, 2017. http://www.mmc.cm/views/Kroll_HIMSS_Study_April2008.pdf.
- [26] "(PDF) a Survey of Factors Influencing People's Perception of Information Security." n.d. ResearchGate. Accessed July 16, 2021. https://www.researchgate.net/publication/221096519_A_Survey_of_Factors_Influencing_People.
- [27] Guo, Ken H., Yufei Yuan, Norman P. Archer, and Catherine E. Connelly. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model." *Journal of Management Information Systems* 28 (2): 203–36. <https://doi.org/10.2753/mis0742-1222280208>.
- [28] "Malware 101 - Viruses | sans Institute." n.d. [Www.sans.org](http://www.sans.org). Accessed July 16, 2021. <http://www.sans.org/reading-room/whitepapers/incident/malware-101-viruses-32848>.

- [29] Perlroth, Nicole, and David E Sanger. 2017. "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool." *The New York Times*, May 12, 2017. <https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html>.
- [30] Tully, Jeff, Jordan Selzer, James P. Phillips, Patrick O'Connor, and Christian Dameff. 2020. "Healthcare Challenges in the Era of Cybersecurity." *Health Security* 18 (3): 228–31. <https://doi.org/10.1089/hs.2019.0123>.
- [31] Nast, Condé. n.d. "The Untold Story of a Cyberattack, a Hospital and a Dying Woman." Wired UK. Accessed July 16, 2021. <https://www.wired.co.uk/article/ransomware-hospital-death-germany#:~:text=The%20untold%20story%20of%20a%20cyberattack%2C%20a%20hospital%20and%20a%20dying%20woman>.
- [32] Deal, T E, and Allen A Kennedy. 2002. *Corporate Cultures : The Rites and Rituals of Corporate Life*. New York: Basic Books.
- [33] Wiant, Terry L. 2005. "Information Security Policy's Impact on Reporting Security Incidents." *Computers & Security* 24 (6): 448–59. <https://doi.org/10.1016/j.cose.2005.03.008>.
- [34] Urbaczewski, Andrew, and Leonard M. Jessup. 2002. "Does Electronic Monitoring of Employee Internet Usage Work?" *Communications of the ACM* 45 (1). <https://doi.org/10.1145/502269.502303>.
- [35] Jones, Andy. 2008. "Catching the Malicious Insider." *Information Security Technical Report* 13 (4): 220–24. <https://doi.org/10.1016/j.istr.2008.10.008>.
- [36] Johnson, M. Eric, and Eric Goetz. 2007. "Embedding Information Security into the Organization." *IEEE Security & Privacy Magazine* 5 (3): 16–24. <https://doi.org/10.1109/msp.2007.59>.

- [37] Rotvold, Glenda. 2008. "How to Create a Security Culture in Your Organization," *The Information Management Journal*.
- [38] Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." *MIS Quarterly* 34 (3): 523. <https://doi.org/10.2307/25750690>.
- [39] "Online Trust Alliance (OTA)." n.d. Internet Society. Accessed July 16, 2021. <https://www.otalliance.org/system/files/files/resource/documents/ota2015-bestpractices.pdf>.
- [40] Schultz, Eugene. 2005. "The Human Factor in Security." *Computers & Security* 24 (6): 425–26. <https://doi.org/10.1016/j.cose.2005.07.002>.
- [41] Albarrak, A.. "Evaluation of Users Information Security Practices at King Saud University Hospitals." *Global Business and Management Research: An International Journal* 3 (2011): 1.
- [42] Beaudry, and Pinsonneault. 2005. "Understanding User Responses to Information Technology: A Coping Model of User Adaptation." *MIS Quarterly* 29 (3): 493. <https://doi.org/10.2307/25148693>.
- [43] Gaunt, N. 2000. "Practical Approaches to Creating a Security Culture." *International Journal of Medical Informatics* 60 (2): 151–57. [https://doi.org/10.1016/s1386-5056\(00\)00115-5](https://doi.org/10.1016/s1386-5056(00)00115-5).
- [44] Herath, Tejaswini, and H.R. Rao. 2009. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness." *Decision Support Systems* 47 (2): 154–65. <https://doi.org/10.1016/j.dss.2009.02.005>.

- [45] Lacey, David. 2010. "Understanding and Transforming Organizational Security Culture." Edited by Steven M. Furnell. *Information Management & Computer Security* 18 (1): 4–13.
<https://doi.org/10.1108/09685221011035223>.
- [46] McIntosh, Barry. 2011. "An Ethnographic Investigation of the Assimilation of New Organizational Members into an Information Security Culture." *CCE Theses and Dissertations*, January.
https://nsuworks.nova.edu/gscis_etd/240/.
- [47] Probst, Christian W. 2010. *Insider Threats in Cyber Security*. New York: Springer.
- [48] Li, Jingquan, and Michael J. Shaw. 2008. "Electronic Medical Records, HIPAA, and Patient Privacy." *International Journal of Information Security and Privacy* 2 (3): 45–54. <https://doi.org/10.4018/jisp.2008070104>.
- [49] Möller, Sebastian, Noam Ben-Asher, Klaus-Peter Engelbrecht, Roman Englert, and Joachim Meyer. 2011. "Modeling the Behavior of Users Who Are Confronted with Security Mechanisms." *Computers & Security* 30 (4): 242–56.
<https://doi.org/10.1016/j.cose.2011.01.001>.
- [50] Brady, James. 2010. "An Investigation of Factors That Affect HIPAA Security Compliance in Academic Medical Centers." *CCE Theses and Dissertations*, January. https://nsuworks.nova.edu/gscis_etd/100/.
- [51] Ernest Chang, Shuchih, and Chin-Shien Lin. 2007. "Exploring Organizational Culture for Information Security Management." *Industrial Management & Data Systems* 107 (3): 438–58.
<https://doi.org/10.1108/02635570710734316>.

- [52] D'Arcy, John, Anat Hovav, and Dennis Galletta. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach." *Information Systems Research* 20 (1): 79–98. <https://doi.org/10.1287/isre.1070.0160>.
- [53] Warkentin, Merrill, Allen C Johnston, and Jordan Shropshire. 2011. "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention." *European Journal of Information Systems* 20 (3): 267–84. <https://doi.org/10.1057/ejis.2010.72>.
- [54] White, Garry. 2009. "STRATEGIC, TACTICAL, & OPERATIONAL MANAGEMENT SECURITY MODEL." *Spring Journal of Computer Information Systems* 71. http://130.18.86.27/faculty/warkentin/SecurityPapers/Leigh/White2009_JCIS49_3_ManagementandSecurity.pdf.
- [55] Bunker, Guy. 2012. "Technology Is Not Enough: Taking a Holistic View for Information Assurance." *Information Security Technical Report* 17 (1-2): 19–25. <https://doi.org/10.1016/j.istr.2011.12.002>.
- [56] Cannoy, Sherrie Drye, and A. F. Salam. 2010. "A Framework for Health Care Information Assurance Policy and Compliance." *Communications of the ACM* 53 (3): 126–31. <https://doi.org/10.1145/1666420.1666453>.
- [57] Vroom, Cheryl, and Rossouw von Solms. 2004. "Towards Information Security Behavioural Compliance." *Computers & Security* 23 (3): 191–98. <https://doi.org/10.1016/j.cose.2004.01.012>.
- [58] Thomson, Kerry-Lynn, and Rossouw von Solms. 2005. "Information Security Obedience: A Definition." *Computers & Security* 24 (1): 69–75. <https://doi.org/10.1016/j.cose.2004.10.005>.

- [59] Pahnla, Seppo, Siponen, Mikko, and Mahmood, Adam. 2007. "Employees' Behaviour Toward IS Security Policy Compliance," in 40th Annual Hawaii International Conference on Systems Sciences, Honolulu.
- [60] Corriss, Laura. 2010. "Information security governance: Integrating security into the organizational culture," in Governance of Technology Information and Policy, 26th annual Computer Security Applications Conference, West Point, New York.
- [61] Weber, B., B. Alcaro, and V. Ciotti. 2001. "Avoiding HIPAA Hype: Preparing for HIPAA Affordably." *Healthcare Financial Management: Journal of the Healthcare Financial Management Association* 55 (8): 62–65.
<https://pubmed.ncbi.nlm.nih.gov/11499283/>.
- [62] Myyry, Liisa, Mikko Siponen, Seppo Pahnla, Tero Vartiainen, and Anthony Vance. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study." *European Journal of Information Systems* 18 (2): 126–39. <https://doi.org/10.1057/ejis.2009.10>.
- [63] Karjalainen, Mari, and Mikko Siponen. 2011. "Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches." *Journal of the Association for Information Systems* 12 (8): 518–55.
<https://doi.org/10.17705/1jais.00274>.
- [64] Chen, Charlie, Shaw, Ruey-Shiang, & Yang, Samuel. 2010. "Mitigating Information Security Risks By Increasing User Security Awareness: A Case Study of An Information Security Awareness System," *Information Technology, Learning and Performance Journal* 16 (3).
- [65] Veiga, Adéle da, and Nico Martins. 2015. "Improving the Information Security Culture through Monitoring and Implementation Actions Illustrated through a Case Study." *Computers & Security* 49 (March): 162–76.
<https://doi.org/10.1016/j.cose.2014.12.006>.
- [66] Shaw, R.S., Charlie C. Chen, Albert L. Harris, and Hui-Jou Huang. 2009. "The Impact of Information Richness on Information Security Awareness Training

Effectiveness." *Computers & Education* 52 (1): 92–100.
<https://doi.org/10.1016/j.compedu.2008.06.011>.

- [67] Puhakainen, and Siponen. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study." *MIS Quarterly* 34 (4): 757. <https://doi.org/10.2307/25750704>.
- [68] Leach, John. 2003. "Improving User Security Behaviour." *Computers & Security* 22 (8): 685–92. [https://doi.org/10.1016/s0167-4048\(03\)00007-5](https://doi.org/10.1016/s0167-4048(03)00007-5).
- [69] Parsons, Kathryn, Agata McCormac, Marcus Butavicius, Malcolm Pattinson, and Cate Jerram. 2014. "Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q)." *Computers & Security* 42 (May): 165–76. <https://doi.org/10.1016/j.cose.2013.12.003>.
- [70] Van Niekerk, J.F., and R. Von Solms. 2010. "Information Security Culture: A Management Perspective." *Computers & Security* 29 (4): 476–86.
<https://doi.org/10.1016/j.cose.2009.10.005>.
- [71] Ruighaver, A.B., S.B. Maynard, and S. Chang. 2007. "Organisational Security Culture: Extending the End-User Perspective." *Computers & Security* 26 (1): 56–62. <https://doi.org/10.1016/j.cose.2006.10.008>.
- [72] Posey, Clay, Rebecca J. Bennett, and Tom L. Roberts. 2011. "Understanding the Mindset of the Abusive Insider: An Examination of Insiders' Causal Reasoning Following Internal Security Changes." *Computers & Security* 30 (6-7): 486–97. <https://doi.org/10.1016/j.cose.2011.05.002>.
- [73] Spears, and Barki. 2010. "User Participation in Information Systems Security Risk Management." *MIS Quarterly* 34 (3): 503.
<https://doi.org/10.2307/25750689>.

- [74] Smith, Winchester, Bunker, and Jamieson. 2010. "Circuits of Power: A Study of Mandated Compliance to an Information Systems Security 'de Jure' Standard in a Government Organization." *MIS Quarterly* 34 (3): 463. <https://doi.org/10.2307/25750687>.
- [75] Bowen, Pauline, Joan Hash, and Mark Wilson. 2006. "Information Security Handbook: A Guide for Managers." *Www.nist.gov*, December. <https://www.nist.gov/publications/information-security-handbook-guide-managers>.
- [76] HIPAA. 2019. "Healthcare Data Breach Statistics." *HIPAA Journal*. 2019. Accessed July 16, 2021. <https://www.hipaajournal.com/healthcare-data-breach-statistics/>.
- [77] "Cost of a Data Breach Report 2020 2 Contents." Accessed July 16, 2021. n.d. <https://www.ibm.com/downloads/cas/RZAX14GX>.
- [78] Box, Debra, and Dalenca Pottas. 2013. "Improving Information Security Behaviour in the Healthcare Context." *Procedia Technology* 9: 1093–1103. <https://doi.org/10.1016/j.protcy.2013.12.122>.
- [79] "16th Pacific Asia Conference on Information Systems, PACIS 2012, Ho Chi Minh City, Vietnam, 11-15 July 2012 - Researcher Publication." n.d. *Researchr.org*. Accessed July 16, 2021. <https://researchr.org/publication/pacis-2012>.
- [80] Alumaran, Saleh, Giampaolo Bella, and Feng Chen. 2015. "Culture Dimensions of Information Systems Security in Saudi Arabia National Health Services." *International Journal of Computer and Information Engineering* 9 (2): 510–14. <https://publications.waset.org/10000522/culture-dimensions-of-information-systems-security-in-saudi-arabia-national-health-services>.

- [18] Mansur Hasib. 2014. *Impact of Security Culture on Security Compliance in Healthcare in the USA*. S.L.: Createspace Independent P.
- [82] Maurer, Cara C., Pratima Bansal, and Mary M. Crossan. 2011. "Creating Economic Value through Social Values: Introducing a Culturally Informed Resource-Based View." *Organization Science* 22 (2): 432–48.
<https://doi.org/10.1287/orsc.1100.0546>.
- [83] Pendleton, Marcus, Garcia-Lebron, Richard, Cho, Jin-Hee, Xu, Shouhuai. 2016. "A Survey on Security Metrics," *ACM Computing Surveys*, 49(4): 1-35.
- [84] Andress, Jason. 2015. *The Basics of Information Security : Understanding the Fundamentals of InfoSec in Theory and Practice*. Waltham, Ma: Syngress ; Amsterdam.
- [85] It Governance Institute. 2006. *Information Security Governance : Guidance for Boards of Directors and Executive Management*. Rolling Meadows. Ill.: It Governance Institute.
- [86] Saleh, Mohamed S., and Abdulkader Alfantookh. 2011. "A New Comprehensive Framework for Enterprise Information Security Risk Management." *Applied Computing and Informatics* 9 (2): 107–18.
<https://doi.org/10.1016/j.aci.2011.05.002>.
- [87] Venter, H.S, and J.H.P Eloff. 2003. "A Taxonomy for Information Security Technologies." *Computers & Security* 22 (4): 299–307.
[https://doi.org/10.1016/s0167-4048\(03\)00406-1](https://doi.org/10.1016/s0167-4048(03)00406-1).
- [88] Shamala, Palaniappan, Rabiah Ahmad, and Mariana Yusoff. 2013. "A Conceptual Framework of Info Structure for Information Security Risk Assessment (ISRA)." *Journal of Information Security and Applications* 18 (1): 45–52. <https://doi.org/10.1016/j.jisa.2013.07.002>.
- [89] Haufe, Knut, Ricardo Colomo-Palacios, Srdan Dzombeta, Knud Brandis, and Vladimir Stantchev. n.d. "Security Management Standards: A

Mapping.” *Procedia Computer Science* 100: 755–61. Accessed July 16, 2021. https://www.academia.edu/29737963/Security_Management_Standards_A_Mapping.

- [90] Yasasin, Emrah, Julian Prester, Gerit Wagner, and Guido Schryen. 2020. “Forecasting IT Security Vulnerabilities – an Empirical Analysis.” *Computers & Security* 88 (January): 101610. <https://doi.org/10.1016/j.cose.2019.101610>.
- [91] Ifenthaler, Dirk, and Marc Egloffstein. 2019. “Development and Implementation of a Maturity Model of Digital Transformation.” *TechTrends*, November. <https://doi.org/10.1007/s11528-019-00457-4>.
- [92] Brooks, Patti, Omar El-Gayar, and Surendra Sarnikar. 2015. “A Framework for Developing a Domain Specific Business Intelligence Maturity Model: Application to Healthcare.” *International Journal of Information Management* 35 (3): 337–45. <https://doi.org/10.1016/j.ijinfomgt.2015.01.011>.
- [93] Carvalho, João Vidal, Álvaro Rocha, and António Abreu. 2019. “Maturity Assessment Methodology for HISMM - Hospital Information System Maturity Model.” *Journal of Medical Systems* 43 (2). <https://doi.org/10.1007/s10916-018-1143-y>.
- [94] Thomas, Louise, and Joseph M. Woodside. 2016. “Social Media Maturity Model.” *International Journal of Healthcare Management* 9 (1): 67–73. <https://doi.org/10.1080/20479700.2015.1101940>.
- [95] ISACA.. 2012. *Cobit 5 : For Information Security*. Rolling Meadows, IL.
- [96] ISO - International Organization for Standardization. 2019. “ISO/IEC 27000:2018.” ISO. February 4, 2019. <https://www.iso.org/standard/73906.html>.

- [97] Keller, Nicole. 2018. "Framework Documents." NIST. February 5, 2018. <https://www.nist.gov/cyberframework/framework>.
- [98] "Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0." 1999. Cmu.edu. Accessed July 16, 2021. <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473>.
- [99] "HITRUST Alliance | HITRUST CSF | Information Risk Management." 2021. HITRUST Alliance. July 15, 2021. https://hitrustalliance.net/product-tool/hitrust-csf/?gclid=CjwKCAjw3MSHBhB3EiwAxcaEu3Y7ENT8zDShA-ffetQACAzA1If6YRDvLrr0qeoVQebXoU1taLfwHRoCAqsQAvD_BwE.
- [100] Sepúlveda Estay, Daniel A., Rishikesh Sahay, Michael B. Barfod, and Christian D. Jensen. 2020. "A Systematic Review of Cyber-Resilience Assessment Frameworks." *Computers & Security* 97 (October): 101996. <https://doi.org/10.1016/j.cose.2020.101996>.
- [101] Van Niekerk, J.F., and R. Von Solms. 2010. "Information Security Culture: A Management Perspective." *Computers & Security* 29 (4): 476–86. <https://doi.org/10.1016/j.cose.2009.10.005>.
- [102] Da Veiga, A., and J.H.P. Eloff. 2010. "A Framework and Assessment Instrument for Information Security Culture." *Computers & Security* 29 (2): 196–207. <https://doi.org/10.1016/j.cose.2009.09.002>.
- [103] Hajny, Jan, Sara Ricci, Edmundas Piesarskas, Olivier Levillain, Letterio Galletta, and Rocco De Nicola. 2021. "Framework, Tools and Good Practices for Cybersecurity Curricula." *IEEE Access* 9: 94723–47. <https://doi.org/10.1109/access.2021.3093952>.
- [104] Chowdhury, Noman H., Marc T.P. Adam, and Timm Teubner. 2020. "Time Pressure in Human Cybersecurity Behavior: Theoretical Framework and

Countermeasures.” *Computers & Security* 97 (October): 101963.
<https://doi.org/10.1016/j.cose.2020.101963>.

- [105] Bodin, Lawrence D., Lawrence A. Gordon, and Martin P. Loeb. 2005. “Evaluating Information Security Investments Using the Analytic Hierarchy Process.” *Communications of the ACM* 48 (2): 78–83.
<https://doi.org/10.1145/1042091.1042094>.
- [106] Nazareth, Derek L., and Jae Choi. 2015. “A System Dynamics Model for Information Security Management.” *Information & Management* 52 (1): 123–34. <https://doi.org/10.1016/j.im.2014.10.009>.
- [107] Liu, Zhaoxi, Wei Wei, Lingfeng Wang, Chee-Wooi Ten, and Yeonwoo Rho. 2021. “An Actuarial Framework for Power System Reliability Considering Cybersecurity Threats.” *IEEE Transactions on Power Systems* 36 (2): 851–64.
<https://doi.org/10.1109/tpwrs.2020.3018701>.
- [108] Gordon, Lawrence A., Martin P. Loeb, and Lei Zhou. 2020. “Integrating Cost-Benefit Analysis into the NIST Cybersecurity Framework via the Gordon-Loeb Model.” *Journal of Cybersecurity* 6 (1).
<https://doi.org/10.1093/cybsec/tyaa005>.
- [109] Lee, In. 2021. “Cybersecurity: Risk Management Framework and Investment Cost Analysis.” *Business Horizons*, February.
<https://doi.org/10.1016/j.bushor.2021.02.022>.
- [110] Solic, Kresimir, Hrvoje Ocevcic, and Marin Golub. 2015. “The Information Systems’ Security Level Assessment Model Based on an Ontology and Evidential Reasoning Approach.” *Computers & Security* 55 (November): 100–112. <https://doi.org/10.1016/j.cose.2015.08.004>.

- [111] M. Zaki, V. Sivakumar, S. Shrivastava, K. Gaurav," 2021. Third International conference on intelligent communication technologies and virtual mobile networks.
- [112] Gourisetti, Sri Nikhil Gupta, Michael Mylrea, and HIRAK Patangia. 2020. "Cybersecurity Vulnerability Mitigation Framework through Empirical Paradigm: Enhanced Prioritized Gap Analysis." *Future Generation Computer Systems* 105 (April): 410–31. <https://doi.org/10.1016/j.future.2019.12.018>.
- [113] "(PDF) a Framework for Comparing Different Information Security Risk Analysis Methodologies." n.d. ResearchGate. Accessed July 16, 2021. https://www.researchgate.net/publication/228866471_A_framework_for_comparing_different_information_security_risk_analysis_methodologies.
- [114] "Dependable Computing - EDCC 2020 Workshops | SpringerLink." n.d. [Link.springer.com](https://link.springer.com). Accessed July 16, 2021. <https://link.springer.com/content/pdf/10.1007%2F978-3-030-58462-7.pdf>.
- [115] Benz, Michael, and Dave Chatterjee. 2020. "Calculated Risk? A Cybersecurity Evaluation Tool for SMEs." *Business Horizons* 63 (4): 531–40. <https://doi.org/10.1016/j.bushor.2020.03.010>.
- [116] Karabacak, Bilge, and Ibrahim Sogukpinar. 2005. "ISRAM: Information Security Risk Analysis Method." *Computers & Security* 24 (2): 147–59. <https://doi.org/10.1016/j.cose.2004.07.004>.
- [117] Feng, Nan, and Minqiang Li. 2011. "An Information Systems Security Risk Assessment Model under Uncertain Environment." *Applied Soft Computing* 11 (7): 4332–40. <https://doi.org/10.1016/j.asoc.2010.06.005>.
- [118] Gusmão, Ana Paula Henriques de, Lúcio Camara e Silva, Maisa Mendonça Silva, Thiago Poletto, and Ana Paula Cabral Seixas Costa. 2016. "Information Security Risk Analysis Model Using Fuzzy Decision Theory." *International*

Journal of Information Management 36 (1): 25–34.
<https://doi.org/10.1016/j.ijinfomgt.2015.09.003>.

- [119] Aliyu, Aliyu, Leandros Maglaras, Ying He, Iryna Yevseyeva, Eerke Boiten, Allan Cook, and Helge Janicke. 2020. “A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom.” *Applied Sciences* 10 (10): 3660.
<https://doi.org/10.3390/app10103660>.
- [120] Rea-Guaman, Angel Marcelo, Jezreel Mejía, Tomas San Feliu, and Jose A. Calvo-Manzano. 2020. “AVARCIBER: A Framework for Assessing Cybersecurity Risks.” *Cluster Computing*, January.
<https://doi.org/10.1007/s10586-019-03034-9>.
- [121] Swanson, Marianne, and National Institute Of Standards And Technology (U.S. 2003. *Security Metrics Guide for Information Technology Systems*. Gaithersburg, Md: U.S. Dept. Of Commerce, National Institute Of Standards And Technology ; Washington, D.C.
- [122] “(PDF) the Adoption of Information Security Management Standards: A Literature Review.” n.d. ResearchGate. Accessed July 16, 2021.
https://www.researchgate.net/publication/260019491_The_Adoption_of_Information_Security_Management_Standards_A_Literature_Review.
doi:10.4018/978-1-60566-326-5.ch006
- [123] Vroom, Cheryl, and Rossouw von Solms. 2004. “Towards Information Security Behavioural Compliance.” *Computers & Security* 23 (3): 191–98.
<https://doi.org/10.1016/j.cose.2004.01.012>.
- [124] Saint-Germain, René. 2005. “Information Security Management Best Practice Based on ISO/IEC 17799 the International Information Security Standard Provides a Framework for Ensuring Business Continuity, Maintaining Legal Compliance, and Achieving a Competitive Edge.” Undefined. 2005.
<https://www.semanticscholar.org/paper/Information-Security->

Management-Best-Practice-Based-Saint-Germain/53f16a5a62e2bac36fea38158c1e8af80fac683a.

- [125] Alter, Steven, and Susan A. Sherer. 2004. "A General, but Readily Adaptable Model of Information System Risk." *Communications of the Association for Information Systems* 14. <https://doi.org/10.17705/1cais.01401>.
- [126] Jansen, Wayne. 2009. "Directions in Security Metrics Research." Csrc.nist.gov. April 30, 2009. <https://csrc.nist.gov/publications/detail/nistir/7564/final>.
- [127] W Krag Brothby. 2009. *Information Security Management Metrics : A Definitive Guide to Effective Security Monitoring and Measurement*. Boca Raton: Crc Press.
- [128] Sohrabi Safa, Nader, Rossouw Von Solms, and Steven Furnell. 2016. "Information Security Policy Compliance Model in Organizations." *Computers & Security* 56 (February): 70–82. <https://doi.org/10.1016/j.cose.2015.10.006>.
- [129] Kotulic, Andrew G., and Jan Guynes Clark. 2004. "Why There Aren't More Information Security Research Studies." *Information & Management* 41 (5): 597–607. <https://doi.org/10.1016/j.im.2003.08.001>.
- [130] Black, Paul E., Karen Scarfone, and Murugiah Souppaya. 2008. "Cyber Security Metrics and Measures." *Wiley Handbook of Science and Technology for Homeland Security*, November. <https://doi.org/10.1002/9780470087923.hhs440>.
- [131] Da Veiga, Adéle, and Nico Martins. 2015. "Information Security Culture and Information Protection Culture: A Validated Assessment Instrument." *Computer Law & Security Review* 31 (2): 243–56. <https://doi.org/10.1016/j.clsr.2015.01.005>.

- [132] "4 - SMART Metrics — HowTo.comMetrics." n.d. Howto.drkpi.ch. Accessed July 16, 2021. <http://howto.drkpi.ch/smart-benchmarking/>.
- [133] Lean Healthcare Exchange, "SMART Metrics." Accessed March 26, 2018. <http://www.leanhealthcareexchange.com/smart-metrics/>.
- [134] Siponen, Mikko. 2006. "Information Security Standards Focus on the Existence of Process, Not Its Content." *Communications of the ACM* 49 (8): 97. <https://doi.org/10.1145/1145287.1145316>.
- [135] "Electronic Medical Record Adoption Model (EMRAM) | HIMSS." 2021. Wwww.himss.org. January 20, 2021. <http://www.himssanalytics.org/emram>.
- [136] "European Hospitals EMRAM Maturity Overview." n.d. https://na.eventscloud.com/file_uploads/0cf548ab2f4eaeafd0a6b4ce615f0399_Hoyt_Session_1_European_Hospitals_EMRAM_Maturity_Overview_CIOSummit.pdf.
- [137] "News | HIMSS." 2019. Wwww.himss.org. October 24, 2019. <http://www.himss.org/news/himss-survey-finds-increased-efficiencies-clinical-staff-quality-performance-most-frequently-cited>.
- [138] Shah, Kieran, Clifford Lo, Michele Babich, Nicole W Tsao, and Nick J Bansback. 2016. "Bar Code Medication Administration Technology: A Systematic Review of Impact on Patient Safety When Used with Computerized Prescriber Order Entry and Automated Dispensing Devices." *The Canadian Journal of Hospital Pharmacy* 69 (5): 394–402. <https://doi.org/10.4212/cjhp.v69i5.1594>.
- [139] "Adoption Model for Analytics Maturity." 2017. HIMSS Analytics - North America. January 10, 2017. <https://www.himssanalytics.org/amam>.

- [140] "Standards enhance protection against cybercrime." Accessed July 10, 2021. <http://www.rsm.nl/about-rsm/news/detail/1433-standards-enhance-protection-against-cybercrime>.
- [141] "ISO Survey of Global Certificates Shows 3% Growth." 2015. IIOC. September 22, 2015. <https://iio.org/corporate-news/iso-survey-of-global-certificates-shows-3-growth/>.
- [142] Spears, Janine L. n.d. "A Holistic Risk Analysis Method for Identifying Information Security Risks." *Security Management, Integrity, and Internal Control in Information Systems*, 185–202. Accessed July 16, 2021. https://doi.org/10.1007/0-387-31167-x_12.
- [143] Willison, Robert, and Mikko Siponen. 2009. "Overcoming the Insider." *Communications of the ACM* 52 (9): 133. <https://doi.org/10.1145/1562164.1562198>.
- [144] Siponen, Mikko, and Anthony Vance. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations." *MIS Quarterly* 34 (3): 487–502. <https://doi.org/10.2307/25750688>.
- [145] "(R. Rastogi, R. Von Solms) Information Security Service Culture - Information Security for End-Users." n.d. [Www.jucs.org](http://www.jucs.org). Accessed July 16, 2021. http://www.jucs.org/jucs_18_12/information_security_service_culture.
- [146] Zafar, Humayun, and Jan Guynes Clark. 2009. "Current State of Information Security Research in IS." *Communications of the Association for Information Systems* 24. <https://doi.org/10.17705/1cais.02434>.
- [147] D'Arcy, John, and Anat Hovav. 2008. "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures." *Journal of Business Ethics* 89 (S1): 59–71. <https://doi.org/10.1007/s10551-008-9909-7>.

- [148] Ashenden, Debi. 2008. "Information Security Management: A Human Challenge?" *Information Security Technical Report* 13 (4): 195–201. <https://doi.org/10.1016/j.istr.2008.10.006>.
- [149] Rabii, Anass, Saliha Assoul, Khadija Ouazzani Touhami, and Ounsa Roudies. 2020. "Information and Cyber Security Maturity Models: A Systematic Literature Review." *Information & Computer Security* ahead-of-print (ahead-of-print). <https://doi.org/10.1108/ics-03-2019-0039>.
- [150] Anderson, Kent. 2007. "Convergence: A Holistic Approach to Risk Management." *Network Security* 2007 (5): 4–7. [https://doi.org/10.1016/s1353-4858\(07\)70033-8](https://doi.org/10.1016/s1353-4858(07)70033-8).
- [151] Frayssinet Delgado, Maurice, Doris Esenarro, Francisco Fernando Juárez Regalado, and Mónica Díaz Reátegui. 2021. "Methodology Based on the NIST Cybersecurity Framework as a Proposal for Cybersecurity Management in Government Organizations." *3C TIC: Cuadernos de Desarrollo Aplicados a Las TIC* 10 (2): 123–41. <https://doi.org/10.17993/3ctic.2021.102.123-141>.
- [152] Syafrizal, Melwin, Siti Rahayu Selamat, and Nurul Azma Zakaria. 2020. "Analysis of Cybersecurity Standard and Framework Components." *International Journal of Communication Networks and Information Security (IJCNIS)* 12 (3). <https://www.ijcnis.org/index.php/ijcnis/article/view/4817>.
- [153] "Incorporating Multiple Criteria in HTA: Methods and Processes." 2011. [Www.ohe.org](http://www.ohe.org). March 1, 2011. <https://www.ohe.org/publications/incorporating-multiple-criteria-hta-methods-and-processes>.
- [154] Marsh, Kevin, Maarten IJzerman, Praveen Thokala, Rob Baltussen, Meindert Boysen, Zoltán Kaló, Thomas Lönngren, et al. 2016. "Multiple Criteria

Decision Analysis for Health Care Decision Making—Emerging Good Practices: Report 2 of the ISPOR MCDA Emerging Good Practices Task Force.” *Value in Health* 19 (2): 125–37.
<https://doi.org/10.1016/j.jval.2015.12.016>.

- [155] Langemeyer, Johannes, Erik Gómez-Baggethun, Dagmar Haase, Sebastian Scheuer, and Thomas Elmqvist. 2016. “Bridging the Gap between Ecosystem Service Assessments and Land-Use Planning through Multi-Criteria Decision Analysis (MCDA).” *Environmental Science & Policy* 62 (August): 45–56.
<https://doi.org/10.1016/j.envsci.2016.02.013>.
- [156] Adunlin, Georges, Vakaramoko Diaby, and Hong Xiao. 2014. “Application of Multicriteria Decision Analysis in Health Care: A Systematic Review and Bibliometric Analysis.” *Health Expectations* 18 (6): 1894–1905.
<https://doi.org/10.1111/hex.12287>.
- [157] Drake, Julia I., Juan Carlos Trujillo de Hart, Clara Monleón, Walter Toro, and Joice Valentim. 2017. “Utilization of Multiple-Criteria Decision Analysis (MCDA) to Support Healthcare Decision-Making FIFARMA, 2016.” *Journal of Market Access & Health Policy* 5 (1).
<https://doi.org/10.1080/20016689.2017.1360545>.
- [158] Mühlbacher, Axel C., and Anika Kaczynski. 2015. “Making Good Decisions in Healthcare with Multi-Criteria Decision Analysis: The Use, Current Research and Future Development of MCDA.” *Applied Health Economics and Health Policy* 14 (1): 29–40. <https://doi.org/10.1007/s40258-015-0203-4>.
- [159] Nutt, David J, Leslie A King, and Lawrence D Phillips. 2010. “Drug Harms in the UK: A Multicriteria Decision Analysis.” *The Lancet* 376 (9752): 1558–65.
[https://doi.org/10.1016/s0140-6736\(10\)61462-6](https://doi.org/10.1016/s0140-6736(10)61462-6).
- [160] Diaby, Vakaramoko, Ron Goeree, Jeffrey Hoch, and Uwe Siebert. 2014. “Multi-Criteria Decision Analysis for Health Technology Assessment in Canada: Insights from an Expert Panel Discussion.” *Expert Review of*

Pharmacoeconomics & Outcomes Research 15 (1): 13–19.
<https://doi.org/10.1586/14737167.2015.965155>.

- [161] Marsh, Kevin, Tereza Lanitis, David Neasham, Panagiotis Orfanos, and Jaime Caro. 2014. "Assessing the Value of Healthcare Interventions Using Multi-Criteria Decision Analysis: A Review of the Literature." *PharmacoEconomics* 32 (4): 345–65.
<https://doi.org/10.1007/s40273-014-0135-0>.
- [162] Ou, Yang, Yu-Ping, Shieh, How-Ming, Tzeng, Gwo-Hshiung. 2009. "A VIKOR Technique Based on DEMATEL and ANP for Information Security Risk Control Assessment." *International Journal of Information Technology & Decision Making* 08 (02): 267–87.
<https://doi.org/10.1142/s0219622009003375>.
- [163] Ou Yang, Yu-Ping, How-Ming Shieh, and Gwo-Hshiung Tzeng. 2013. "A VIKOR Technique Based on DEMATEL and ANP for Information Security Risk Control Assessment." *Information Sciences* 232 (May): 482–500.
<https://doi.org/10.1016/j.ins.2011.09.012>.
- [164] Lo, Chi-Chun, and Wan-Jia Chen. 2012. "A Hybrid Information Security Risk Assessment Procedure Considering Interdependences between Controls." *Expert Systems with Applications* 39 (1): 247–57.
<https://doi.org/10.1016/j.eswa.2011.07.015>.
- [165] El-Gayar, Omar F., and Brian D. Fritz. 2010. "A Web-Based Multi-Perspective Decision Support System for Information Security Planning." *Decision Support Systems* 50 (1): 43–54. <https://doi.org/10.1016/j.dss.2010.07.001>.

- [166] AouniBelaïd, and Ossama Kettani. 2001. "Goal Programming Model: A Glorious History and a Promising Future." *European Journal of Operational Research* 133 (2): 225–31. [https://doi.org/10.1016/s0377-2217\(00\)00294-0](https://doi.org/10.1016/s0377-2217(00)00294-0).
- [167] Sussex, Jon, Pierrick Rollet, Martina Garau, Claude Schmitt, Alastair Kent, and Adam Hutchings. 2013. "A Pilot Study of Multicriteria Decision Analysis for Valuing Orphan Medicines." *Value in Health* 16 (8): 1163–69. <https://doi.org/10.1016/j.jval.2013.10.002>.
- [168] Aldlaigan, Abdullah H., and Francis A. Buttle. 2002. "SYSTRA-SQ: A New Measure of Bank Service Quality." *International Journal of Service Industry Management* 13 (4): 362–81. <https://doi.org/10.1108/09564230210445041>.
- [169] Gerd Sri, Pisek, and Dundar F. Kocaoglu. 2007. "Technology Policy Instrument (TPI): A Decision Model for Evaluating Emerging Technologies for National Technology Policy - Research Framework." IEEE Xplore. August 1, 2007. <https://doi.org/10.1109/PICMET.2007.4349478>.
- [170] Saaty, Thomas L. 2008. "Decision Making with the Analytic Hierarchy Process." *International Journal of Services Sciences* 1 (1): 83. <https://doi.org/10.1504/ijssci.2008.017590>.
- [171] Kodali, Rambabu, and Subhash Chandra. 2001. "Analytical Hierarchy Process for Justification of Total Productive Maintenance." *Production Planning & Control* 12 (7): 695–705. <https://doi.org/10.1080/09537280010024045>.
- [172] Coates, Joseph F. 2010. "The Future of Foresight—a US Perspective." *Technological Forecasting and Social Change* 77 (9): 1428–37. <https://doi.org/10.1016/j.techfore.2010.07.009>.

- [173] Calof, Jonathan, and Jack Smith. 2009. "The Integrative Domain of Foresight and Competitive Intelligence and Its Impact on R&D Management." *R&D Management* 40 (1): 31–39. <https://doi.org/10.1111/j.1467-9310.2009.00579.x>.
- [174] Fordham, Richard, and M Ba. n.d. "Volume 4, Number 2." Accessed July 16, 2021. <http://www.bandolier.org.uk/painres/download/whatis/pbma.pdf>.
- [175] Edwards, Rhiannon Tudor, Joanna M Charles, Sara Thomas, Julie Bishop, David Cohen, Sam Groves, Ciaran Humphreys, Helen Howson, and Peter Bradley. 2014. "A National Programme Budgeting and Marginal Analysis (PBMA) of Health Improvement Spending across Wales: Disinvestment and Reinvestment across the Life Course." *BMC Public Health* 14 (1). <https://doi.org/10.1186/1471-2458-14-837>.
- [176] Roy, Bernard. 1991. "The Outranking Approach and the Foundations of Electre Methods." *Theory and Decision* 31 (1): 49–73. <https://doi.org/10.1007/bf00134132>.
- [177] Figueira, José Rui, Salvatore Greco, Bernard Roy, and Roman Słowiński. 2012. "An Overview of ELECTRE Methods and Their Recent Extensions." *Journal of Multi-Criteria Decision Analysis* 20 (1-2): 61–85. <https://doi.org/10.1002/mcda.1482>.
- [178] Roy, Bernard, and Daniel Vanderpooten. 1997. "An Overview on 'the European School of MCDA: Emergence, Basic Features and Current Works.'" *European Journal of Operational Research* 99 (1): 26–27. [https://doi.org/10.1016/s0377-2217\(96\)00379-7](https://doi.org/10.1016/s0377-2217(96)00379-7).
- [179] S. K. Amponsah. 2012. "Logistic Preference Function for Preference Ranking Organization Method for Enrichment Evaluation (PROMETHEE) Decision

Analysis.” *African Journal of Mathematics and Computer Science Research* 5 (6). <https://doi.org/10.5897/ajmcsr12.011>.

- [180] Hyde, Kylie, Holger R. Maier, and Christopher Colby. 2003. “Incorporating Uncertainty in the PROMETHEE MCDA Method.” *Journal of Multi-Criteria Decision Analysis* 12 (4-5): 245–59. <https://doi.org/10.1002/mcda.361>.
- [181] Miettinen, Kaisa. 2012. “Survey of Methods to Visualize Alternatives in Multiple Criteria Decision Making Problems.” *OR Spectrum* 36 (1): 3–37. <https://doi.org/10.1007/s00291-012-0297-0>.
- [182] Goswami, Shankha Shubhra. 2020. “Outranking Methods: Promethee I and Promethee II.” *Foundations of Management* 12 (1): 93–110. <https://doi.org/10.2478/fman-2020-0008>.
- [183] Goetghebeur, MM, M Wagner, H Khoury, R Levitt, LJ Erickson, and D Rindress. 2008. “PMC50 EVIDENCE ANDVALUE: IMPACT on DECISION MAKING—the EVIDEM FRAMEWORK and POTENTIAL APPLICATIONS.” *Value in Health* 11 (3): A183–84. [https://doi.org/10.1016/s1098-3015\(10\)70584-2](https://doi.org/10.1016/s1098-3015(10)70584-2).
- [184] Thokala, P. 2012. “PRM60 Operationalising Multiple Criteria Decision Analysis for Health Technology Assessment.” *Value in Health* 15 (4): A169. <https://doi.org/10.1016/j.jval.2012.03.915>.
- [185] Xu, Zeshui. 2005. “On Method for Uncertain Multiple Attribute Decision Making Problems with Uncertain Multiplicative Preference Information on Alternatives.” *Fuzzy Optimization and Decision Making* 4 (2): 131–39. <https://doi.org/10.1007/s10700-004-5869-2>.
- [186] Panda, Monalisa, and Alok Kumar Jagadev. 2018. “TOPSIS in Multi-Criteria Decision Making: A Survey.” IEEE Xplore. September 1, 2018. <https://doi.org/10.1109/ICDSBA.2018.00017>.

- [187] Lin, Kuo-Sui. 2019. "A New Distance Measure for MCDM Problem Using TOPSIS Method." IEEE Xplore. December 1, 2019.
<https://doi.org/10.1109/iCMLDE49015.2019.00015>.
- [188] Shih, Hsu-Shih, Huan-Jyh Shyur, and E. Stanley Lee. 2007. "An Extension of TOPSIS for Group Decision Making." *Mathematical and Computer Modelling* 45 (7-8): 801–13. <https://doi.org/10.1016/j.mcm.2006.03.023>.
- [189] Alessio Ishizaka, and Philippe Nemery. 2013. *Multi-Criteria Decision Analysis : Methods and Software*. Chichester, West Sussex, United Kingdom: Wiley.
- [190] International Conference on Multiple Criteria Decision Making, Theodor J Stewart, and Robin C Van den Honert, eds. 1998. *Trends in Multicriteria Decision Making: Proceedings of the 13th International Conference on Multiple Criteria Decision Making, Cape Town, South Africa, January 1997*. Open WorldCat. Berlin; New York: Springer-Verlag.
<https://www.worldcat.org/title/trends-in-multicriteria-decision-making-proceedings-of-the-13th-international-conference-on-multiple-criteria-decision-making-cape-town-south-africa-january-1997/oclc/39360544>.
- [191] "(PDF) an Analysis of Multi-Criteria Decision Making Methods." n.d. ResearchGate. Accessed July 16, 2021.
https://www.researchgate.net/publication/275960103_An_analysis_of_multi-criteria_decision_making_methods.
- [192] Gerdri, N., and D.F. Kocaoglu. 2003. "An Analytical Approach to Building a Technology Development Envelope (TDE) for Roadmapping of Emerging Technologies: A Case Study of Emerging Electronic Cooling Technologies for Computer Servers." IEEE Xplore. July 1, 2003.
<https://doi.org/10.1109/PICMET.2003.1222817>.

- [193] Martino, Joseph P. 1993. "Forecasting and Management of Technology." *Technological Forecasting and Social Change* 43 (3-4): 383–84. [https://doi.org/10.1016/0040-1625\(93\)90064-e](https://doi.org/10.1016/0040-1625(93)90064-e).
- [194] Cantrill, J. A., B. Sibbald, and Buetow, S. . 1996. "The Delphi and Nominal Group Techniques in Health Services Research." *International Journal of Pharmacy Practice* 4 (2): 67–74. <https://doi.org/10.1111/j.2042-7174.1996.tb00844.x>.
- [195] Phan, Kenny. 2013. "Innovation Measurement: A Decision Framework to Determine Innovativeness of a Company." *Dissertations and Theses*, May. <https://doi.org/10.15760/etd.1017>.
- [196] Gibson, Elizabeth, Tugrul U. Daim, and Marina Dabic. 2019. "Evaluating University Industry Collaborative Research Centers." *Technological Forecasting and Social Change* 146 (September): 181–202. <https://doi.org/10.1016/j.techfore.2019.05.014>.
- [197] Meelen, Toon, and Jacco Farla. 2013. "Towards an Integrated Framework for Analysing Sustainable Innovation Policy." *Technology Analysis & Strategic Management* 25 (8): 957–70. <https://doi.org/10.1080/09537325.2013.823146>.
- [198] Saaty, Thomas L. 1984. "The Analytic Hierarchy Process: Decision Making in Complex Environments." *Quantitative Assessment in Arms Control*, 285–308. https://doi.org/10.1007/978-1-4613-2805-6_12.
- [199] Cetindamar, Dilek, Tugrul U. Daim, Berna Beyhan, and Nuri Başoğlu, eds. 2013. *Strategic Planning Decisions in the High Tech Industry*. www.springer.com. London: Springer-Verlag. <https://www.springer.com/gp/book/9781447148869>.

- [200] Daim, Tugrul U., Byung-Sung Yoon, John Lindenberg, Robert Grizzi, Judith Estep, and Terry Oliver. 2018. "Strategic Roadmapping of Robotics Technologies for the Power Industry: A Multicriteria Technology Assessment." *Technological Forecasting and Social Change* 131 (June): 49–66. <https://doi.org/10.1016/j.techfore.2017.06.006>.
- [201] Khalifa, Rafea I., and Tugrul U. Daim. 2021. "Project Assessment Tools Evaluation and Selection Using the Hierarchical Decision Modeling: Case of State Departments of Transportation in the United States." *Journal of Management in Engineering* 37 (1): 05020015. [https://doi.org/10.1061/\(asce\)me.1943-5479.0000858](https://doi.org/10.1061/(asce)me.1943-5479.0000858).
- [202] "Logistics Service Provider Selection Decision Making for Healthcare Industry Based on a Novel Weighted Density-Based Hierarchical Clustering." 2021. *Advanced Engineering Informatics* 48 (April): 101301. <https://doi.org/10.1016/j.aei.2021.101301>.
- [203] Sheikh, Nasir J., Kiyoon Kim, and Dundar F. Kocaoglu. 2016. "Use of Hierarchical Decision Modeling to Select Target Markets for a New Personal Healthcare Device." *Health Policy and Technology* 5 (2): 99–112. <https://doi.org/10.1016/j.hlpt.2015.12.001>.
- [204] Chan, Leong, and Tugrul Daim. 2017. "A Research and Development Decision Model for Pharmaceutical Industry: Case of China." *R&D Management* 48 (2): 223–42. <https://doi.org/10.1111/radm.12285>.
- [205] Pereira, Cristiano Gonçalves, Joao Ricardo Lavoie, Edwin Garces, Fernanda Basso, Marina Dabić, Geciane Silveira Porto, and Tugrul Daim. 2019. "Forecasting of Emerging Therapeutic Monoclonal Antibodies Patents Based on a Decision Model." *Technological Forecasting and Social Change* 139 (February): 185–99. <https://doi.org/10.1016/j.techfore.2018.11.002>.

- [206] Hogaboam, Liliya, and Tugrul Daim. 2018. "Technology Adoption Potential of Medical Devices: The Case of Wearable Sensor Products for Pervasive Care in Neurosurgery and Orthopedics." *Health Policy and Technology* 7 (4): 409–19. <https://doi.org/10.1016/j.hlpt.2018.10.011>.
- [207] Lavoie, Joao Ricardo, Tugrul Daim, and Elias G. Carayannis. 2021. "Technology Transfer Evaluation: Driving Organizational Changes through a Hierarchical Scoring Model." *IEEE Transactions on Engineering Management*, 1–15. <https://doi.org/10.1109/tem.2020.3042452>.
- [208] Daim, Tugrul U., ed. 2016. *Hierarchical Decision Modeling: Essays in Honor of Dundar F. Kocaoglu*. *Www.springer.com*. Springer International Publishing. <https://www.springer.com/gp/book/9783319185576>.
- [209] Giadedi, Abdulhakim. 2020. "A Scoring Model to Evaluate Offshore Oil Projects: Case of Eni and Mellitah Oil & Gas." *Dissertations and Theses*, September. <https://doi.org/10.15760/etd.7473>.
- [210] Rahman, Nayem, Tugrul Daim, and Nuri Basoglu. 2021. "Exploring the Factors Influencing Big Data Technology Acceptance." *IEEE Transactions on Engineering Management*, 1–16. <https://doi.org/10.1109/tem.2021.3066153>.
- [211] Garces, Edwin, Daim, Tugrul. 2021. "Evaluating R&D Projects in Regulated Utilities: the case of Power Transmission Utilities." *IEEE Transactions on Engineering Management*, 2021.
- [212] Khanam, Momtaj, and Tugrul Daim. 2021. "A Market Diffusion Potential (MDP) Assessment Model for Residential Energy Efficient (EE) Technologies in the U.S." *Renewable and Sustainable Energy Reviews* 144 (July): 110968. <https://doi.org/10.1016/j.rser.2021.110968>.

- [213] Barham, Husam, and Tugrul Daim. 2020. "The Use of Readiness Assessment for Big Data Projects." *Sustainable Cities and Society* 60 (September): 102233. <https://doi.org/10.1016/j.scs.2020.102233>.
- [214] Lavoie, Joao Ricardo, and Tugrul Daim. 2020. "Towards the Assessment of Technology Transfer Capabilities: An Action Research-Enhanced HDM Model." *Technology in Society* 60 (February): 101217. <https://doi.org/10.1016/j.techsoc.2019.101217>.
- [215] Abotah, Remal, and Tugrul U. Daim. 2017. "Towards Building a Multi Perspective Policy Development Framework for Transition into Renewable Energy." *Sustainable Energy Technologies and Assessments* 21 (June): 67–88. <https://doi.org/10.1016/j.seta.2017.04.004>.
- [216] Neshati, Ramin, and Tugrul U. Daim. 2017. "Participation in Technology Standards Development: A Decision Model for the Information and Communications Technology (ICT) Industry." *The Journal of High Technology Management Research* 28 (1): 47–60. <https://doi.org/10.1016/j.hitech.2017.04.004>.
- [217] Iskin, Ibrahim, and Tugrul U. Daim. 2016. "An Assessment Model for Energy Efficiency Program Planning in Electric Utilities: Case of Northwest U.S." *Sustainable Energy Technologies and Assessments* 15 (June): 42–59. <https://doi.org/10.1016/j.seta.2016.03.002>.
- [218] Wang, Bing, Dundar F. Kocaoglu, Tugrul U. Daim, and Jiting Yang. 2010. "A Decision Model for Energy Resource Selection in China." *Energy Policy* 38 (11): 7130–41. <https://doi.org/10.1016/j.enpol.2010.07.031>.
- [219] Chen, Hongyi, and Dundar F. Kocaoglu. 2008. "A Sensitivity Analysis Algorithm for Hierarchical Decision Models." *European Journal of Operational Research* 185 (1): 266–88. <https://doi.org/10.1016/j.ejor.2006.12.029>.

- [220] "Assessment of Technology Adoption Potential of Medical Devices: Case of Wearable Sensor Products for Pervasive Care in Neurosurgery and Orthopedics - ProQuest." n.d. www.proquest.com. Accessed July 16, 2021. <https://www.proquest.com/docview/2030566122?pq-origsite=gscholar&fromopenview=true>.
- [221] Fink, A, J Kosecoff, M Chassin, and R H Brook. 1984. "Consensus Methods: Characteristics and Guidelines for Use." *American Journal of Public Health* 74 (9): 979–83. <https://doi.org/10.2105/ajph.74.9.979>.
- [222] McKenna, Hugh P. 1994. "The Delphi Technique: A Worthwhile Research Approach for Nursing?" *Journal of Advanced Nursing* 19 (6): 1221–25. <https://doi.org/10.1111/j.1365-2648.1994.tb01207.x>.
- [223] Hasson, Felicity, Sinead Keeney, and Hugh McKenna. 2000. "Research Guidelines for the Delphi Survey Technique." *Journal of Advanced Nursing* 32 (4): 1008–15. <https://doi.org/10.1046/j.1365-2648.2000.t01-1-01567.x>.
- [224] "What Is a Security Expert?" n.d. (ISC)² Blog. Accessed July 16, 2021. http://blog.isc2.org/isc2_blog/2015/02/what-is-a-security-expert.html.
- [225] Tran, Thien. 2000. "Strategic Evaluation of University Knowledge and Technology Transfer Effectiveness," January. <https://doi.org/10.15760/etd.1059>.
- [226] Goodman, Claire M. 1987. "The Delphi Technique: A Critique." *Journal of Advanced Nursing* 12 (6): 729–34. <https://doi.org/10.1111/j.1365-2648.1987.tb01376.x>.
- [227] Okoli, Chitu, and Suzanne D. Pawlowski. 2004. "The Delphi Method as a Research Tool: An Example, Design Considerations and Applications." *Information & Management* 42 (1): 15–29. <https://spectrum.library.concordia.ca/976864/>.

- [228] Knol, Anne B, Pauline Slottje, Jeroen P van der Sluijs, and Erik Lebret. 2010. "The Use of Expert Elicitation in Environmental Health Impact Assessment: A Seven Step Procedure." *Environmental Health* 9 (1).
<https://doi.org/10.1186/1476-069x-9-19>.
- [229] Dalkey, Norman, and Olaf Helmer. 1963. "An Experimental Application of the DELPHI Method to the Use of Experts." *Management Science* 9 (3): 458–67.
<https://doi.org/10.1287/mnsc.9.3.458>.
- [230] Preble, John F. 1984. "The Selection of Delphi Panels for Strategic Planning Purposes." *Strategic Management Journal* 5 (2): 157–70.
<https://doi.org/10.1002/smj.4250050206>.
- [231] Akins, Ralitsa B, Homer Tolson, and Bryan R Cole. 2005. "Stability of Response Characteristics of a Delphi Panel: Application of Bootstrap Data Expansion." *BMC Medical Research Methodology* 5 (1).
<https://doi.org/10.1186/1471-2288-5-37>.
- [232] "Cleland, David I. And Dundar F. Kocaoglu Engineering Management, McGraw-Hill, 1981 (CK) | Engineering | System." n.d. Scribd. Accessed July 16, 2021. <https://www.scribd.com/document/308713942/Cleland-David-I-and-Dundar-F-Kocaoglu-Engineering-Management-McGraw-Hill-1981-CK>.
- [233] Kocaoglu, Dundar. "Hierarchical decision modeling – a participative approach to technology planning, in *Proceedings of International Congress on Technology & Technology Exchange: Technology & the World Around Us*, 1984, pp. 481–482.
- [234] Portland State University, Department of Engineering and Technology Management. "HDM Software."
- [235] Abbas, Mustafa. 2016. "Consistency Analysis for Judgment Quantification in Hierarchical Decision Model." *Dissertations and Theses*, March.
<https://doi.org/10.15760/etd.2695>.

- [236] “Encyclopedia of Quantitative Risk Analysis and Assessment | Wiley.” n.d. Wiley.com. Accessed August 16, 2020. <https://www.wiley.com/en-us/Encyclopedia+of+Quantitative+Risk+Analysis+and+Assessment-p-9780470035498>.
- [237] Sheskin, David J. 2007. *Handbook of Parametric and Nonparametric Statistical Procedures*. Boca Raton, Fl: Chapman & Hall/Crc.
- [238] Bartko, John J. 1976. “On Various Intraclass Correlation Reliability Coefficients.” *Psychological Bulletin* 83 (5): 762–65. <https://doi.org/10.1037/0033-2909.83.5.762>.
- [239] Shrout, Patrick E., and Joseph L. Fleiss. 1979. “Intraclass Correlations: Uses in Assessing Rater Reliability.” *Psychological Bulletin* 86 (2): 420–28. <https://doi.org/10.1037/0033-2909.86.2.420>.
- [240] Gibson, Elizabeth. 2016. “A Measurement System for Science and Engineering Research Center Performance Evaluation.” *Dissertations and Theses*, November. <https://doi.org/10.15760/etd.3276>.
- [241] Estep, Judith. 2017. “Development of a Technology Transfer Score for Evaluating Research Proposals: Case Study of Demand Response Technologies in the Pacific Northwest.” *Dissertations and Theses*, February. <https://doi.org/10.15760/etd.5363>.
- [242] Kostoff, Ronald N. 2006. “Systematic Acceleration of Radical Discovery and Innovation in Science and Technology.” *Technological Forecasting and Social Change* 73 (8): 923–36. <https://doi.org/10.1016/j.techfore.2005.09.004>.
- [243] Geisler, Eliezer. 2002. “The Metrics of Technology Evaluation: Where We Stand and Where We Should Go from Here.” *International Journal of Technology Management* 24 (4): 341. <https://doi.org/10.1504/ijtm.2002.003060>.

- [244] Martin, Ben R. 2010. "The Origins of the Concept of 'Foresight' in Science and Technology: An Insider's Perspective." *Technological Forecasting and Social Change* 77 (9): 1438–47. <https://doi.org/10.1016/j.techfore.2010.06.009>.
- [245] Lynn, Mary R., Eve L. Layman, and Sheila P. Englebardt. 1998. "Nursing Administration Research Priorities." *The Journal of Nursing Administration* 28 (5): 7–11. <https://doi.org/10.1097/00005110-199805000-00002>.
- [246] Jones, J., and D. Hunter. 1995. "Qualitative Research: Consensus Methods for Medical and Health Services Research." *BMJ* 311 (7001): 376–80. <https://doi.org/10.1136/bmj.311.7001.376>.
- [247] Gerdasri, Nathasit. 2005. "An Analytical Approach on Building a Technology Development Envelope (TDE) for Roadmapping of Emerging Technologies." *Dissertations and Theses*.
- [248] Merrick, Jason R. W., J. Rene van Dorp, and Amita Singh. 2005. "Analysis of Correlated Expert Judgments from Extended Pairwise Comparisons." *Decision Analysis* 2 (1): 17–29. <https://doi.org/10.1287/deca.1050.0031>.
- [249] Meyer, Mary A., and Jane M. Booker. 1987. *Eliciting and Analyzing Expert Judgment: A Practical Guide*. Amazon. <https://www.amazon.com/Eliciting-Analyzing-Expert-Judgment-Probability/dp/0898714745>.
- [250] Handcock, Mark S., and Krista J. Gile. 2011. "Comment: On the Concept of Snowball Sampling." *Sociological Methodology* 41 (1): 367–71. <https://doi.org/10.1111/j.1467-9531.2011.01243.x>.
- [251] "The Sage Encyclopedia of Qualitative Research Methods." 2008. <http://www.yanchukvladimir.com/docs/Library/Sage%20Encyclopedia%20of%20Qualitative%20Research%20Methods-%202008.pdf>.

- [252] Lappas, Theodoros, Kun Liu, and Evimaria Terzi. 2009. "Finding a Team of Experts in Social Networks." *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining - KDD '09*. <https://doi.org/10.1145/1557019.1557074>.
- [253] Center for Internet Security (CIS). Accessed April 4, 2021. <https://www.cisecurity.org/>.
- [254] HealthITSecurity. 2021. "Scripps Reports Data Theft, EHR Back Online, but Global Outages Persist." HealthITSecurity. June 1, 2021. <https://healthitsecurity.com/news/attack-updates-scripps-health-ehr-back-online-global-outages-persist>.
- [255] "Does Your Board Really Understand Your Cyber Risks?" 2020. Harvard Business Review. September 1, 2020. <https://hbr.org/2020/09/does-your-board-really-understand-your-cyber-risks>.
- [256] Tsiakis, Theodosios, and George Stephanides. 2005. "The Economic Approach of Information Security." *Computers & Security* 24 (2): 105–8. <https://doi.org/10.1016/j.cose.2005.02.001>.
- [257] Vance, Anthony, Mikko T. Siponen, and Detmar W. Straub. 2020. "Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations across Cultures." *Information & Management* 57 (4): 103212. <https://doi.org/10.1016/j.im.2019.103212>.
- [258] Guo, Ken H., and Yufei Yuan. 2012. "The Effects of Multilevel Sanctions on Information Security Violations: A Mediating Model." *Information & Management* 49 (6): 320–26. <https://doi.org/10.1016/j.im.2012.08.001>.
- [259] Li, Ling, Li Xu, Wu He, Yong Chen, and Hong Chen. 2016. "Cyber Security Awareness and Its Impact on Employee's Behavior." *Lecture Notes in Business*

Information Processing, 103–11. https://doi.org/10.1007/978-3-319-49944-4_8.

- [260] “What Is Enterprise Information Portal (EIP)? - Definition from Techopedia.” n.d. Techopedia.com. <https://www.techopedia.com/definition/13775/enterprise-information-portal-eip>.
- [261] Albrechtsen, Eirik, and Jan Hovden. 2010. “Improving Information Security Awareness and Behaviour through Dialogue, Participation and Collective Reflection. An Intervention Study.” *Computers & Security* 29 (4): 432–45. <https://doi.org/10.1016/j.cose.2009.12.005>.
- [262] “American Hospital Directory - Advanced Search.” 2019. Ahd.com. 2019. <https://www.ahd.com/search.php>.
- [263] Saltelli, A., S. Tarantola, and K. P.-S. Chan. 1999. “A Quantitative Model-Independent Method for Global Sensitivity Analysis of Model Output.” *Technometrics* 41 (1): 39–56. <https://doi.org/10.1080/00401706.1999.10485594>.
- [264] Khan, Tanveer, Masoom Alam, Adnan Akhunzada, Ali Hur, Muhammad Asif, and Muhammad Khurram Khan. 2019. “Towards Augmented Proactive Cyberthreat Intelligence.” *Journal of Parallel and Distributed Computing* 124 (February): 47–59. <https://doi.org/10.1016/j.jpdc.2018.10.006>.
- [265] Wang, Yaosheng. 2020. “Network Information Security Risk Assessment Based on Artificial Intelligence.” *Journal of Physics: Conference Series* 1648 (October): 042109. <https://doi.org/10.1088/1742-6596/1648/4/042109>.
- [266] Khan, Saifull ah, Akanksha Jadhav, Indraje et Bharadwaj, Mayukh Rooj, and Sandeep Shiravale. 2020. “Blockchain and the Identity Based Encryption Scheme for High Data Security.” *2020 Fourth International Conference on*

Computing Methodologies and Communication (ICCMC), March.
<https://doi.org/10.1109/iccmc48092.2020.iccmc-000187>.

- [267] Lee, Shinho, Jung, Wookhyun, Lee Seohyun, and Tak Kim, Eui. 2020. "Malware Response Naming Scheme for Security Control Service," *2020 International Conference on Information and Communication Technology Convergence (ICTC)* pp. 1549-1552.
- [268] Skula, Bohacik and Zabovsky. 2020. "Use of Different Channels for User Awareness and Education Related to Fraud and Phishing in a Banking Institution," *2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, pp. 606-612.
- [269] FBI & HHS. "Joint cyber advisory: Activity targeting the healthcare and public sector." Accessed July 10, 2020. https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf,
- [270] Culbertson, Nick. n.d. "Council Post: Increased Cyberattacks on Healthcare Institutions Shows the Need for Greater Cybersecurity." *Forbes*.
<https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=1c991b35650d>.
- [271] Jalali, Mohammad S, Adam Landman, and William J Gordon. 2020. "Telemedicine, Privacy, and Information Security in the Age of COVID-19." *Journal of the American Medical Informatics Association*, December.
<https://doi.org/10.1093/jamia/ocaa310>.

APPENDICES

Appendix A: Research Instruments

Appendix A-1: Invitation Letter

Good Morning,

I am writing to request your assistance. I am a PhD student in Engineering and Technology Management Department (ETM) at Portland State University (PSU). I am also a peer as Chief Information Officer at Oregon Health & Science University.

I am conducting my dissertation research entitled "Healthcare Information Security Maturity Model". As part of my research, I am forming expert panels to help me validate and quantify my research model. I have identified you as an expert in the field. Your knowledge, background, experience, and expertise will be very helpful for my research.

If you agree to participate in this research, a consent form will be sent to you for signature. After I receive the signed form, I will send you web-based data collection instruments for you to provide your response. You will be asked to participate in 1-3 surveys. The surveys vary in length taking from 3 to 15 minutes each. All questions are multiple choice or ranking of items, no open-ended questions. To access the survey, you will be asked for an email address. This will be to assure no one takes the assessment twice and it is also where a free copy of your survey results will be emailed. You do not have to use your work or business email address. Your information will only be utilized for this research and will never be seen, sold, given to, or utilized outside this research (so no spam or unsolicited emails). No personally identifiable information will be utilized and your answers to the survey will be combined with every other participant.

Thank you in advance for considering my request for assistance. If you have any questions or concerns, please feel free to contact me at any time, my contact information is listed below.

Bridget Barnes Page
PhD Student
Engineering and Technology Management Department (ETM) Portland State University (PSU)
Chief Information Officer
Oregon Health & Science University
Phone: 503-702-7866
Email: pagebridget@outlook.com
barnesbr@ohsu.edu

Appendix A-2: Consent Form

Consent to Participate in Research

Project Title: Healthcare Information Security Maturity Model

Researcher: Bridget Barnes Page

Department of Engineering Management

Portland State University

Researcher Contact: pagebridget@outlook.com or barnesbr@ohsu.edu

(503) 702-7866

You are being asked to take part in a research study. The box below highlights key information about this research for you to consider when making a decision whether or not to participate. Carefully review the information provided on this form. Please ask questions about any of the information you do not understand before you decide to participate.

Key Information for You to Consider

- **Voluntary Consent.** You are being asked to volunteer for a research study. It is up to you whether you choose to participate or not. There is no penalty if you choose not to participate or discontinue participation.
- **Purpose.** The purpose of this research is to develop a multi-criteria-based measuring approach to be used in evaluating the maturity of Health Information Security at healthcare organizations.
- **Duration.** It is expected that your participation will last 20-50 minutes for responding to the research questionnaire. The questionnaires will be sent to you once or twice between March and August 2020.
- **Procedures and Activities.** You will be asked to validate or quantify the perspective, criteria, or desirability metrics listed in the research model.
- **Risks.** There are no foreseeable risks or discomforts of your participation.
- **Benefits.** Some of the benefits that may be expected include facilitation of follow up research or application or research model on your organization.
- **Alternatives.** Participation is voluntary, the only alternative is to choose not to participate.

What happens if I agree to participate?

If you agree to be in this research, your participation will include serving as one of the experts within one or two expert panels, which will help validate and quantify the research model. You may also be asked to participate as an expert to provide insight for a case study. We will tell you

about any new information that may affect your willingness to continue participation in this research.

What happens to the information collected?

Information collected for this research will be used to validate and quantify the research model or will be used for case study analysis. The information and analytical results will be documented in a PhD dissertation, which will be accessible from the university or from academic databases. Your identifiable information, such as your name, will be kept confidential.

How will my privacy and data confidentiality be protected?

We will take measures to protect your privacy including keeping your name and identifiable information hidden. Despite these precautions, we can never fully guarantee the confidentiality of all study information. Individuals and organizations that conduct or monitor this research may be permitted access to inspect research records. This may include private information. These individuals and organizations include [the Institutional Review Board that reviewed this research.

What if I want to stop participating in this research?

Your participation is voluntary. You do not have to take part in this study, but if you do, you may stop at any time. You have the right to choose not to participate in any study activity or completely withdraw from participation at any point without penalty or loss of benefits to which you are otherwise entitled. Your decision whether or not to participate will not affect your relationship with the researchers or Portland State University.

Will I be paid for participating in this research?

You will not be paid for participating in this research.

Who can answer my questions about this research?

If you have questions, concerns, or have experienced a research related injury, contact the research team at:

Bridget Barnes Page

(503) 702-7866

pagebridget@outlook.com or barnesbr@ohsu.edu

Who can I speak to about my rights as a research participant?

The Portland State University Institutional Review Board (“IRB”) is overseeing this research. The IRB is a group of people who independently review research studies to ensure the rights and welfare of participants are protected. The Office of Research Integrity is the office at Portland State University that supports the IRB. If you have questions about your rights, or wish to speak with someone other than the research team, you may contact:

Office of Research Integrity

PO Box 751

Portland, OR 97207-0751

Phone: (503) 725-5484

Toll Free: 1 (877) 480-4400

Email: psuirb@pdx.edu

Consent Statement

I have had the opportunity to read and consider the information in this form. I have asked any questions necessary to make a decision about my participation. I understand that I can ask additional questions throughout my participation.

By signing below, I understand that I am volunteering to participate in this research. I understand that I am not waiving any legal rights. I have been provided with a copy of this consent form. I understand that if my ability to consent for myself changes, either I or my legal representative may be asked to provide consent prior to me continuing in the study.

I consent to participate in this study.

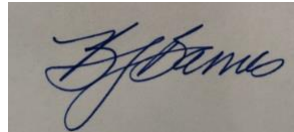
Name of Adult Participant	Signature of Adult Participant	Date
---------------------------	--------------------------------	------

Researcher Signature (to be completed at time of informed consent)

I have explained the research to the participant and answered all of his/her questions. I believe that he/she understands the information described in this consent form and freely consents to participate.

Name of Research Team Member	Signature of Research Team Member	Date
------------------------------	-----------------------------------	------

Bridget Barnes Page



3/2/21

Appendix A-3: Example of web based validation instrument



Bridget Barnes Page

Information Security Maturity Model in Healthcare Organizations in the United States

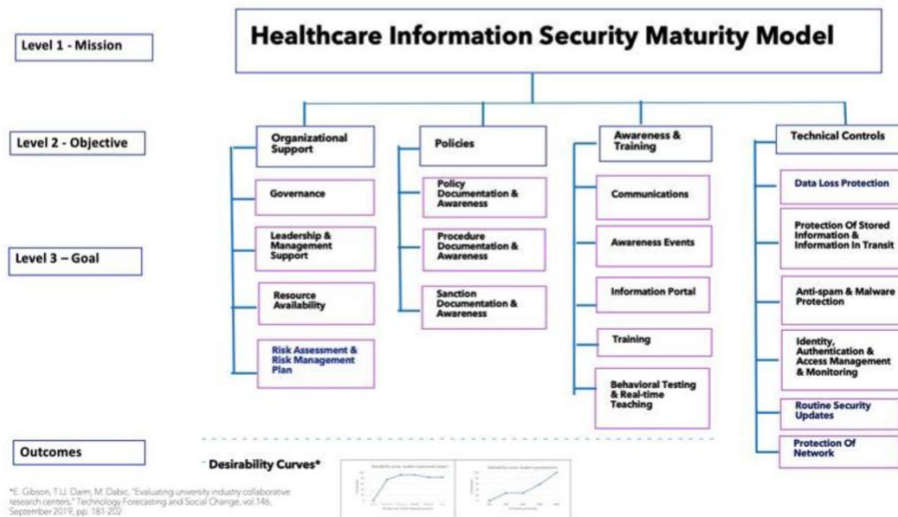
Healthcare Information Security Maturity Model

Thank you for participating in evaluating my research model as a subject matter expert.

My research goal is to create a maturity model for information security in healthcare organizations. This model would provide a framework by which healthcare organizations may: Assess their information security maturity from multiple perspectives to increase self-awareness; and Provide insight on strengths and weaknesses related to specific risk mitigation criteria in order to best focus limited resources to improve information security within their organizations.

The second step is to validate the goals within the objectives affecting information security maturity in healthcare organizations in the United States.

An illustration of the model is provided below:



Complete instrument is available from the author.

Appendix A-4: Web based judgment quantification instrument

Good Afternoon,

Thank you again for agreeing to participate in my research in the development of a Healthcare Information Security Model. Your feedback has been essential to validation of the model. I received very positive feedback and agreement with the model as well as a few suggestions for improvement. I have incorporated those suggestions for feedback in the model and am now seeking your assistance in quantifying the model. To that end, I am seeking your help once again by completing the links below to 4 more surveys. Each survey should take no more than 4 minutes to complete. These surveys are conducted in a Hierarchy Decision Model tool which, in addition to quantifying the model elements, aids calculation of any inconsistency or disagreement in the model so it looks a little different than the Qualtrics tools which was used to collect initial model validation.

In quantifying the model you will be asked to compare the importance of two model elements against one another – dividing a total “importance” score of 100 between the pair of comparison elements using a sliding bar tool. For example, one element might receive a 40 while the second comparator would receive a 60, for a total of 100, the element receiving the higher score is deemed more important than the element receiving the lower score in the pairwise comparison.

I've attached a PowerPoint presentation instruction guide for each survey that can be used as a resource to working through the survey in the event you have questions. You can also contact me directly by email or phone if you wish (contact info below).

I have also attached a copy of the visual of the revised model as well as a document which defines each element of the model in the event you wish to reference that information. In order to minimize the burden on any specific subject matter expert you have not been asked to quantify all elements of the model.

In the first survey you are asked to quantify the Objective level of the model using this link:

<http://research1.etm.pdx.edu/hdm2/expert.aspx?id=aaf147df4a072ae3/78b97ef44601a56f>

In the second survey you are asked to quantify the Goal level of the model – specifically the Organizational Support Goal using this link:

<http://research1.etm.pdx.edu/hdm2/expert.aspx?id=aaf147df4a072ae3/812c8f9631b5cf28>

In the third survey you are asked to quantify the Goal level of the model – specifically the Information Security Technical Hygiene Goal using this link:

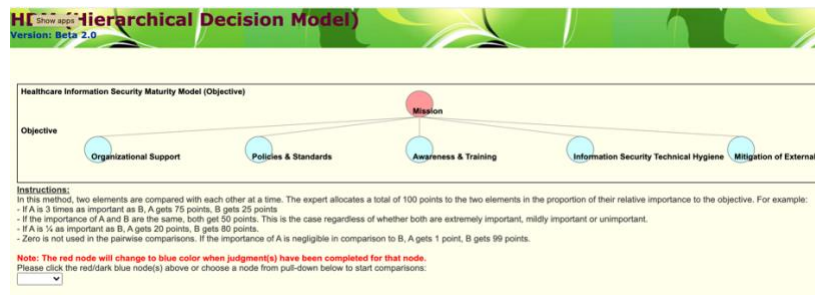
<http://research1.etm.pdx.edu/hdm2/expert.aspx?id=aaf147df4a072ae3/a76adc778c052a03>

In the fourth survey you are asked to quantify the Goal level of the model -specifically the Mitigation of External Threats Goal using this link:

<http://research1.etm.pdx.edu/hdm2/expert.aspx?id=aaf147df4a072ae3/c4d69974757abbf5>

Please know that I know your time is valuable and I am grateful for the gift of your time in participating in my research.

Bridget Barnes Page
PhD Student
Engineering and Technology Management Department (ETM) Portland State University (PSU)
Chief Information Officer
Oregon Health & Science University
Phone: 503-702-7866
Email: pagebridget@outlook.com
barnesbr@ohsu.edu



The full instrument is available from the author.

Appendix A-5: Table of research instruments

Instrument	Purpose	Data Collected	Method
Expert Invitation	Determine willingness of expert to participate in research.	Binary acceptance (yes/no)	Personal email
Consent form	Full research disclosure. Compliance with IRB standards.	Electronic signature and date	Fillable open text box form attached to personal email.
Criteria validation of Objectives	Validation of construct of content at level 2 (Objectives) of model. Data used to develop final model for data collection.	Binary acceptance (yes/no) with open text box for additional qualitative data.	Personal email with link to Qualtrics survey.
Criteria validation of Goals	Validation of construct of content at level 3 (Goals) of model. Data used to develop final model for data collection.	Binary acceptance (yes/no) with open text box for additional qualitative data.	Personal email with link to Qualtrics survey.
Model criteria validation part 2	Validation of revised model criteria based on expert feedback in first round.	Binary acceptance (yes/no)	Closed end questions during Webex interview.
Criteria Quantification for	Quantification of criteria at level 2 (Objectives) of model.	pair-wise comparison	Email invite with links to HDM software.
Criteria Quantification for	Quantification of criteria at level 3 (Goals) of model.	pair-wise comparison	Email invite with links to HDM software.
Desirability Curves Validation and Quantification	Validation and quantification of desirability curves for each output criterion.	Acceptance of metric and context. Quantified desirability values for each metric.	Webex interviews combined with Qualtrics survey.

Appendix B: Expert Panels

Appendix B-1: Expert Panel Configuration

ID#	Purpose	Expert Panel Qualification
P1	Validate and Quantify Level 2 (Objective) of Model	CIOs, CPOs, CISOs
P2	Validate and Quantify Level 3 (Organizational Support) Goal	CIOs
P3	Validate and Quantify Level 3 (Policies & Standards) Goal	CPOs, CIOs
P4	Validate and Quantify Level 3 (Awareness & Training) Goal	CPOs, CIOs
P5	Validate and Quantify Level 3 (Information Security Technical Hygiene) Goal	CISOs, CIOs
P6	Validate and Quantify Level 3 (Mitigation of External Threat) Goal	CISOs, CIOs
P7	Validate Metrics and Quantify "goodness" of data to develop desirability curves	CIOs

Appendix B-2: Expert Background

#	Role/ Expertise	Organization Type
Expert 1	Chief Information Officer	Community Hospital
Expert 2	Chief Information Officer	Large Healthcare System
Expert 3	Chief Information Officer	Academic Medical Center
Expert 4	Chief Information Officer	Community Hospital
Expert 5	Chief Information Officer	Integrated Delivery Network
Expert 6	Chief Information Officer	Integrated Delivery Network
Expert 7	Chief Information Officer	Community Hospital
Expert 8	Chief Information Officer	Community Hospital
Expert 9	Chief Information Officer	Academic Medical Center
Expert 10	Chief Information Officer	Academic Medical Center
Expert 11	Chief Information Officer	Community Hospital
Expert 12	Chief Information Officer	Integrated Delivery Network
Expert 13	Chief Information Officer	Large Healthcare System
Expert 14	Chief Information Officer	Academic Medical Center
Expert 15	Chief Information Officer	Large Healthcare System
Expert 16	Chief Information Officer	Large Healthcare System
Expert 17	Chief Information Officer	Community Hospital
Expert 18	Chief Information Officer	Integrated Delivery Network
Expert 19	Chief Information Officer	Academic Medical Center
Expert 20	Chief Information Officer	Academic Medical Center
Expert 21	Chief Information Officer	Academic Medical Center
Expert 22	Chief Information Officer	Large Healthcare System
Expert 23	Chief Information Officer	Large Healthcare System
Expert 24	Chief Information Officer	Academic Medical Center
Expert 25	Chief Information Officer	Large Healthcare System
Expert 26	Chief Information Officer	Integrated Delivery Network
Expert 27	Chief Information Officer	Academic Medical Center
Expert 28	Chief Information Officer	Community Hospital
Expert 29	Chief Information Officer	Critical Access Hospital
Expert 30	Chief Information Officer	Community Hospital
Expert 31	Chief Information Officer	Community Hospital
Expert 32	Chief Information Officer	Academic Medical Center
Expert 33	Chief Information Officer	Academic Medical Center
Expert 34	Chief Information Officer	Community Hospital
Expert 35	Chief Privacy Officer	Integrated Delivery Network
Expert 36	Chief Privacy Officer	Academic Medical Center
Expert 37	Chief Privacy Officer	Large Healthcare System
Expert 38	Chief Privacy Officer	Academic Medical Center
Expert 39	Chief Privacy Officer	Academic Medical Center
Expert 40	Chief Information Security Officer	Integrated Delivery Network
Expert 41	Chief Information Security Officer	Integrated Delivery Network
Expert 41	Chief Information Security Officer	Large Healthcare System
Expert 42	Chief Information Security Officer	Health Insurance Provider
Expert 43	Chief Information Security Officer	Large Healthcare System
Expert 44	Chief Information Security Officer	Large Healthcare System
Expert 45	Chief Information Security Officer	Large Healthcare System
Expert 46	Chief Information Security Officer	Academic Medical Center
Expert 47	Chief Information Security Officer	Academic Medical Center
Expert 48	Chief Information Security Officer	Integrated Delivery Network
Expert 49	Chief Information Security Officer	Community Hospital

Appendix B-3: Expert Panel Assignments

#	Role/ Expertise	Organization Type	Panel #1	Panel #2	Panel #3	Panel #4	Panel #5	Panel #6	Panel #7
Expert 1	Chief Information Officer	Community Hospital	x	x	x	x			
Expert 2	Chief Information Officer	Large Healthcare System	x	x	x	x			
Expert 3	Chief Information Officer	Academic Medical Center	x	x	x	x			
Expert 4	Chief Information Officer	Community Hospital	x	x	x	x			
Expert 5	Chief Information Officer	Integrated Delivery Network	x	x	x	x			
Expert 6	Chief Information Officer	Integrated Delivery Network	x	x	x	x			
Expert 7	Chief Information Officer	Community Hospital	x	x	x	x			
Expert 8	Chief Information Officer	Community Hospital	x	x	x	x			
Expert 9	Chief Information Officer	Academic Medical Center	x	x	x	x			
Expert 10	Chief Information Officer	Academic Medical Center	x	x	x	x			
Expert 11	Chief Information Officer	Community Hospital	x	x	x	x			
Expert 12	Chief Information Officer	Integrated Delivery Network	x	x	x	x			
Expert 13	Chief Information Officer	Large Healthcare System	x	x	x	x			
Expert 14	Chief Information Officer	Academic Medical Center	x	x	x	x			
Expert 15	Chief Information Officer	Large Healthcare System	x	x	x	x			
Expert 16	Chief Information Officer	Large Healthcare System	x	x	x	x			
Expert 17	Chief Information Officer	Community Hospital	x	x	x	x			
Expert 18	Chief Information Officer	Integrated Delivery Network	x	x			x	x	
Expert 19	Chief Information Officer	Academic Medical Center	x	x			x	x	
Expert 20	Chief Information Officer	Academic Medical Center	x	x			x	x	
Expert 21	Chief Information Officer	Academic Medical Center	x	x			x	x	
Expert 22	Chief Information Officer	Large Healthcare System	x	x			x	x	
Expert 23	Chief Information Officer	Large Healthcare System	x	x			x	x	
Expert 24	Chief Information Officer	Academic Medical Center	x	x			x	x	
Expert 25	Chief Information Officer	Large Healthcare System	x	x			x	x	x
Expert 26	Chief Information Officer	Integrated Delivery Network	x	x			x	x	x
Expert 27	Chief Information Officer	Academic Medical Center	x	x			x	x	x
Expert 28	Chief Information Officer	Community Hospital	x	x			x	x	x
Expert 29	Chief Information Officer	Critical Access Hospital	x	x			x	x	x
Expert 30	Chief Information Officer	Community Hospital	x	x			x	x	
Expert 31	Chief Information Officer	Community Hospital	x	x			x	x	
Expert 32	Chief Information Officer	Academic Medical Center	x	x			x	x	
Expert 33	Chief Information Officer	Academic Medical Center	x	x			x	x	
Expert 34	Chief Information Officer	Community Hospital	x	x			x	x	
Expert 35	Chief Privacy Officer	Integrated Delivery Network	x		x	x			
Expert 36	Chief Privacy Officer	Academic Medical Center	x		x	x			
Expert 37	Chief Privacy Officer	Large Healthcare System	x		x	x			
Expert 38	Chief Privacy Officer	Academic Medical Center	x		x	x			
Expert 39	Chief Privacy Officer	Academic Medical Center	x		x	x			
Expert 40	Chief Information Security Officer	Integrated Delivery Network	x				x	x	
Expert 41	Chief Information Security Officer	Integrated Delivery Network	x				x	x	
Expert 41	Chief Information Security Officer	Large Healthcare System	x				x	x	
Expert 42	Chief Information Security Officer	Health Insurance Provider	x				x	x	
Expert 43	Chief Information Security Officer	Large Healthcare System	x				x	x	
Expert 44	Chief Information Security Officer	Large Healthcare System	x				x	x	
Expert 45	Chief Information Security Officer	Large Healthcare System	x				x	x	
Expert 46	Chief Information Security Officer	Academic Medical Center	x				x	x	
Expert 47	Chief Information Security Officer	Academic Medical Center	x				x	x	
Expert 48	Chief Information Security Officer	Integrated Delivery Network	x				x	x	
Expert 49	Chief Information Security Officer	Community Hospital	x				x	x	

Appendix C: Validation Data

Appendix C-1: Validation Data at Level 2 (Objective)

Objective	# responses	Yes	No	% agreement
Organization Support	50	50	0	100%
Policies	50	49	1	98%
Awareness & Training	50	50	0	100%
Technical Controls	50	50	0	100%



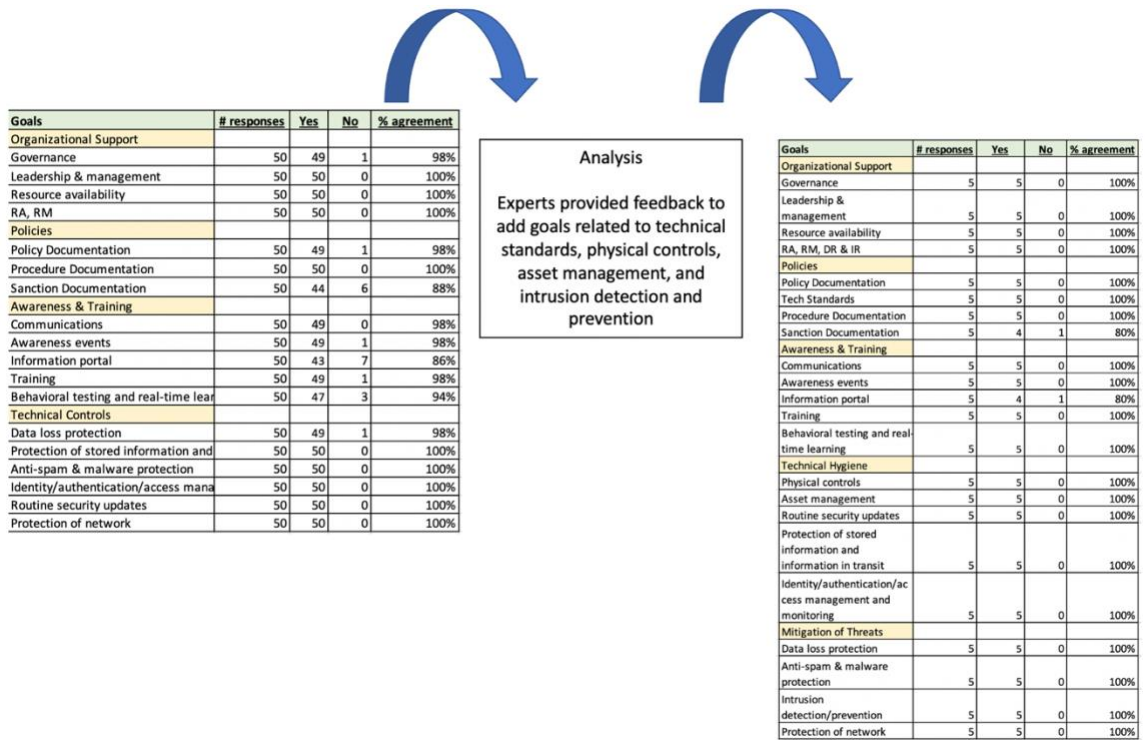
Analysis

Increase in number of “technical controls”
required splitting of objective into two discrete
technically focused objectives



Objective	# responses	Yes	No	% agreement
Organization Support	5	5	0	100%
Policies & Standards	5	5	0	100%
Awareness & Training	5	5	0	100%
Technical Hygiene	5	5	0	100%
Mitigation of Threats	5	5	0	100%

Appendix C-2: Validation Data for Level 3 (Goals)



Appendix C-3: Validation Data for Level 4 (Outputs)

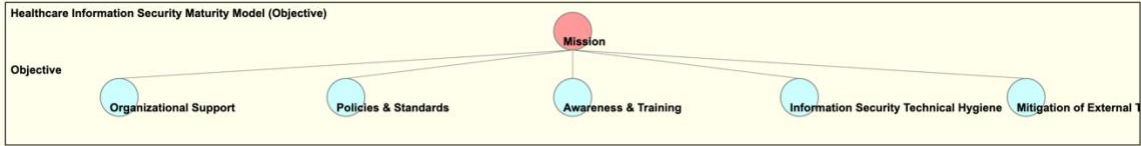
Metrics	# responses	Yes	No	% agreement
Organizational Support				
Governance				
There is no governance related to information security at organization.	5	5	0	100%
The organization has a limited governance structure related to information security, with some defined policies, roles and responsibilities.	5	5	0	100%
The organization has well established policies related to information security as well as defined roles and responsibilities.	5	5	0	100%
The organization has well established information security governance which includes routine monitoring and measurement of performance associated with a defined strategic plan.	5	5	0	100%
The organization has a comprehensive governance structure which includes aligning information security strategies to business objectives.	5	5	0	100%
Leadership & management				
Organizational management and leadership is uninterested in or unaware of information security policies, practices, performance.	5	5	0	100%
Organization leaders and managers have some awareness of the need for information security and understand their role in supporting information security through policies and practices.	5	5	0	100%
Organizational leaders and managers act as model for expectations of behavior related to information security best practices.	5	5	0	100%
Organizational leaders and managers are actively engaged in information security governance process, policy and procedures, ensuring alignment with business objectives.	5	5	0	100%
Organizational leadership at the highest level receive routine updates regarding information security performance across the organization and provide support for information security through dedication of resources and personal behaviors.	5	5	0	100%
Resource availability				
There are no specific resources dedicated to information security at organization.	5	5	0	100%
There are a few resources available to support information security at the organization, but there are no resources dedicated exclusively to information security.	5	5	0	100%
The organization has a dedicated information security team that provides support for information security tools.	5	5	0	100%
The organization has a dedicated information security team that supports operational information security tools, provides information security training to organizational members and conducts routine information security assessments.	5	5	0	100%
There are robust resources committed to information security which allow not only maintenance and monitoring of existing system but also consistent improvement in information security posture of the organization.	5	5	0	100%
RA, RM, DR & IR				
The organization does not conduct information security risks assessments or have an information security risk management plan.	5	5	0	100%
The organization conducts infrequent risk assessments and has not developed a risk management plan for information security.	5	5	0	100%
The organization conducts routine risk assessments and has developed a risk management plan for information security.	5	5	0	100%
The organization conducts routine risk assessment and has a risk management plan for information security that is actively monitored and managed. The organization also has a disaster recovery and/or incident response plan.	5	5	0	100%
The organization conducts routine risk assessments, has a risk management plan for information security that is actively monitored and engages with national standards organizations to benchmark performance against others. The organization also has a disaster recovery and/or incident response plan.	5	5	0	100%
Policies & Standards				
Policy Documentation				
The organization has no policy documentation related to information security.	5	5	0	100%
The organization has some documentation related to information security policies.	5	5	0	100%
The organization has well documented policies related to information security but they are not well known to organizational members.	5	5	0	100%
The organization has a comprehensive set of information security policies which are regularly updated and well understood by members of the organization.	5	5	0	100%
Tech Standards Documentation				
The organization has no procedure documentation related to information security.	5	5	0	100%
The organization has some documentation related to information security procedures.	5	5	0	100%
The organization has well documented procedures related to information security but they are not well known to organizational members.	5	5	0	100%
Organization has a comprehensive set of information security procedures which are regularly updated and well understood by members of the organization.	5	5	0	100%
Procedure Documentation				
The organization has no technical standards documentation related to information security.	5	5	0	100%
The organization has some documentation related to information security technical standards.	5	5	0	100%
The organization has well documented technical standards related to information security but they are not well known to organizational members.	5	5	0	100%
Organization has a comprehensive set of technical standards related to information security which are regularly updated and well understood by members of the organization.	5	5	0	100%
Sanction Documentation				
The organization has no documentation or awareness related to sanctions that may be implemented as a result of non-compliance with information security policies.	5	5	0	100%
The organization has some documentation related to sanctions that may be implemented as a result of non-compliance with information security policies.	5	5	0	100%
The organization has completed documentation of sanctions that may be implemented as a result of non-compliance with information security policies but they are not well known to organizational members or are not implemented in an equitable way.	5	5	0	100%
The organization has well documented and broadly known sanctions guidance associated with information security policy violations. The defined sanctions are believed to be fair by organizational members and are applied equitably by the organization.	5	5	0	100%

Metrics	# responses	Yes	No	% agreement
Awareness & Training				
Communications				
The organization does not communicate information about information security threats or expectations.	5	5	0	100%
The organization provides limited or inconsistent communication related to information security threats and expectations.	5	5	0	100%
The organization provides regular communication through a single channel (e.g., employee newsletter) related to information security threats and expectations.	5	5	0	100%
The organization provides regular communication through multiple print or digital channels (e.g. newsletters, posters, blogs) but does not create forums for in-person delivery of information related to information security threats and expectations.	5	5	0	100%
The organization has dedicated communication resources for information security that create and deliver content about the current state of information security, changes to information security threats, tools, policies and procedures. Communication is delivered on a regular basis through multiple communication channels including print, digital and in-person delivery.	5	5	0	100%
Awareness events				
The organization does not host information security awareness events.	5	5	0	100%
The organization hosts limited (e.g. small group) or inconsistent security awareness events.	5	5	0	100%
The organization hosts regular security awareness events that are not well known or attended by organizational members.	5	5	0	100%
The organization hosts regular security awareness events that are well attended by small groups of organizational members.	5	5	0	100%
The organization hosts regular security awareness events. Some events are uniquely designed to appeal to discrete stakeholder types (e.g., web-developers) and others are large security awareness events which are well attended by large numbers of organizational members.	5	5	0	100%
Information portal				
The organization does not have a digital presence/portal focused on information security as part of a broader communication toolkit.	5	5	0	100%
The organization has a digital presence/portal which provides limited information (e.g. only minimal information regarding information security policies).	5	5	0	100%
The organization has a digital presence/portal which provides comprehensive information related to information security policies, procedures, sanctions, and tools, but is not well known to organizational members.	5	5	0	100%
The organization has a digital presence/portal which provides comprehensive information related to information security policies, procedures and tools, which is well known to organizational members.	5	5	0	100%
The organization has a digital presence/portal which provides comprehensive information related to information security policies, procedures and tools, and where to get additional help or ask questions. The portal is frequently visited and seen as a valuable resource by organizational members.	5	5	0	100%
Training				
The organization provides no training related to information security threats or expectations.	5	5	0	100%
The organization provides a single, annual, online training related to information security threats and expectations which is optional.	5	5	0	100%
The organization provides annual online training related to information security threats and expectations which is mandatory for all organizational members.	5	5	0	100%
The organization provides annual online training related to information security threats and expectations which is mandatory for all organizational members. In addition, the organization provides small group training upon request.	5	5	0	100%
The organization provides a combination of computer-based training, small group training, and one-on-one training upon request related to information security threats, expectations and best practices. The organization proactively identifies individuals and/or groups who may need additional ad-hoc training and provides those services regularly. At least one annual training is required of all organizational members.	5	5	0	100%
Behavioral testing and real-time learning				
The organization provides no behavioral testing or real-time teaching related to information security threats or expectations.	5	5	0	100%
The organization provides limited or inconsistent behavioral testing or real-time teaching related to information security threats and expectations.	5	5	0	100%
The organization provides consistent behavioral testing or real-time teaching related to information security threats and expectations through a single channel (e.g. phishing) but does not share results broadly or shames those organizational members who perform poorly.	5	5	0	100%
The organization provides consistent behavioral testing or real-time teaching related to information security threats and expectations through multiple channels (e.g. phishing, USB drops) but does not share results broadly or shames those organizational members who perform poorly.	5	5	0	100%
The organization regularly and frequently tests members compliance with information security policies, procedures, best practices. Tests are conducted through a variety of delivery mechanisms (e.g. phishing tests, USB drops). Results of individual tests are shared with individual organizational members in real-time privately to avoid blaming/shaming and encourage learning. Organizational members who repeatedly fail behavioral tests are offered personal coaching. Organization wide performance related to behavioral compliance is shared broadly with all members to increase awareness and associated compliance.	5	5	0	100%

Metrics	# responses	Yes	No	% agreement
Technical Hygiene				
Physical controls				
The organization regularly and frequently tests members compliance with information security policies, procedures, best practices. Tests are conducted through a variety of delivery mechanisms (e.g. phishing tests, USB drops). Results of individual tests are shared with individual organizational members in real-time privately to avoid blaming/shaming and encourage learning. Organizational members who repeatedly fail behavioral tests are offered personal coaching. Organization wide performance related to behavioral compliance is shared broadly with all members to increase awareness and associated compliance.	5	5	0	100%
The organization has some physical controls that limit access to technology infrastructure and/or confidential information (e.g., locked doors in some locations, badge access to highly sensitive areas).	5	5	0	100%
The organization has comprehensive physical controls that limit access to technology infrastructure and/or confidential information.	5	5	0	100%
The organization has comprehensive physical controls that limit access to technology infrastructure and/or confidential information which are actively monitored by information security or public safety professionals.	5	5	0	100%
Asset management				
The organization has no tools, processes or staffing to provide asset management capabilities for physical and virtual technology assets (hardware and software).	5	5	0	100%
The organization has some tools, process or staffing to support limited asset management capabilities for physical and virtual technology assets (hardware and software).	5	5	0	100%
The organization has tools, processes, and staffing to support asset management for most but not all physical and virtual technical assets (hardware and software).	5	5	0	100%
The organization has comprehensive tools, processes and staffing to support full life cycle management related to all physical and virtual technology assets (hardware and software).	5	5	0	100%
Routine security updates				
The organization does not perform routine information security patching/updates.	5	5	0	100%
The organization performs periodic information security patching/updates and may have technical tools which aid in identifying required patching.	5	5	0	100%
The organization performs routine information security patching and updating and has technical tools which aid in identifying required patching, but often fails to meet patching updates as frequently as defined in service level agreements or policies or is unable to patch all software, end points, servers, operating systems, bio-medical devices.	5	5	0	100%
The organization has a robust information security patching/updates process in place with defined roles and responsibilities to patch all systems and devices across the enterprise. Information security patching/updates is completed as defined in service level agreements or policies.	5	5	0	100%
Protection of stored information and information in transit				
The organization has no technical tools to support protection of stored information and information in transit.	5	5	0	100%
The organization has some tools to support protection of stored information and information in transit.	5	5	0	100%
The organization has comprehensive tools to support stored information and information in transit for applications and systems that are on-premise.	5	5	0	100%
The organization has comprehensive tools which are actively monitored by information security professionals to support protection of stored information and information in transit for applications and systems that are on-premise as well as cloud-based platforms.	5	5	0	100%
Identity/authentication/access management and monitoring				
The organization has no technical tools to support identity, authentication or access management and monitoring.	5	5	0	100%
The organization has some tools to support authentication and access management capabilities.	5	5	0	100%
The organization has some tools to support protection of stored information and access management capabilities.	5	5	0	100%
The organization has comprehensive tools which are actively monitored by information security professionals to support identity, authentication and access management in both on-premise and cloud-based platforms.	5	5	0	100%
Mitigation of Threats				
Data loss protection				
The organization has no technical tools to support data loss protection.	5	5	0	100%
The organization has some tools to support data loss protection.	5	5	0	100%
The organization has comprehensive tools to support data loss protection for applications and systems that are on-premise.	5	5	0	100%
The organization has comprehensive tools which are actively monitored by information security professionals to support data loss protection for applications and systems that are on-premise as well as cloud-based platforms.	5	5	0	100%
Anti-spam & malware protection				
The organization has no technical tools to provide anti-spam or malware protection capabilities.	5	5	0	100%
The organization has some tools to support anti-spam protection capabilities.	5	5	0	100%
The organization has some tools to support both anti-spam and malware protection capabilities.	5	5	0	100%
The organization has comprehensive tools which are actively monitored by information security professionals to support both anti-spam and malware protection in both on-premise and cloud-based platforms.	5	5	0	100%
Intrusion detection/prevention				
The organization has no technical tools to provide intrusion detection and prevention capabilities.	5	5	0	100%
The organization has some tools to support intrusion prevention capabilities.	5	5	0	100%
The organization has some tools to support both intrusion prevention and intrusion detection capabilities.	5	5	0	100%
The organization has comprehensive tools and staffing to support a 24x7 Intrusion detection and prevention (a.k.a. Managed Detection Response) program utilizing a Security Information and Event Manage system.	5	5	0	100%
Protection of network				
The organization has no technical tools to support network protection capabilities.	5	5	0	100%
The organization has a limited set of tools to support network protection capabilities (e.g., firewalls, network access control).	5	5	0	100%
The organization has both basic and some advanced tools to support network protection capabilities (e.g., firewalls, network access controls, routine vulnerability scanning, network segmentation).	5	5	0	100%
The organization has comprehensive tools which are actively monitored by information security professionals to support protection of network.	5	5	0	100%

Appendix D: Quantification Data Collection Instrument and Data

Appendix D-1: Quantification of Level 2 (Objectives)*



Mission	Organizational Support	Policies & Standards	Awareness & Training	Information Security Technical Hygiene	Mitigation of External Threats	Inconsistency
0.17	0.1	0.29	0.24	0.2	0.01	
0.19	0.12	0.25	0.26	0.18	0.02	
0.19	0.12	0.19	0.29	0.2	0.02	
0.2	0.16	0.15	0.18	0.31	0.04	
0.27	0.07	0.2	0.16	0.3	0.01	
0.23	0.14	0.18	0.27	0.18	0.01	
0.27	0.14	0.17	0.2	0.22	0.01	
0.16	0.03	0.12	0.28	0.4	0.11	
0.13	0.2	0.18	0.22	0.27	0.02	
0.08	0.15	0.2	0.27	0.29	0.03	
0.17	0.21	0.24	0.16	0.21	0.02	
0.19	0.12	0.16	0.27	0.27	0	
0.1	0.14	0.21	0.23	0.33	0.02	
0.13	0.1	0.12	0.34	0.32	0.03	
0.17	0.13	0.24	0.24	0.21	0.02	
0.25	0.18	0.16	0.21	0.21	0	
0.21	0.08	0.16	0.28	0.27	0.09	
0.19	0.13	0.11	0.26	0.31	0.01	
0.18	0.14	0.27	0.15	0.27	0.03	
0.23	0.1	0.18	0.34	0.15	0.01	
0.18	0.12	0.28	0.14	0.28	0.06	
0.17	0.17	0.18	0.23	0.25	0	
0.3	0.15	0.15	0.25	0.15	0.1	
0.21	0.17	0.2	0.24	0.19	0.02	
0.14	0.13	0.18	0.4	0.16	0.02	
0.23	0.08	0.19	0.27	0.23	0.01	
0.18	0.17	0.21	0.22	0.22	0.05	
0.2	0.2	0.2	0.2	0.2	0	
0.22	0.18	0.15	0.25	0.2	0	
Mean	0.19	0.14	0.19	0.24	0.24	
Minimum	0.08	0.03	0.11	0.14	0.15	
Maximum	0.3	0.21	0.29	0.4	0.4	
Std. Deviation	0.05	0.04	0.05	0.06	0.06	
Disagreement					0.048	

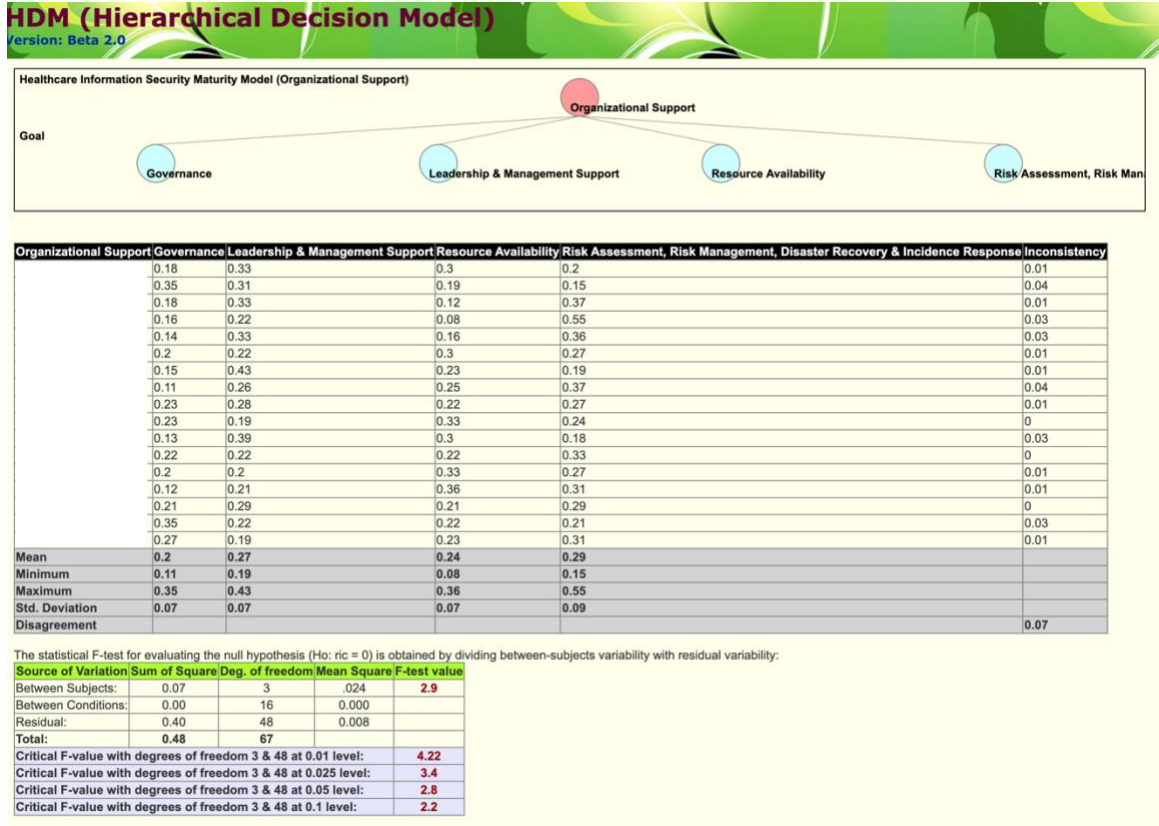
The statistical F-test for evaluating the null hypothesis (Ho: ric = 0) is obtained by dividing between-subjects variability with residual variability:

Source of Variation	Sum of Square	Deg. of freedom	Mean Square	F-test value
Between Subjects:	0.23	4	.057	17.19
Between Conditions:	0.00	28	0.000	
Residual:	0.37	112	0.003	
Total:	0.60	144		
Critical F-value with degrees of freedom 4 & 112 at 0.01 level:				3.49
Critical F-value with degrees of freedom 4 & 112 at 0.025 level:				2.9
Critical F-value with degrees of freedom 4 & 112 at 0.05 level:				2.45
Critical F-value with degrees of freedom 4 & 112 at 0.1 level:				2

* expert identification information has been removed from the far left hand column to protect anonymity

Appendix D-2: Quantification of Level 3 (Goals) *

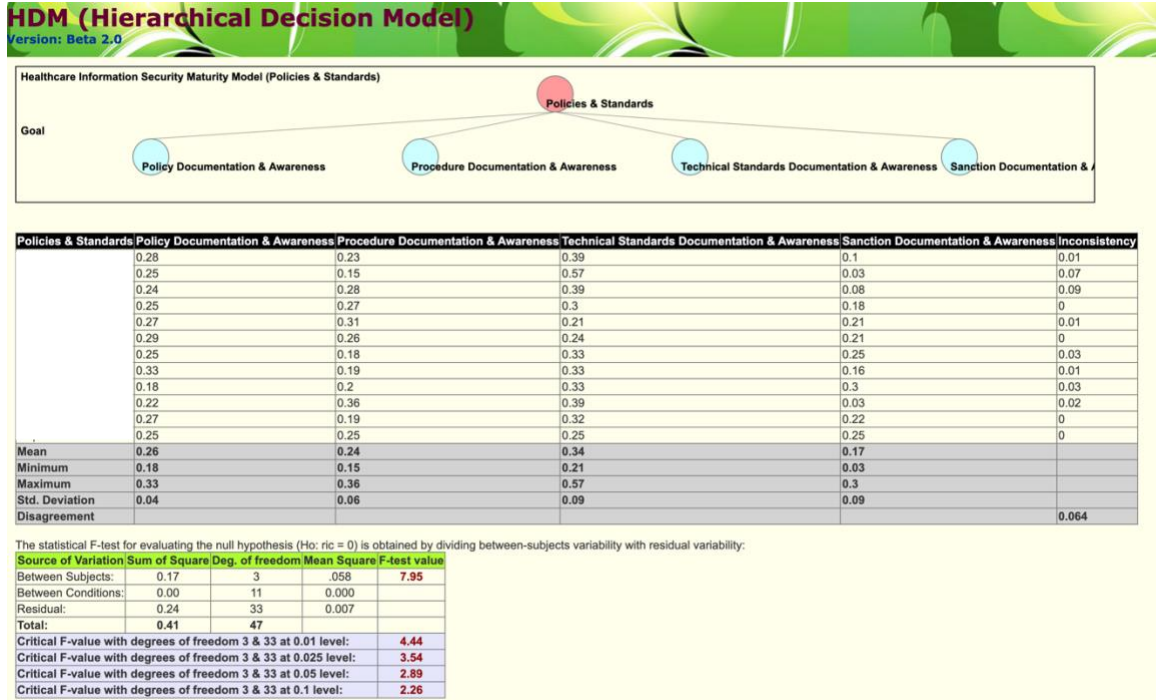
Appendix D-2-1: Organizational Support Goal



* expert identification information has been removed from the far left hand column to protect anonymity

Appendix D-2: Quantification of Level 3 (Goals) *

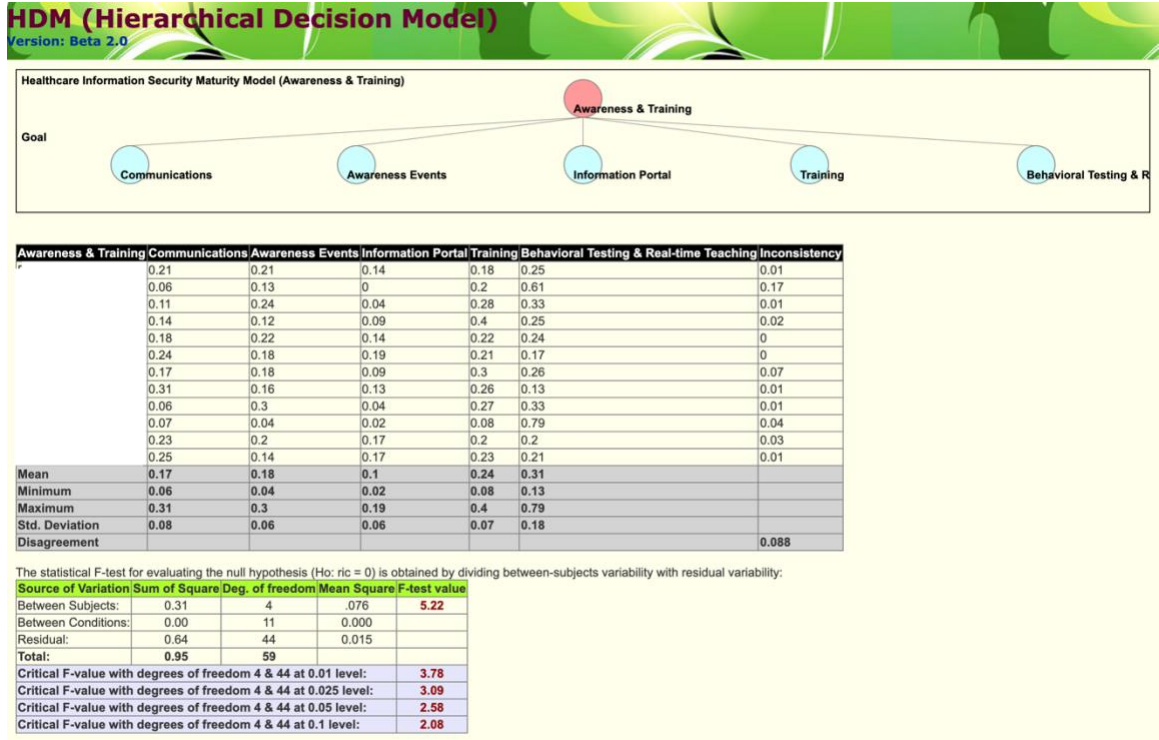
Appendix D-2-2: Policies & Standards Goal



* expert identification information has been removed from the far left hand column to protect anonymity

Appendix D-2: Quantification of Level 3 (Goals) *

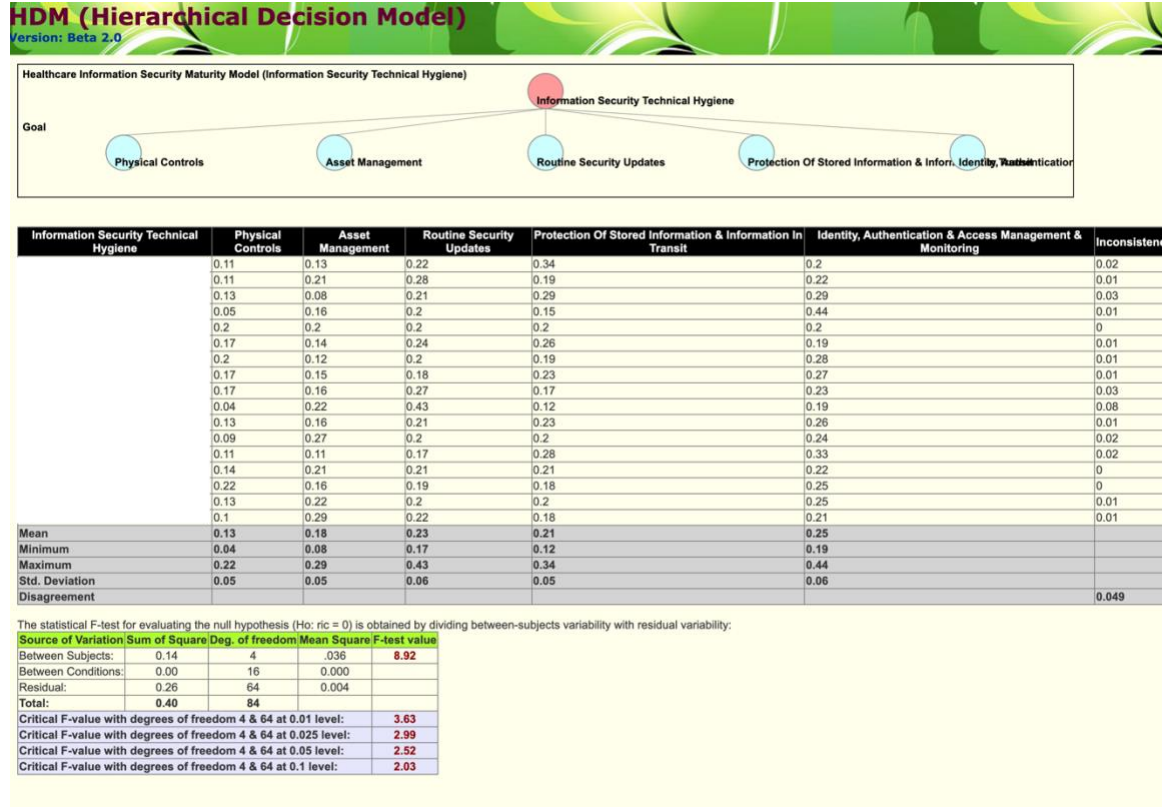
Appendix D-2-3: Training & Awareness Goal



* expert identification information has been removed from the far left hand column to protect anonymity

Appendix D-2: Quantification of Level 3 (Goals) *

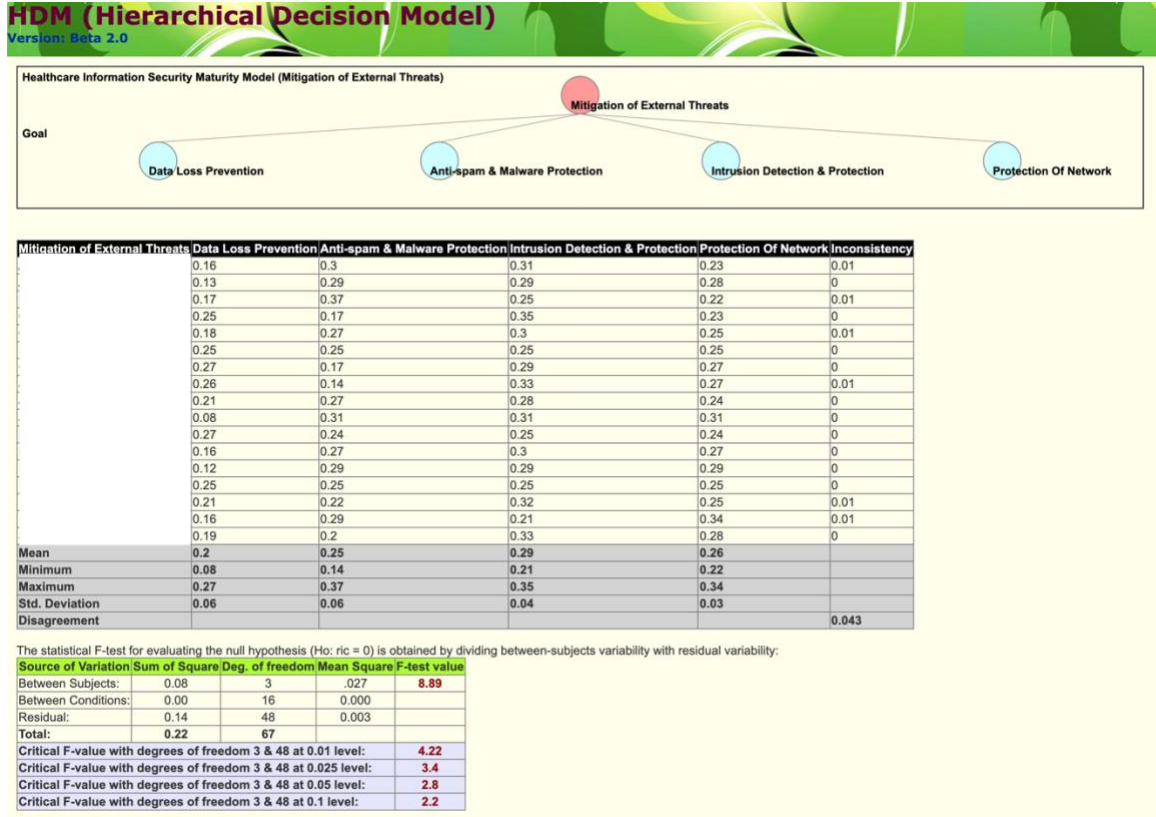
Appendix D-2-4: Technical Hygiene Goal



* expert identification information has been removed from the far left hand column to protect anonymity

Appendix D-2: Quantification of Level 3 (Goals) *

Appendix D-2-5: Mitigation of External Threat Goal



* expert identification information has been removed from the far left hand column to protect anonymity

Appendix D-3: Quantification Data Entry and Analysis Tool

The HDM 2.0 © software is used to quantify the expert data. This figure below shows the interface that experts used to conduct the pair-wise comparison for the Organizational Support objective (as an example).

HDM (Hierarchical Decision Model)
Version: Beta 2.0

Healthcare Information Security Maturity Model (Organizational Support)

```
graph TD; OS((Organizational Support)) --- G((Governance)); OS --- LMS((Leadership & Management Support)); OS --- RA((Resource Availability)); OS --- RMDR((Risk Assessment, Risk Management, Disaster Recovery & Incidence Response));
```

[Show Instructions](#)

Please give your judgment for each pair of nodes below toward Organizational Support:

Leadership & Management Support	<input type="text" value="50"/>	<input type="text" value="50"/>	Governance
	<input type="text" value="1"/>	<input type="text" value="1"/>	

Resource Availability	<input type="text" value="50"/>	<input type="text" value="50"/>	Governance
	<input type="text" value="1"/>	<input type="text" value="1"/>	

Risk Assessment, Risk Management, Disaster Recovery & Incidence Response	<input type="text" value="50"/>	<input type="text" value="50"/>	Governance
	<input type="text" value="1"/>	<input type="text" value="1"/>	

Resource Availability	<input type="text" value="50"/>	<input type="text" value="50"/>	Leadership & Management Support
	<input type="text" value="1"/>	<input type="text" value="1"/>	

Risk Assessment, Risk Management, Disaster Recovery & Incidence Response	<input type="text" value="50"/>	<input type="text" value="50"/>	Leadership & Management Support
	<input type="text" value="1"/>	<input type="text" value="1"/>	

Risk Assessment, Risk Management, Disaster Recovery & Incidence Response	<input type="text" value="50"/>	<input type="text" value="50"/>	Resource Availability
	<input type="text" value="1"/>	<input type="text" value="1"/>	

Appendix E: Desirability Curves Data Collection Tool & Data

Appendix E-1: Desirability Curve Data Collection Instrument (limited sample for technical hygiene)



Bridget Barnes

Information Security Maturity Model in Healthcare Organizations in the United States

Thank you for participating in evaluating my research model as a subject matter expert.

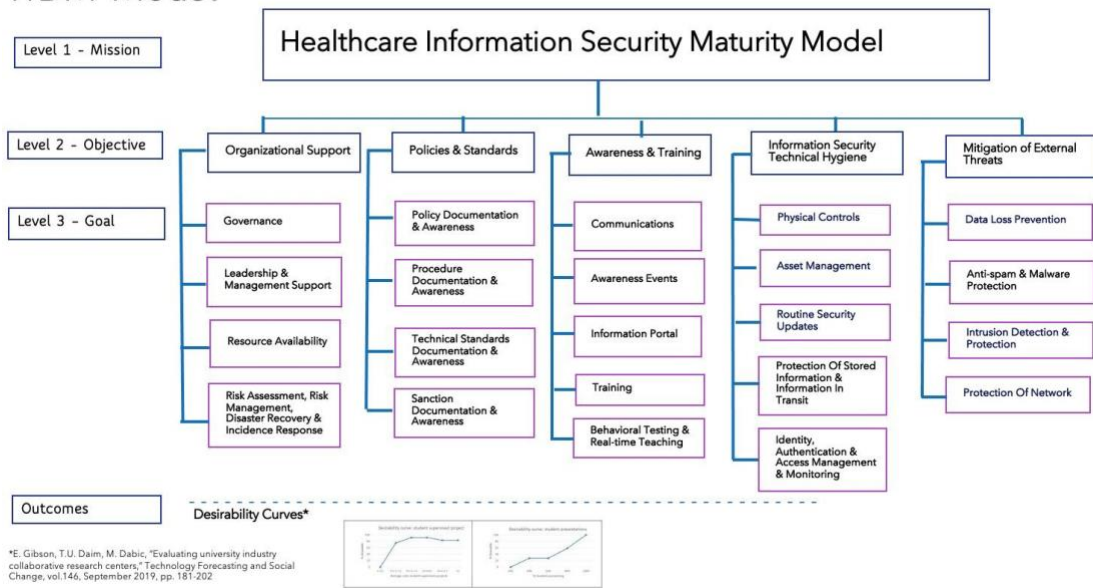
My research goal is to create a maturity model for information security in healthcare organizations. This model would provide a framework by which healthcare organizations may:

- Assess their information security maturity from multiple perspectives to increase self-awareness; and
- Provide insight on strengths and weaknesses related to specific risk mitigation criteria in order to best focus limited resources to improve information security within their organizations.

During this part of the data collection, your assessment of each criterion in the model will be used to develop desirability curves, quantifying the elements associated with information security maturity.

An illustration of the model is provided below:

HDM Model



Objective description:

	Objective	Definition	
Information Security Maturity	Organizational support for information security	Organization has high level of support for information security, including support at the Board level of the organization. Support is demonstrated by engagement and understanding of information security risk modeling behaviors and by financial support.	(Johnson & E. Goetz, 2007), (Brady, 2010), (Bunker, 2012), (Da Veiga & Martins, 2015), (Bowen, 2006), (Tsiakis & Stephanides, 2005), (Huang, 2008), (Alnatheer et al., 2012), (ONC 2015), (CIS, 2021), (Vance et al., 2020)
	Information security policies and standards	Organization has documented information security policies and procedures and updates them routinely.	(Alnatheer et al., 2012), (Rotvold, 2008), (D'Arcy et al., 2009), (Bunker, 2012), (Bulgurcu, 2010), (White, 2009), (CIS, 2021), (NIST, 2021), (ISO, 2021), (Guo & Yuan, 2012), (Vance et al., 2020)
	Information security awareness and training	Workforce members have access to training and possess understanding and acceptance about the need for all organizational members to protect information assets of the organization and mitigate risks associated with information security.	(Bada et al., 2015), (Da Veiga & Martins, 2015), (Albarak, 2011), (Brady, 2010), (Alnatheer et al., 2012), (Pierce et al., 2013), (D'Arcy et al., 2009), (Bunker, 2012), (Karjalainen & Siponen, 2011), (Albrechtsen & Hayden, 2010), (Rotvold, 2008)
	Information security technical hygiene	Organization has implemented technology and process controls to maintain system health and improve information security.	(HITRUST, 2018), (CIS, 2021), (ONC, 2015), (NIST, 2021)
	Mitigation of external threats	Organization has implemented technical controls to mitigate external information security threats.	(HITRUST, 2018), (CIS, 2021), (ONC, 2015), (NIST, 2021)

Please enter your name:

Name

Last Name

Information Security Technical Hygiene

Objective	Goals	Short Definition	References
Information Security Technical Hygiene	Physical Controls	Physical access controls which limit access to technology infrastructure (equipment/media) or confidential information. Examples include, but are not limited to, locked barriers, badged access, security cameras.	(HITRUST, 2018), (CIS, 2021), (ONC, 2015), (NIST, 2021)
	Asset management	Technology that supports life cycle management related to physical and virtual technology assets.	(HITRUST, 2018), (CIS, 2021), (ONC, 2015), (NIST, 2021)
	Routine security updates	Processes and technical tools that facilitate routine security updates for software, endpoints, bio-medical devices, and other systems.	(HITRUST, 2018), (CIS, 2021), (NIST, 2021)
	Protection of stored information and information in transit	Technology that ensures data at rest and in transit is not vulnerable to misuse (e.g. encryption technologies).	(HITRUST, 2018), (CIS, 2021), (ONC, 2015), (NIST, 2021)
	Identity/authentication/access management and monitoring	Technical tools that ensure only those that need to access sensitive data and systems are able to do so.	(HITRUST, 2018), (CIS, 2021), (ONC, 2015), (NIST, 2021)

Please provide a metric score from 0 (least favorable state) to 100 (most favorable state) for each possible state noted.

Physical Controls

What level of physical controls are established at organization?

Physical Controls

What level of physical controls are established at organization?

Quantification

0 10 20 30 40 50 60 70 80 90 100

The organization has no physical controls that limit access to technology infrastructure and/or confidential information.

The organization has some physical controls that limit access to technology infrastructure and/or confidential information (e.g., locked doors in some locations, badge access to highly sensitive areas).

The organization has comprehensive physical controls that limit access to technology infrastructure and/or confidential information.

The organization has comprehensive physical controls that limit access to technology infrastructure and/or confidential information which are actively monitored by information security or public safety professionals.

The full instrument is available from the author.

Appendix E-2: Desirability Curve Definition and Values

Table E-2-1: Organizational Support – Governance

Goal	Metric / Level	Desirability
Governance	no governance related to information security	0
	limited governance structure related to information security	15.75
	well established policies, roles and responsibilities related to information security	63.75
	well established information security governance including monitoring and measurement	83.75
	comprehensive governance structure which includes aligning information security strategies to business objectives.	100

Table E-2-2: Organizational Support – Leadership & Management Support

Goal	Metric / Level	Desirability
Leadership & Management Support	management and leadership is uninterested in or unaware of information security policies, practices, performance.	0
	leaders and managers have some awareness of the need for information security and understand their role	20
	leaders and managers act as model for expectations of behavior related to information security best practices	65
	leaders and managers are actively engaged in information security governance ensuring alignment with business objectives	83.75
	leadership at the highest level receives routine updates regarding information security performance	100

Table E-2-3: Organizational Support – Resource Availability

Goal	Metric / Level	Desirability
Resource Availability	no specific resources dedicated to information security	0
	few, but no dedicated resources available to support information security	16.25
	dedicated information security team that provides support for information security tools	52.5
	dedicated information security team that supports tools, training and routine information security assessments	80
	robust resources committed to information security supporting maintenance, monitoring and improvement in information security	100

Table E-2-4: Organizational Support – Risk Assessment, Risk Management, Disaster Recovery and Incident Response

Goal	Metric / Level	Desirability
Risk Assessment, Risk Management, Disaster Recovery, & Incidence Response	No information security risks assessments or risk management plan	0
	infrequent risk assessments and no risk management plan for information security	12.5
	routine risk assessments and a risk management plan for information security	55
	routine risk assessment and risk management plan for information security, plus disaster recovery and/or incident response plan	83.75
	routine risk assessment, risk management plan (includes national benchmarking), disaster recovery and incident response plan	100

Table E-2-5: Policies and Standards – Policy Documentation and Awareness

Goal	Metric / Level	Desirability
Policy Doc & Aware	no policy documentation related to information security	0
	some documentation related to information security policies	17.5
	well documented policies related to information security but they are not well known to organizational members	57.5
	comprehensive set of information security policies which are regularly updated and well understood by members	100

Table E-2-6: Policies and Standards – Procedure Documentation and Awareness

Goal	Metric / Level	Desirability
Procedure Doc & Aware	no procedure documentation related to information security	0
	some documentation related to information security procedures	27.75
	well documented procedures related to information security but they are not well known to organizational members	55.75
	comprehensive set of information security procedures which are regularly updated and well understood by members	100

Table E-2-7: Policies and Standards – Technical Standards Documentation and Awareness

Goal	Metric / Level	Desirability
Technical Standards Doc & Aware	no technical standards documentation related to information security	0
	some documentation related to information security technical standards	23.75
	well documented technical standards related to information security but they are not well known to organizational members	55
	comprehensive set of information security technical standards which are regularly updated and well understood by members	100

Table E-2-8: Policies and Standards – Sanctions Documentation and Awareness

Goal	Metric / Level	Desirability
Sanctions Doc & Aware	no sanction documentation related to information security	0
	some documentation related to information security sanctions	20
	well documented sanctions related to information security but they are not well known to organizational members	62.5
	comprehensive set of information security sanctions which are regularly updated and well understood by members	100

Table E-2-9: Training & Awareness – Communications

Goal	Metric / Level	Desirability
Communications	no communication related to information security threats or expectations	0
	limited or inconsistent communication related to information security threats and expectations	13.75
	regular communication through a single channel related to information security threats and expectations	41.25
	regular communication through multiple channels related to information security threats and expectations	68.75
	dedicated communication resources for information security that create and deliver content related to information security	100

Table E-2-10: Training & Awareness – Awareness Events

Goal	Metric / Level	Desirability
Awareness Events	no information security awareness events	0
	limited or inconsistent security awareness events	18.75
	regular information security awareness events that are not well known or attended by organizational members	42.5
	regular information security awareness events that are well attended by small groups of organizational members	73.75
	regular, well attended information security awareness events, some uniquely designed to appeal to discrete stakeholders	100

Table E-2-11: Training & Awareness – Informational Portal

Goal	Metric / Level	Desirability
Information Portal	No digital presence/portal focused on information security as part of a broader communication toolkit	0
	digital presence/portal which provides limited information regarding information security policies	18.75
	digital presence/portal provides comprehensive information related to information security, not well known to members	42.5
	digital presence/portal provides comprehensive information related to information security, well known to members	80
	digital presence/portal provides comprehensive information related to information security, actively used by members	100

Table E-2-12: Training & Awareness – Training

Goal	Metric / Level	Desirability
Training	no training related to information security threats or expectations	0
	single, annual, online training related to information security threats and expectations which is optional	26.25
	annual online training related to information security threats and expectations which is mandatory	47.5
	annual online training for information security threats and expectations which is mandatory and small group training upon request	78.75
	diverse and comprehensive training related to information security threats, expectations and best practices	100

Table E-2-13: Training & Awareness – Behavioral Testing and Real-time Teaching

Goal	Metric / Level	Desirability
Behavioral Testing & RT Teaching	no behavioral testing or real-time teaching related to information security threats or expectations	0
	limited or inconsistent behavioral testing or real-time teaching related to information security threats and expectations	15
	consistent behavioral testing or real-time teaching delivered through a single channel, results not broadly shared	38.75
	consistent behavioral testing or real-time teaching through multiple channels, results not broadly shared	67.5
	regularly and frequently tests for information security compliance through diverse channels, results broadly shared	100

Table E-2-14: Technical Hygiene – Physical Controls

Goal	Metric / Level	Desirability
Physical Controls	no physical controls that limit access to technology infrastructure and/or confidential information	0
	some physical controls that limit access to technology infrastructure and/or confidential information	28.75
	comprehensive physical controls that limit access to technology infrastructure and/or confidential information	77.75
	comprehensive physical controls that limit access to technology infrastructure and/or confidential information, actively monitored	100

T

able E-2-15: Technical Hygiene – Asset Management

Goal	Metric / Level	Desirability
Asset Management	no tools, processes or staffing to provide asset management capabilities for physical and virtual technology assets	0
	some tools, process or staffing to support limited asset management capabilities for physical and virtual technology assets	26.25
	tools, processes, and staffing to support asset management for most but not all physical and virtual technical assets	76.25
	comprehensive tools, processes and staffing to support full life cycle management for all physical and virtual technology assets	100

Table E-2-16: Technical Hygiene – Routine Security Updates

Goal	Metric / Level	Desirability
Routine Security Updates	no routine information security patching/updating	0
	periodic information security patching/updating and may have technical tools which aid in identifying required patching	30
	routine information security patching and updating, but often fails to meet patching updates as frequently as defined in SLAs	75
	robust information security patching/updating for all systems and devices across the enterprise	100

Table E-2-17: Technical Hygiene – Protection of Stored Info & Info in Transit

Goal	Metric / Level	Desirability
Protect Stored Info & Info in Transit	no technical tools to support protection of stored information and information in transit	0
	some tools to support protection of stored information and information in transit	33.75
	comprehensive tools to support stored information and information in transit for applications and systems that are on-premise	68.75
	comprehensive tools for protection of stored information and information in transit for systems that are on-prem & in the "cloud"	100

Table E-2-18: Technical Hygiene – Identity, Authentication and Access Management & Monitoring

Goal	Metric / Level	Desirability
Identity, Authentication, Access	no technical tools to support identity, authentication or access management and monitoring	0
	some tools to support authentication and access management capabilities	28.75
	some tools to support identity, authentication and access management capabilities	65
	comprehensive tools to support identity, authentication and access management in both on-premise and cloud-based platforms	100

Table E-2-19: Mitigation of External Threats – Data Loss Prevention

Goal	Metric / Level	Desirability
Data Loss Protection	no technical tools to support data loss protection	0
	some tools to support data loss protection	16.25
	comprehensive tools to support data loss protection for applications and systems that are on-premise	70
	comprehensive tools to support data loss protection for systems that are on-premise as well as cloud-based platforms	100

Table E-2-20: Mitigation of External Threats – Anti-spam and Malware Protection

Goal	Metric / Level	Desirability
Anti-spam & Malware Protection	no technical tools to provide anti-spam or malware protection capabilities	0
	some tools to support anti-spam protection capabilities	16.25
	some tools to support both anti-spam and malware protection capabilities	50
	comprehensive tools to support both anti-spam and malware protection in both on-premise and cloud-based platforms	100

Table E-2-21: Mitigation of External Threats – Intrusion Detection & Prevention

Goal	Metric / Level	Desirability
Intrusion Detection & Prevention	no technical tools to provide intrusion detection and prevention capabilities	0
	some tools to support intrusion prevention capabilities	13.75
	some tools to support both intrusion prevention and intrusion detection capabilities	57.5
	comprehensive tools and staffing to support a 24x7 Intrusion detection and prevention	100

Table E-2-22: Mitigation of External Threats – Protection of Network

Goal	Metric / Level	Desirability
Protection of Network	no technical tools to support network protection capabilities	0
	limited set of tools to support network protection capabilities	18.75
	has both basic and some advanced tools to support network protection capabilities	72.75
	comprehensive tools which are actively monitored by information security professionals to support protection of network	100

Appendix F: Case Study Data

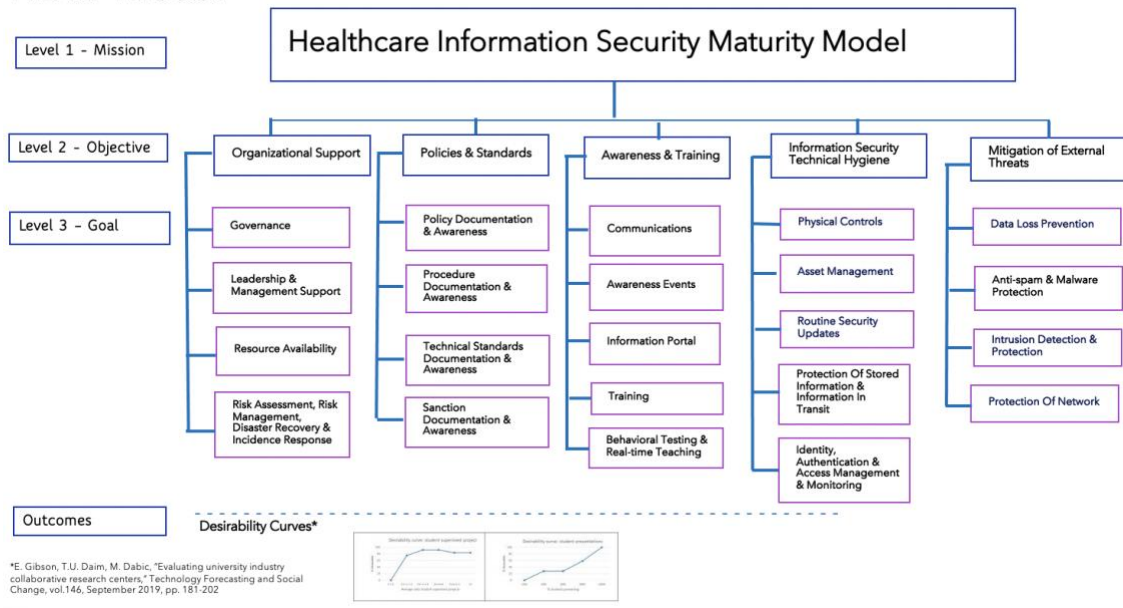
Appendix F-1: Data Collection Instrument

Healthcare Information Security Maturity Model – Case Study Interview

Thank you for agreeing to serve as a case study for the healthcare information security maturity model which I have developed with the help of subject matter experts from across the country.

Over the next 30 minutes I will ask you a series of questions related to each information security goal within the model. The comprehensive model is provided below to provide context for the assessment.

HDM Model



*E. Gibson, T.U. Daim, M. Dabic, "Evaluating university industry collaborative research centers," Technology Forecasting and Social Change, vol.146, September 2019, pp. 181-202

You will be asked to rate your organization along a spectrum of maturity for each goal within the model by answering the question noted below. As we move through the levels noted below you can think of them as advancing – i.e., level “c” is more advanced than level “a”, level “e” is more advanced than level “c”. Please select the BEST answer for your organization, understanding that no answer may be exactly perfect in representing your organization.

The first set of questions relate to **Organizational Support** for information security:

Governance

What level of governance for information security is established at your organization?

- a) There is no governance related to information security at organization.
- b) The organization has a limited governance structure related to information security, with some defined policies, roles and responsibilities.
- c) The organization has well established policies related to information security as well as defined roles and responsibilities.
- d) The organization has well established information security governance which includes routine monitoring and measurement of performance associated with a defined strategic plan.
- e) The organization has a comprehensive governance structure which includes aligning information security strategies to business objectives.

Leadership and management support

What level of leadership and management support for information security is available at organization?

- a) Organizational management and leadership is uninterested in or unaware of information security policies, practices, performance.
- b) Organization leaders and managers have some awareness of the need for information security and understand their role in supporting information security through policies and practices.
- c) Organizational leaders and managers act as model for expectations of behavior related to information security best practices.
- d) Organizational leaders and managers are actively engaged in information security governance process, policy and procedures, ensuring alignment with business objectives.
- e) Organizational leadership at the highest level receive routine updates regarding information security performance across the organization and provide support for information security through dedication of resources and personal behaviors.

Resource availability

What level of access to resources for information security are available at organization?

- a) There are no specific resources dedicated to information security at organization.
- b) There are a few resources available to support information security at the organization, but there are no resources dedicated exclusively to information security.
- c) The organization has a dedicated information security team that provides support for information security tools.
- d) The organization has a dedicated information security team that supports operational information security tools, provides information security training to organizational members and conducts routine information security assessments.
- e) There are robust resources committed to information security which allow not only maintenance and monitoring of existing system but also consistent improvement in information security posture of the organization.

Risk assessment, risk management plan, disaster recovery and incident response

What level of risk assessment, risk management, disaster recovery and incident response plans for information security are available at organization?

- a) The organization does not conduct information security risks assessments or have an information security risk management plan.
- b) The organization conducts infrequent risk assessments and has not developed a risk management plan for information security.
- c) The organization conducts routine risk assessments and has developed a risk management plan for information security.
- d) The organization conducts routine risk assessment and has a risk management plan for information security that is actively monitored and managed. The organization also has a disaster recovery and/or incident response plan.
- e) The organization conducts routine risk assessments, has a risk management plan for information security that is actively monitored and engages with national standards organizations to benchmark performance against others. The organization also has a disaster recovery and/or incident response plan.

The next set of questions relate to ***Policies & Standards*** for information security:

Policy documentation and awareness

What level of policy documentation and awareness related to information security is established at organization?

- a) The organization has no policy documentation related to information security.
- b) The organization has some documentation related to information security policies.
- c) The organization has well documented policies related to information security but they are not well known to organizational members.
- d) The organization has a comprehensive set of information security policies which are regularly updated and well understood by members of the organization.

Procedure documentation and awareness

What level of information security procedure documentation and awareness is established at organization?

- a) The organization has no procedure documentation related to information security.
- b) The organization has some documentation related to information security procedures.
- c) The organization has well documented procedures related to information security but they are not well known to organizational members.
- d) Organization has a comprehensive set of information security procedures which are regularly updated and well understood by members of the organization.

Technical standard documentation and awareness

What level of information security procedure documentation and awareness is established at organization?

- a) The organization has no technical standards documentation related to information security.
- b) The organization has some documentation related to information security technical standards.
- c) The organization has well documented technical standards related to information security but they are not well known to organizational members.
- d) Organization has a comprehensive set of technical standards related to information security which are regularly updated and well understood by members of the organization.

Sanction documentation and awareness

What level of sanction documentation and awareness related to information security is established at organization?

- a) The organization has no documentation or awareness related to sanctions that may be implemented as a result of non-compliance with information security policies.
- b) The organization has some documentation related to sanctions that may be implemented as a result of non-compliance with information security policies.
- c) The organization has completed documentation of sanctions that may be implemented as a result of non-compliance with information security policies but they are not well known to organizational members or are not implemented in an equitable way.
- d) The organization has well documented and broadly known sanctions guidance associated with information security policy violations. The defined sanctions are believed to be fair by organizational members and are applied equitably by the organization.

The next set of questions relate to ***Awareness & Training*** for information security:

Communications

What level of information security communications are established at organization?

- a) The organization does not communicate information about information security threats or expectations.
- b) The organization provides limited or inconsistent communication related to information security threats and expectations.
- c) The organization provides regular communication through a single channel (e.g., employee newsletter) related to information security threats and expectations.
- d) The organization provides regular communication through multiple print or digital channels (e.g. newsletters, posters, blogs) but does not create forums for in-person delivery of information related to information security threats and expectations.
- e) The organization has dedicated communication resources for information security that create and deliver content about the current state of information security, changes to information security threats, tools, policies and procedures. Communication is delivered on a regular basis through multiple communication channels including print, digital and in-person delivery.

Awareness events

What level of information security awareness events are established at organization?

- a) The organization does not host information security awareness events.
- b) The organization hosts limited (e.g. small group) or inconsistent security awareness events.
- c) The organization hosts regular security awareness events that are not well known or attended by organizational members.
- d) The organization hosts regular security awareness events that are well attended by small groups of organizational members.
- e) The organization hosts regular security awareness events. Some events are uniquely designed to appeal to discrete stakeholder types (e.g., web-developers) and others are large security awareness events which are well attended by large numbers of organizational members.

Information portal

What level of an information security portal is established at organization?

- a) The organization does not have a digital presence/portal focused on information security as part of a broader communication toolkit.
- b) The organization has a digital presence/portal which provides limited information (e.g. only minimal information regarding information security policies).
- c) The organization has a digital presence/portal which provides comprehensive information related to information security policies, procedures, sanctions, and tools, but is not well known to organizational members.
- d) The organization has a digital presence/portal which provides comprehensive information related to information security policies, procedures and tools, which is well known to organizational members
- e) The organization has a digital presence/portal which provides comprehensive information related to information security policies, procedures and tools, and where to get additional help or ask questions. The portal is frequently visited and seen as a valuable resource by organizational members.

Training

What level of information security training is established at organization?

- a) The organization provides no training related to information security threats or expectations.
- b) The organization provides a single, annual, online training related to information security threats and expectations which is optional.
- c) The organization provides annual online training related to information security threats and expectations which is mandatory for all organizational members.
- d) The organization provides annual online training related to information security threats and expectations which is mandatory for all organizational members. In addition, the organization provides small group training upon request.
- e) The organization provides a combination of computer-based training, small group training, and one-on-one training upon request related to information security threats, expectations

and best practices. The organization proactively identifies individuals and/or groups who may need additional ad-hoc training and provides those services regularly. At least one annual training is required of all organizational members.

Behavioral testing and real-time teaching

What level of information security behavioral testing and real-time teaching is established at organization?

- a) The organization provides no behavioral testing or real-time teaching related to information security threats or expectations.
- b) The organization provides limited or inconsistent behavioral testing or real-time teaching related to information security threats and expectations.
- c) The organization provides consistent behavioral testing or real-time teaching related to information security threats and expectations through a single channel (e.g. phishing) but does not share results broadly or shames those organizational members who perform poorly.
- d) The organization provides consistent behavioral testing or real-time teaching related to information security threats and expectations through multiple channels (e.g. phishing, USB drops) but does not share results broadly or shames those organizational members who perform poorly.
- e) The organization regularly and frequently tests members compliance with information security policies, procedures, best practices. Tests are conducted through a variety of delivery mechanisms (e.g. phishing tests, USB drops). Results of individual tests are shared with individual organizational members in real-time privately to avoid blaming/shaming and encourage learning. Organizational members who repeatedly fail behavioral tests are offered personal coaching. Organization wide performance related to behavioral compliance is shared broadly with all members to increase awareness and associated compliance.

The next set of questions relate to **Technical Hygiene** for information security:

Physical Controls

What level of physical controls are established at organization?

- a) The organization has no physical controls that limit access to technology infrastructure and/or confidential information.
- b) The organization has some physical controls that limit access to technology infrastructure and/or confidential information (e.g., locked doors in some locations, badge access to highly sensitive areas).
- c) The organization has comprehensive physical controls that limit access to technology infrastructure and/or confidential information.
- d) The organization has comprehensive physical controls that limit access to technology infrastructure and/or confidential information which are actively monitored by information security or public safety professionals.

Asset Management

What level of asset management for physical and virtual technology assets is established at organization?

- a) The organization has no tools, processes or staffing to provide asset management capabilities for physical and virtual technology assets (hardware and software).
- b) The organization has some tools, process or staffing to support limited asset management capabilities for physical and virtual technology assets (hardware and software).
- c) The organization has tools, processes, and staffing to support asset management for most but not all physical and virtual technical assets (hardware and software).
- d) The organization has comprehensive tools, processes and staffing to support full life cycle management related to all physical and virtual technology assets (hardware and software).

Routine security updates

What level of routine information security updating is established at organization?

- a) The organization does not perform routine information security patching/updating.
- b) The organization performs periodic information security patching/updating and may have technical tools which aid in identifying required patching.
- c) The organization performs routine information security patching and updating and has technical tools which aid in identifying required patching, but often fails to meet patching updates as frequently as defined in service level agreements or policies or is unable to patch all software, end points, servers, operating systems, bio-medical devices.
- d) The organization has a robust information security patching/updating process in place with defined roles and responsibilities to patch all systems and devices across the enterprise. Information security patching/updating is completed as defined in service level agreements or policies.

Protection of Stored Information and Information in Transit

What level of protection of stored information and information in transit is established at organization?

- a) The organization has no technical tools to support protection of stored information and information in transit.
- b) The organization has some tools to support protection of stored information and information in transit.
- c) The organization has comprehensive tools to support stored information and information in transit for applications and systems that are on-premise.
- d) The organization has comprehensive tools which are actively monitored by information security professionals to support protection of stored information and information in transit for applications and systems that are on-premise as well as cloud-based platforms.

Identity/Authentication/Access Management and Monitoring

What level of identity, authentication, access management and access monitoring is established at organization?

- a) The organization has no technical tools to support identity, authentication or access management and monitoring.
- b) The organization has some tools to support authentication and access management capabilities.
- c) The organization has some tools to support identity, authentication and access management capabilities.
- d) The organization has comprehensive tools which are actively monitored by information security professionals to support identity, authentication and access management in both on-premise and cloud-based platforms.

The next set of questions relate to *Mitigation of External Threats* for information security:

Data Loss Protection

What level of data loss protection is established at organization?

- a) The organization has no technical tools to support data loss protection.
- b) The organization has some tools to support data loss protection.
- c) The organization has comprehensive tools to support data loss protection for applications and systems that are on-premise.
- d) The organization has comprehensive tools which are actively monitored by information security professionals to support data loss protection for applications and systems that are on-premise as well as cloud-based platforms.

Anti-spam and malware protection

What level of anti-spam and malware protection is established at organization?

- a) The organization has no technical tools to provide anti-spam or malware protection capabilities.
- b) The organization has some tools to support anti-spam protection capabilities.
- c) The organization has some tools to support both anti-spam and malware protection capabilities.
- d) The organization has comprehensive tools which are actively monitored by information security professionals to support both anti-spam and malware protection in both on-premise and cloud-based platforms.

Intrusion detection and prevention

What level of intrusion detection and prevention is established at organization?

- a) The organization has no technical tools to provide intrusion detection and prevention capabilities.
- b) The organization has some tools to support intrusion prevention capabilities.
- c) The organization has some tools to support both intrusion prevention and intrusion detection capabilities.

- d) The organization has comprehensive tools and staffing to support a 24x7 Intrusion detection and prevention (a.k.a. Managed Detection Response) program utilizing a Security Information and Event Manage system.

Protection of network

What level of network protection is established at organization?

- a) The organization has no technical tools to support network protection capabilities.
- b) The organization has a limited set of tools to support network protection capabilities (e.g., firewalls, network access control).
- c) The organization has both basic and some advanced tools to support network protection capabilities (e.g., firewalls, network access controls, routine vulnerability scanning, network segmentation).
- d) The organization has comprehensive tools which are actively monitored by information security professionals to support protection of network.

We have now reached the conclusion of the maturity model-based questions.

Can you share with me what key next steps your organization plans to move forward with or that you would like to implement to improve your information security posture?

Appendix G: Sensitivity Scenario Data

Baseline for Stand-alone Community Hospital						
Perspective	O Weight	Criteria	Local W	Global W	D score	Score= GW*D
Organizational Support	0.19	Governance	0.20	0.04	0.64	0.02
		Leadership & Management Support	0.27	0.05	0.65	0.03
		Resource Availability	0.24	0.05	0.80	0.04
		Risk Assessment, Risk Mgmt, DR, and IR	0.29	0.06	0.55	0.03
Policies & Standards	0.14	Policy Documentation & Awareness	0.26	0.04	0.58	0.02
		Procedure Documentation & Awareness	0.24	0.03	0.28	0.01
		Technical Standards Doc & Awareness	0.34	0.05	0.24	0.01
		Sanction Documentation & Awareness	0.17	0.02	1.00	0.02
Awareness & Training	0.19	Communications	0.17	0.03	0.69	0.02
		Awareness Events	0.18	0.03	0.74	0.03
		Information Portal	0.10	0.02	0.19	0.00
		Training	0.24	0.05	0.79	0.04
		Behavioral Testing & Real-time Teaching	0.31	0.06	0.68	0.04
Technical Hygiene	0.24	Physical Controls	0.13	0.03	0.78	0.02
		Asset Management	0.18	0.04	0.26	0.01
		Routine Security Updates	0.23	0.06	0.75	0.04
		Protection of Store Info & Info in Transit	0.21	0.05	0.69	0.03
		Identity, Authentication, Access Mgmt	0.25	0.06	0.65	0.04
Mitigation of External Threats	0.24	Data Loss Prevention	0.20	0.05	0.70	0.03
		Anti-spam & Malware Protection	0.25	0.06	1.00	0.06
		Intrusion Detection & Protection	0.29	0.07	0.58	0.04
		Protection of Network	0.26	0.06	0.73	0.05
						0.65

Change Priority Weight Focused on Organizational Support for Stand-alone Community Hospital						
Perspective	P Weight	Criteria	Local W	Global W	D score	Score= GW*D
Organizational Support	0.96	Governance	0.20	0.19	0.64	0.12
		Leadership & Management Support	0.27	0.26	0.65	0.17
		Resource Availability	0.24	0.23	0.80	0.18
		Risk Assessment, Risk Mgmt, DR, and IR	0.29	0.28	0.55	0.15
Policies & Standards	0.01	Policy Documentation & Awareness	0.26	0.00	0.58	0.00
		Procedure Documentation & Awareness	0.24	0.00	0.28	0.00
		Technical Standards Doc & Awareness	0.34	0.00	0.24	0.00
		Sanction Documentation & Awareness	0.17	0.00	1.00	0.00
Awareness & Training	0.01	Communications	0.17	0.00	0.69	0.00
		Awareness Events	0.18	0.00	0.74	0.00
		Information Portal	0.10	0.00	0.19	0.00
		Training	0.24	0.00	0.79	0.00
		Behavioral Testing & Real-time Teaching	0.31	0.00	0.68	0.00
Technical Hygiene	0.01	Physical Controls	0.13	0.00	0.78	0.00
		Asset Management	0.18	0.00	0.26	0.00
		Routine Security Updates	0.23	0.00	0.75	0.00
		Protection of Store Info & Info in Transit	0.21	0.00	0.69	0.00
		Identity, Authentication, Access Mgmt	0.25	0.00	0.65	0.00
Mitigation of External Threats	0.01	Data Loss Prevention	0.20	0.00	0.70	0.00
		Anti-spam & Malware Protection	0.25	0.00	1.00	0.00
		Intrusion Detection & Protection	0.29	0.00	0.58	0.00
		Protection of Network	0.26	0.00	0.73	0.00
						0.65

Change Priority Weight Focused on Policies & Standards for Stand-alone Community Hospital						
Perspective	P Weight	Criteria	Local W	Global W	D score	Score= GW*D
Organizational Support	0.01	Governance	0.20	0.00	0.64	0.00
		Leadership & Management Support	0.27	0.00	0.65	0.00
		Resource Availability	0.24	0.00	0.80	0.00
		Risk Assessment, Risk Mgmt, DR, and IR	0.29	0.00	0.55	0.00
Policies & Standards	0.96	Policy Documentation & Awareness	0.26	0.25	0.58	0.14
		Procedure Documentation & Awareness	0.24	0.23	0.28	0.06
		Technical Standards Doc & Awareness	0.34	0.33	0.24	0.08
		Sanction Documentation & Awareness	0.17	0.16	1.00	0.16
Awareness & Training	0.01	Communications	0.17	0.00	0.69	0.00
		Awareness Events	0.18	0.00	0.74	0.00
		Information Portal	0.10	0.00	0.19	0.00
		Training	0.24	0.00	0.79	0.00
		Behavioral Testing & Real-time Teaching	0.31	0.00	0.68	0.00
Technical Hygiene	0.01	Physical Controls	0.13	0.00	0.78	0.00
		Asset Management	0.18	0.00	0.26	0.00
		Routine Security Updates	0.23	0.00	0.75	0.00
		Protection of Store Info & Info in Transit	0.21	0.00	0.69	0.00
		Identity, Authentication, Access Mgmt	0.25	0.00	0.65	0.00
Mitigation of External Threats	0.01	Data Loss Prevention	0.20	0.00	0.70	0.00
		Anti-spam & Malware Protection	0.25	0.00	1.00	0.00
		Intrusion Detection & Protection	0.29	0.00	0.58	0.00
		Protection of Network	0.26	0.00	0.73	0.00
						0.48

Change Priority Weight Focused on Awareness & Training for Stand-alone Community Hospital						
Perspective	P Weight	Criteria	Local W	Global W	D score	Score= GW*D
Organizational Support	0.01	Governance	0.20	0.00	0.64	0.00
		Leadership & Management Support	0.27	0.00	0.65	0.00
		Resource Availability	0.24	0.00	0.80	0.00
		Risk Assessment, Risk Mgmt, DR, and IR	0.29	0.00	0.55	0.00
Policies & Standards	0.01	Policy Documentation & Awareness	0.26	0.00	0.58	0.00
		Procedure Documentation & Awareness	0.24	0.00	0.28	0.00
		Technical Standards Doc & Awareness	0.34	0.00	0.24	0.00
		Sanction Documentation & Awareness	0.17	0.00	1.00	0.00
Awareness & Training	0.96	Communications	0.17	0.16	0.69	0.11
		Awareness Events	0.18	0.17	0.74	0.13
		Information Portal	0.10	0.10	0.19	0.02
		Training	0.24	0.23	0.79	0.18
		Behavioral Testing & Real-time Teaching	0.31	0.30	0.68	0.20
Technical Hygiene	0.01	Physical Controls	0.13	0.00	0.78	0.00
		Asset Management	0.18	0.00	0.26	0.00
		Routine Security Updates	0.23	0.00	0.75	0.00
		Protection of Store Info & Info in Transit	0.21	0.00	0.69	0.00
		Identity, Authentication, Access Mgmt	0.25	0.00	0.65	0.00
Mitigation of External Threats	0.01	Data Loss Prevention	0.20	0.00	0.70	0.00
		Anti-spam & Malware Protection	0.25	0.00	1.00	0.00
		Intrusion Detection & Protection	0.29	0.00	0.58	0.00
		Protection of Network	0.26	0.00	0.73	0.00
						0.66

Change Priority Weight Focused on Mitigation of Threats for Stand-alone Community Hospital						
Perspective	P Weight	Criteria	Local W	Global W	D score	Score= GW*D
Organizational Support	0.01	Governance	0.20	0.00	0.64	0.00
		Leadership & Management Support	0.27	0.00	0.65	0.00
		Resource Availability	0.24	0.00	0.80	0.00
		Risk Assessment, Risk Mgmt, DR, and IR	0.29	0.00	0.55	0.00
Policies & Standards	0.01	Policy Documentation & Awareness	0.26	0.00	0.58	0.00
		Procedure Documentation & Awareness	0.24	0.00	0.28	0.00
		Technical Standards Doc & Awareness	0.34	0.00	0.24	0.00
		Sanction Documentation & Awareness	0.17	0.00	1.00	0.00
Awareness & Training	0.01	Communications	0.17	0.00	0.69	0.00
		Awareness Events	0.18	0.00	0.74	0.00
		Information Portal	0.10	0.00	0.19	0.00
		Training	0.24	0.00	0.79	0.00
Technical Hygiene	0.01	Behavioral Testing & Real-time Teaching	0.31	0.00	0.68	0.00
		Physical Controls	0.13	0.00	0.78	0.00
		Asset Management	0.18	0.00	0.26	0.00
		Routine Security Updates	0.23	0.00	0.75	0.00
Mitigation of External Threats	0.96	Protection of Store Info & Info in Transit	0.21	0.00	0.69	0.00
		Identity, Authentication, Access Mgmt	0.25	0.00	0.65	0.00
		Data Loss Prevention	0.20	0.19	0.70	0.13
		Anti-spam & Malware Protection	0.25	0.24	1.00	0.24
						0.16
						0.18
						0.73
						0.26
						0.74

Change Priority Weight Focused on Technical Hygiene for Stand-alone Community Hospital						
Perspective	P Weight	Criteria	Local W	Global W	D score	Score= GW*D
Organizational Support	0.01	Governance	0.20	0.00	0.64	0.00
		Leadership & Management Support	0.27	0.00	0.65	0.00
		Resource Availability	0.24	0.00	0.80	0.00
		Risk Assessment, Risk Mgmt, DR, and IR	0.29	0.00	0.55	0.00
Policies & Standards	0.01	Policy Documentation & Awareness	0.26	0.00	0.58	0.00
		Procedure Documentation & Awareness	0.24	0.00	0.28	0.00
		Technical Standards Doc & Awareness	0.34	0.00	0.24	0.00
		Sanction Documentation & Awareness	0.17	0.00	1.00	0.00
Awareness & Training	0.01	Communications	0.17	0.00	0.69	0.00
		Awareness Events	0.18	0.00	0.74	0.00
		Information Portal	0.10	0.00	0.19	0.00
		Training	0.24	0.00	0.79	0.00
Technical Hygiene	0.96	Behavioral Testing & Real-time Teaching	0.31	0.00	0.68	0.00
		Physical Controls	0.13	0.12	0.78	0.10
		Asset Management	0.18	0.17	0.26	0.05
		Routine Security Updates	0.23	0.22	0.75	0.17
Mitigation of External Threats	0.01	Protection of Store Info & Info in Transit	0.21	0.20	0.69	0.14
		Identity, Authentication, Access Mgmt	0.25	0.24	0.65	0.16
		Data Loss Prevention	0.20	0.00	0.70	0.00
		Anti-spam & Malware Protection	0.25	0.00	1.00	0.00
						0.00
						0.00
						0.00
						0.00
						0.63

Appendix H: Acronyms

Acronym	Description
AEHIS	Association for Executive in Health Information Security
AHP	Analytical Hierarchy Process
ANP	Analytical Network Process
ARRA	American Recovery and Reinvestment Act
CAH	Critical Access Hospital
CCD	Continuity of Care
CHIME	College of Health Information Management Executives
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CMS	Centers for Medicare and Medicaid Services
COBIT	Control Objectives for Information and Related Technologies
CPO	Chief Privacy Officer
CSF	CyberSecurity Framework
DEA	Data Envelopment Analysis
DLP	Data Loss Protection
DMU	Decision Making Unit
EBSCO	Elton B. Stephens Company
ELECTRE	Elimination and Choice Expressing Reality
EMR	Electronic Medical Record
EMRAM	Electronic Medical Record Adoption Model
GIAA	Geometrical Analysis for Interactive Aid
GIAC	Global Information Assurance Certification
HDM	Hierarchical Decision Model
HHS	Health and Human Services
HIMSS	Health Information Management Systems Society
HIPPA	Health Insurance Portability and Accountability Act
HIT	Health Information Technology
HITRUST	Health Information Trust Alliance
ICC	Intraclass Correlation Coefficient
ICU	Intensive Care Unit
IDN	Integrated Delivery Network
INFOSEC	Information Security
ISACA	Information Security and Control Association
ISC2	International Information Systems Security Certification Consortium
ISO	International Organization for Standardization
ISSA	Information Systems Security Association
IT	Information Technology
MAUT	Multi Attribute Utility Theory
MCDA	Multi Criteria Decision Analysis
MDM	Mobile Device Management
MOGSA	Mission Objective Goals Strategies Activities/Actions
NIS	Negative Ideal Solution
NIST	National Institute of Standards and Technology
OAT	One at a time
OCR	(The Department of Health and Human Services') Office for Civil Rights
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Assessment
ONC	Office of the National Coordinator
PBMA	Program Budgeting and Marginal Analysis
PIS	Positive Ideal Solution
PHI	Protected Health Information
PROMETHEE	Elimination and Choice Expressing Reality
SACH	Stand-alone community hospital
SIEM	Security Information and Event Management System
SMART	Specific, Measurable/Manageable, Actionable, Relevant, Timely/Trending
SME	Subject Matter Expert
TOPSIS	Technique for Order Preference by Similarity to Ideal Solutions